

RÉNYI ALFRÉD VÁLOGATOTT MUNKÁI 3

1962–1970

A Magyar Tudományos Akadémia megbízásából
sajtó alá rendezte és jegyzetekkel ellátta

TURÁN PÁL

A Magyar Tudományos Akadémia rendes tagja



AKADÉMIAI KIADÓ · BUDAPEST 1976

SELECTED PAPERS OF ALFRÉD RÉNYI 3 1962–1970

Editor

commissioned by the Hungarian Academy of Sciences

PÁL TURÁN

Member of the Hungarian Academy of Sciences



AKADÉMIAI KIADÓ · BUDAPEST 1976

Co-editors

PÁL BÁRTFAI
IMRE CSISZÁR
JÓZSEF FRITZ
GÁBOR HALÁSZ
GYULA KATONA

PÁL RÉVÉSZ
DOMOKOS SZÁSZ
ENDRE SZEMERÉDI
ISTVÁN VINCZE

Technical editor

GÁBOR SZÉKELY

ISBN 963 05 0913 X Vols 1—3

ISBN 963 05 0916 4 Vol. 3

© Akadémiai Kiadó • Budapest 1976

Printed in Hungary

CONTENTS

General remarks to the edition 11

The life of Alfréd Rényi 13

The works of Alfréd Rényi 17

VOLUME 1

SELECTED PAPERS 1948-1956

3. Integral formulae in the theory of convex curves 33
4. On the minimal number of terms of the square of a polynomial 42
7. On a new application of the I. M. Vinogradov method 48
8. On some conjectures in the theory of Dirichlet characters (with Yu. V. Linnik) 53
12. Simple proof of a theorem of Borel and the law of the iterated logarithm 60
14. Generalization of the "large sieve" of Yu. V. Linnik 68
15. On the zeros of the L -functions of Dirichlet 72
17. On the representation of integers $1, 2, \dots, n$ by differences (with L. Rédei) 76
18. Some remarks on independent random variables 81
19. On the measure of equidistribution of point sets 85
20. Un nouveau théorème concernant les fonctions indépendantes et ses applications à la théorie des nombres 101
23. Sur un théorème général de probabilité 113
24. On the coefficients of schlicht functions 123
26. On a theorem of Erdős and Turán 130
27. Some problems and results on consecutive primes (with P. Erdős) 134
29. On the large sieve of Ju. V. Linnik 145
30. On the geometry of conformal mapping 153
31. On the algebra of distributions 161
33. On Newton's method of approximation 176
34. Mathematical Notes, I. On the summability of Cauchy—Fourier series 188
36. Contributions to the theory of limit theorems for the sum of independent random variables 191
38. Remarks concerning the zeros of certain integral functions 199
39. On composed Poisson distributions, I (with L. Jánosy and J. Aczél) 202
46. Sur l'indépendance des domaines simples dans l'espace euclidien à n dimensions (with Kató Rényi and J. Surányi) 218
50. On composed Poisson distributions, II 224
54. On the approximation of measurable functions (with L. Pukánszky) 238
59. On a conjecture of H. Steinhaus 242
64. On projections of probability distributions 251
67. Probabilistic determination of the electricity need of machine-industrial plants and that of their coefficient of simultaneity and their coefficient of necessity (energy-need) (with T. Szentmártony) 262

- 68. Rational dimensioning of compressors and airtanks to provide compressed air for plants 280
- 69. On processes generated by Poisson process and on their technical and physical applications (with L. Takács) 312
- 71. On the zeros of polynomials (with P. Turán) 319
- 84. On the theory of order statistics 328
- 88. A discussion of chemical reactions using the theory of stochastic processes 367
- 89. New criteria for the comparison of two samples 381
- 94. Elementary proofs of some basic facts concerning order statistics (with G. Hajós) 403
- 100. Mathematical investigation of chemical countercurrent distribution, in case of non-complete diffusion (with P. Medgyessy, K. Tettamanti and I. Vincze) 409
- 106. On a combinatorial problem arising in connection with the selection of alfalfa 424
- 107. On the completeness of certain trigonometric systems (with J. Czipser) 435
- 109. Generalization of an inequality of Kolmogorov (with J. Hájek) 453
- 110. On a new axiomatic theory of probability 457
- 112. On the density of certain sequences of integers 506
- 116. An inequality for uncorrelated random variables (with E. Zergényi) 513
- 117. On the distribution of the digits in Cantor's series 517
- 118. On some combinatorial problems (with P. Erdős) 534
- 119. On the limiting distribution of sums of independent random variables in commutative compact topological groups (with A. Prékopa and K. Urbanik) 542
- 120. On conditional probability spaces generated by a dimensionally ordered set of measures 547
- 121. On the notion of entropy (with J. Balatoni) 558
- 122. The probability of synaptic transmission in simple models of interneuronal synapses with convergent coupling (with J. Szentágothai) 587
- 123. On the number of zeros of successive derivatives of analytic functions (with P. Erdős) 595
- 124. On the regulation of prices (with A. Bródy) 614
- 127. A characterization of the Poisson process 622

VOLUME 2

SELECTED PAPERS 1956-1961

- 128. On the independence in the limit of sums depending on the same sequence of independent random variables (with A. Prékopa) 33
- 131. A new deduction of Maxwell's law of velocity distribution 40
- 132. Probabilistic proof of a theorem on the approximation of continuous functions by means of generalized Bernstein polynomials (with M. Arató) 49
- 133. On the asymptotic distribution of the sum of a random number of independent random variables 57
- 134. On the number of zeros of successive derivatives of entire functions of finite order (with P. Erdős) 64
- 135. A probabilistic approach to problems of diophantine approximation (with P. Erdős) 67
- 136. Mathematical notes, II. On the sequence of generalized partial sums of a series 81
- 137. A remark on the theorem of Simmons 94
- 139. Representations for real numbers and their ergodic properties 96

143. Über den Begriff der Entropie (with J. Balatoni) 113
144. On a theorem of Erdős—Kac (with P. Turán) 131
145. Some remarks on univalent functions 146
146. Some remarks on univalent functions, II 155
148. On mixing sequences of sets 159
149. On a one-dimensional random space-filling problem 173
150. On Engel's and Sylvester's series (with P. Erdős and P. Szűsz) 189
151. Probabilistic methods in number theory 215
152. On Cantor's products 273
153. On mixing sequences of random variables (with P. Révész) 278
154. On singular radii of power series (with P. Erdős) 283
155. On the probabilistic generalization of the large sieve of Linnik 293
157. Some further statistical properties of the digits in Cantor's series (with P. Erdős) 299
158. On random graphs I (with P. Erdős) 308
159. On a theorem of P. Erdős and its application in information theory 316
160. On the dimension and entropy of probability distributions 320
161. New version of the probabilistic generalization of the large sieve 343
162. On the central limit theorem for samples from a finite population (with P. Erdős) 353
163. Some remarks on the theory of trees 363
164. On Cantor's series with convergent $\sum 1/q_n$ (with P. Erdős) 375
165. On serial and parallel coupling of autoclaves and on the theory of mixing 393
166. On measures of dependence 402
167. On connected graphs, I 413
168. Summation methods and probability theory 417
169. On the central limit theorem for the sum of a random number of independent random variables 426
170. Additive properties of random sequences of positive integers (with P. Erdős) 436
171. Limit theorems of random walks 464
172. On the evolution of random graphs (with P. Erdős) 482
174. Some fundamental questions of information theory 526
175. Dimension, entropy and information 553
180. On measures of entropy and information 565
181. A general method for proving theorems in probability theory and some applications 581
182. On random generating elements of a finite Boolean algebra 603
183. On the strength of connectedness of a random graph (with P. Erdős) 610
184. On a classical problem of probability theory (with P. Erdős) 617
185. On Kolmogoroff's inequality 622
186. Legendre polynomials and probability theory 626
187. On a problem of information theory 631
188. On random subsets of a finite set 639

VOLUME 3

SELECTED PAPERS 1962-1970

193. On statistical laws of accumulation of information 33
194. On the extreme elements of observations 50
195. Three new proofs and a generalization of a theorem of Irving Weiss 67

198. On a problem of A. Zygmund (with P. Erdős) 80
199. A new approach to the theory of Engel's series 88
200. On the representation of an even number as the sum of a prime and of an almost prime 96
201. On a problem in the theory of graphs (with P. Erdős) 126
208. Über die konvexe Hülle von n zufällig gewählten Punkten (with R. Sulanke) 143
209. On stable sequences of events 153
210. On the distribution of values of additive number-theoretical functions 164
211. A study of sequences of equivalent events as special stable sequences (with P. Révész) 174
212. On "small" coefficients of the power series of entire functions (with Kató Rényi) 181
213. On two problems of information theory (with P. Erdős) 193
214. On random matrices (with P. Erdős) 207
215. An elementary inequality between the probabilities of events (with P. Erdős and J. Neveu) 214
216. Asymmetric graphs (with P. Erdős) 220
223. Über die konvexe Hülle von n zufällig gewählten Punkten. II (with R. Sulanke) 242
228. On an extremal property of the Poisson process 252
229. A generalization of a theorem of E. Vincze (with R. G. Laha and E. Lukács) 258
230. On two mathematical models of the traffic on a divided highway 261
231. On the amount of information concerning an unknown parameter in a sequence of observations 272
236. On the amount of information in a frequency-count 280
237. Sur les espaces simples des Probabilités conditionnelles 284
242. On the foundations of information theory 304
243. Probabilistic methods in group theory (with P. Erdős) 319
244. Some remarks on periodic entire functions (with Kató Rényi) 331
247. On certain representations of real numbers and on sequences of equivalent events 339
249. On the theory of random search 351
250. On the mean value of nonnegative multiplicative number-theoretical functions (with P. Erdős) 371
251. A new proof of a theorem of Delange 390
260. On a problem of graph theory (with P. Erdős and Vera T. Sós) 397
263. On the existence of a factor of degree one of a connected random graph (with P. Erdős) 420
265. On the amount of missing information and the Neyman-Pearson lemma 432
266. On the amount of information in a random variable concerning an event 440
284. Remarks on the Poisson process 444
285. Statistics and information theory 449
286. On the height of trees (with Gy. Szekeres) 457
287. Remarks on the Poisson process 469
288. On some basic problems of statistics from the point of view of information theory 479
301. On some problems in the theory of order statistics 492
302. Zufällige konvexe Polygone in einem Ringgebiet (with R. Sulanke) 502
303. On quadratic inequalities in probability theory (with J. Galambos) 514
304. On random matrices II (with P. Erdős) 522
305. Information and statistics 528
315. Some remarks on the large sieve of Yu. V. Linnik (with P. Erdős) 531

- 318. On random entire functions (with P. Erdős) 542
- 319. Measures in denumerable spaces (with A. Hanisch and W. M. Hirsch) 551
- 328. On some problems of statistics from the point of view of information theory
- 332. On the enumeration of trees 577
- 341. Stochastische Prozesse in der Biologie 581
- 342. On a new law of large numbers (with P. Erdős) 588
- 343. The Prüfer code for k -trees (with Kató Rényi) 598
- 344. On the enumeration of search-codes 630
- 347. On the number of endpoints of a k -tree 641
- 350. Applications of probability theory to other areas of mathematics 647
- 355. The stochastic geyser 666

GENERAL REMARKS TO THE EDITION

The volumes contain selected papers of Alfréd Rényi. Some of his papers were published in a number of versions, in such cases the most complete version has been published here — translated if necessary into English.

As far as we know no unpublished manuscripts or half-ready notes were left by him; he was a quick worker. The order of the papers printed in these volumes follows the order of chronology.

The first number at the top of the title page of each paper refers to the serial number figuring in the complete list of the works of A. Rényi. The notes are intended to illustrate the effect of Rényi's papers; the name of the commentator is always indicated by initials at the end of the respective notes. Not every paper has been commented on, mostly only groups of coherent papers. In such cases, at the end of the respective paper, a group of numbers is given of which the bold face indicates the citation of the note. The other numbers refer to papers which are connected with the discussed topic.

THE LIFE OF ALFRÉD RÉNYI

(1921 — 1970)

The explosive development of all the sciences has made our age one of specialized research. Fewer and fewer scientists take an active interest in the progress of knowledge outside their own delimited field, and fewer still would ever attempt any kind of interdisciplinary synthesis. Hungary's Alfréd Rényi was one of these very few, a scholar eager and able to use his specialist's knowledge of mathematics to solve problems in altogether different disciplines.

A man of catholic interests, Rényi's life was one of intense and creative involvement in the exchange of ideas and in public affairs. When death claimed him at 49, he was in his prime.

Alfréd Rényi was born in Budapest on March 20, 1921, the only child of Artur Rényi, a mechanical engineer, and Barbara Alexander, a daughter of the philosopher and literary critic Bernát Alexander. One might, thus, say that Rényi's love of literature and his strong devotion to Greek philosophy were his maternal heritage. In 1939, he finished secondary school in Budapest with top marks, but the newly passed racist laws debarred him from the university where his grandfather had once been professor. The autumn of 1939 he won honourable mention in the annual competition of the Mathematical Society, and in a Greek competition. After spending half a year as a labourer in the Ganz Shipyard in Budapest, he was admitted to the university the autumn 1940 to study mathematics and physics. I first met him in October or November of 1941 when he, with N. Schweitzer and G. Freud, started regularly to attend a lecture series I held to June of 1942. The main topic of discussion was number theory; at that time, Schweitzer seemed to be the one more interested in this subject.

Rényi finished his university studies in May of 1944; in June he was called up for forced-labour service. Fortunately, his company was not taken from Hungary immediately. When the order to evacuate to the West did come, Rényi escaped, and lived in Budapest using false documents. Whenever I met him during those days, I was amazed at his level-headedness and courage. In March, 1945, he got his Ph. D. at Szeged under F. Riesz. Returning to Budapest, he held various jobs as a statistician. In 1946 he married Katalin Schulhof, a noted mathematician. In October 1946, he went to Leningrad to work with Linnik; there he stayed till the next June. His progress during these few months — the first time in his life that he could concentrate fully on studying mathematics — was truly amazing. Previously, as appears from his publications, his interest centred mainly on series theory, although, as I mentioned, he also had some experience in number theory. His knowledge of probability theory, however, was unlikely to be more than rudimentary and

his command of Russian was but elementary. Yet these few months were enough for him to acquire a creative understanding of the works of the Soviet number theorists, mainly of the works of I. M. Vinogradov and Linnik; to write and defend his famous thesis; to publish two other papers; and to become thoroughly familiar with the theory of probability which was to become his main mathematical interest. His development during those months was nothing short of phenomenal. By an effort of the will, he had effaced his memories of the war years and of the forced-labour camp, to centre now on his work all the fiery energy of his youth and of his exceptional gifts of understanding and concentration.

On returning to Budapest, he was appointed University Privatdocent and Assistant Professor in October 1947. In 1949, he was appointed Professor Extraordinary in Debrecen and held this position till September 1950, when he became director of the Academy's newly established Institute of Applied Mathematics. He became a corresponding member of the Hungarian Academy of Sciences in 1949, and was elected ordinary member in 1956. From 1952 until his untimely death, he was a professor of the Department of Probability and Statistics of Eötvös Loránd University.

Eloquently as the fruits of Rényi's Leningrad sojourn testify to the extraordinary quickness and perceptiveness of his mind, one can hardly help feeling — on considering how very much he produced in so short a life — that only a man devoted exclusively to his own scientific work could leave behind such an opus. This was, in fact, very far from being the case. His teaching, as much as his administrative duties he fulfilled with great skill and enthusiasm. Indeed, within a short time he made of his Institute (later renamed the Mathematical Research Institute of the Hungarian Academy of Sciences) a mathematical centre of international repute, while as a professor, he laid the foundations of the first school of probability in Hungary. From 1949 to 1953, he was secretary of the Mathematical Section of the reorganised Hungarian Academy of Sciences — the first to hold that office — and took a very active part in the work of several of its committees after that time. From 1949 to 1955, he was secretary of the Bolyai János Mathematical Society, and played a leading role in organising the Ist and IInd Mathematical Congresses held in 1950 and 1960, respectively. He was on the editorial board of all Hungarian mathematical journals: of *Zeitschrift für Wahrscheinlichkeitstheorie*; of the *Journal of Combinatorial Theory*; of the *Journal of Applied Probability*; of *Information and Control*, and of the *International Journal of Computer Mathematics*. Over and above all this, he was active as a reviewer in *Referativnii Zhurnal*, *Mathematical Reviews* and the *Statistical Theory and Method Abstracts*.

Open to public duties, Rényi was at all times open also to mathematical discussion and cooperation. In fact, he produced joint papers with 36 co-authors on a variety of subjects. If one draws a graph taking all mathematicians of the world as the vertices and connects two vertices by an edge iff the corresponding mathematicians have a joint paper, then — as Erdős remarked — he, Rényi, Szekeres and Turán form a complete subgraph of order 4 in this graph.

In a short autobiography written in his last years, Rényi gave the following as the subjects of his papers: probability theory, statistics, information theory, combinatorics, graph theory, number theory and analysis. The order of listing — not an alphabetical one — in itself indicates that his interest in probability theory prevailed over all his other scholarly interests. Practically all his

mathematical works were, in fact, interwoven — though sometimes implicitly — with probabilistic ideas. This is seen most clearly in two papers he wrote in Hungarian, the ones entitled “Probabilistic Methods in Analysis”. In these, he surveys various parts of the analysis, picks out some interesting results, and points out their probabilistic core. There is some indication in these papers that he had intended to continue these investigations. His skill in the application of probability was simply amazing. As even a cursory glance at the complete list of Rényi’s papers (sometimes written with co-authors) will show, he applied probability theory to solve concrete problems ranging from industry, chemistry and biology to traffic and price control. The main difficulty in all these undertakings was to find the suitable model, which “approximated” reality and was “computable”. His ability to understand the essence of a situation and his skill in finding for it an abstract mathematical model — an abstraction that we might think of as analogous to the Brechtian *Verfremdungseffekt* — was really remarkable.

For Rényi, however, abstract models had a charm of their own quite independently of their usefulness in the solution of any concrete problem. That this was indeed so appears from the first lines of the paper (No. 201) he wrote with Erdős, where the starting point is a problem of the “pseudo-application” type: Let there be given a country with n cities, n large, so that a direct air connection between any two cities would require two busy airports. Considering the capacity limits of the airports, what is the minimum number of flights that would get a passenger from any one city to another so that he need change planes not more than once? This is a question that can be nicely reformulated and treated as an extremal graph problem. This airport problem is rather unlikely ever to occur in reality and its solution was in all probability never meant for application. But in a person as imbued with mathematics as Rényi was, speculation as to how to overcome the difficulties of not getting a direct flight to some city almost automatically led to the formulation of a mathematical solution to his dilemma. The desire to find the optimal means of reaching his destination found expression in speculation as to how to devise a schedule so that a *single* change of planes would always suffice. At this point, the fascination of the immediately resulting graph problem tends to make one forget all the impractical features of the model, as one becomes more interested in the exciting mathematical problem that is its result.

A singular part of Rényi’s oeuvre is the essays collected in his *Ars Mathematica*. I have mentioned Rényi’s literary heritage; ever since his childhood, he had been on friendly terms with outstanding literary figures — Gábor Devecseri, Ferenc Karinthy, György Somlyó and many others. All this, however, would probably not have been sufficient to impell him to write these essays. It was rather a series of debates on the applications of mathematics which prompted him to do so. These debates sparked by a paper he had written on commission from an Academy Committee (No. 202) turned into vehement and open personal attacks on Rényi and went on for some years — as some articles from *Magyar Tudomány* (see e.g. No. 219) will show. They were debates that consumed much of his energy. The first three essays, in particular “Dialogue on Applications of Mathematics” and the one on Galileo grew directly out of these debates, and bear witness to a highly cultured and sophisticated mind.

Of course, Rényi’s activities also met with appreciation from many quarters. In 1949, he was awarded the second, in 1954, the first grade of the Kossuth

Prize for his scientific work. In 1951, he received the fourth grade of the "Medal of the People's Republic" for his organizational work. He was invited to lecture at the International Mathematical Congress of Edinburgh in 1958, and was Rouse Ball lecturer in Cambridge in 1966. The summer of 1961 he spent one semester at the Michigan State University; in 1964, one semester at the University of Michigan; and in 1969 one semester at the University of North Carolina as visiting professor. Between 1965 and 1969, he was a member, and then vice president of the International Statistical Institute, and was elected honorary member of Churchill College in Cambridge.

Rényi's zest for life was by no means exhausted in his many-sided intellectual activities and involvement in public affairs. He was fond of rowing and swimming in the Danube in summer and of skiing in winter. With his wife and daughter Zsuzsa (born in 1948) he frequented concerts and theatres; at the parties they gave in their home, Rényi entertained his friends with witty anecdotes and with playing the piano. Those entering his study were welcomed by bookshelves jammed to the ceiling. The books, manuscripts and notes scattered on his desk made the visitor feel that he had entered the scene of creative, productive activity, an activity that Alfréd Rényi carried on unabated to the last day of his life.

PÁL TURÁN

THE WORKS OF ALFRED RÉNYI⁺

1. *Cauchy – Fourier sorok szummálhatóságáról* (On the summability of Cauchy – Fourier series). Doctoral Thesis, Szeged, 1945. (MS.)
2. On a Tauberian theorem of O. Szász. *Acta Sci. Math. Szeged*, 11 (1946/48), 119–123.
3. Integral formulae in the theory of convex curves. *Acta Sci. Math. Szeged*, 11 (1946/48), 158–166.
4. On the minimal number of terms of the square of a polynomial. *Hung. Acta Math.*, 1 (1946/49), No. 2, 30–34.
5. О представлении четных чисел в виде суммы одного простого и одного почти-простого числа. Докл. АН СССР, 56 (1947), 455–458.
6. О представлении четных чисел в виде суммы простого и одного почти-простого числа. Диссертация. Ленинград, 1947. (MS.)
7. Об одном новом применении метода академика И. М. Виноградова. Докл. АН СССР, 56 (1947), 675–678.
8. О некоторых гипотезах теории характеров Дирихле (with Yu. V. Linnik). Изв. АН СССР, 11 (1947), 539–546.
9. О представлении четных чисел в виде суммы простого и почти-простого числа. Изв. АН СССР, 12 (1948), 57–75.
10. Játék a véletlennel. I. (Playing with chances. I.). *Középisk. Mat. Lapok*, 1 (1948), 101–111.
11. Játék a véletlennel. II. (Playing with chances. II.). *Középisk. Mat. Lapok*, 1 (1948), 144–157.
12. Simple proof of a theorem of Borel and of the law of the iterated logarithm. *Mat. Tidsskrift B*, 1948, 41–48.
13. Remarque à la note précédente (to G. Alexits: Sur la convergence des séries lacunaires. *Acta Sci. Math. Szeged*, 11 (1946/48), 251–253). *Acta Sci. Math. Szeged*, 11 (1946/48), 253.
14. Generalization of the “large sieve” of Yu. V. Linnik. Math. Centrum, Amsterdam, (1948) 5 p. (Mimeographed.)
15. On the zeros of the *L*-functions of Dirichlet. Math. Centrum Amsterdam (1948) 4 p. (Mimeographed.)
16. Proof of the theorem that every integer can be represented as the sum of a prime and an almost prime. Math. Centrum, Amsterdam (1948), 3 p. (Mimeographed.)
17. О представлении чисел 1, 2, ..., *n* посредством разностей (with L. Rédei). Мат. сборник, 24 (1949), 385–389.
18. Some remarks on independent random variables. *Hung. Acta Math.*, 1 (1946/48), No. 4, 17–20.
19. On the measure of equidistribution of point sets. *Acta Sci. Math. Szeged*, 13 (1949), 77–92.
20. Un nouveau théorème concernant les fonctions indépendantes et ses applications à la théorie des nombres. *Jour. Math. Pures Appl.*, 28 (1949), 137–149.
21. A szovjet matematika 30 éve (30 years of Soviet mathematics). *Természet és Technika*, 108 (1949), 220–226.
22. Probability methods in number theory. *Publ. Math. Coll., Budapest*, 1 (1949), No. 21, 9 pp.
23. Sur un théorème général de probabilité. *Annales Inst. Fourier*, 1 (1949), 43–52.
24. On the coefficients of schlicht functions. *Publ. Math. Debrecen*, 1 (1949), 18–23.

+ Compiled by P. Medgyessy.

25. A szovjet matematika 30 éve. I. A valószínűségszámítás megalapozásáról (30 years of Soviet mathematics. I. On the foundation of the theory of probability). *Mat. Lapok*, 1 (1949/50), 27–64.
26. On a theorem of Erdős and Turán. *Proc. Amer. Math. Soc.*, 1 (1950), 7–10.
27. Some problems and results on consecutive primes (with P. Erdős). “Simon Stevin”, 27 (1949/50), 115–125.
28. A szovjet matematika 30 éve. II. A valószínűségszámítás új irányai (30 years of Soviet mathematics. II. New tendencies in the theory of probability). *Mat. Lapok*, 1 (1949/50), 91–137.
29. On the large sieve of Ju. V. Linnik. *Comp. Math.*, 8 (1950), 68–75.
30. On the geometry of conformal mapping. *Acta Sci. Math. Szeged*, 12 (1950), Pars B, 215–222.
31. On the algebra of distributions. *Publ. Math. Debrecen*, 1 (1950), 135–149.
32. Az aprítás matematikai elméletéről (On the mathematical theory of pounding). *Építőanyag*, 2 (1950), Nos. 9–10, 7 pp.
33. A Newton-féle gyökközelítő eljárásról (On Newton's method of approximation). *Mat. Lapok*, 1 (1949/50), 278–293.
34. On the summability of Cauchy–Fourier series. *Publ. Math. Debrecen*, 1 (1950), 162–164.
35. Об одной общей теореме теории вероятностей и ее применении в теории чисел. Zpráva o společném 3. sjezdu matematiků Československých a 7. sjezdu matematiku Polských, Praha, 1950. *Časopis Pěst. Mat. Fys.*, 74 (1949), 167–175.
36. К теории предельных теорем для сумм независимых случайных величин. *Acta Math. Acad. Sci. Hung.*, 1 (1950), 99–108.
37. Harc a formalizmus ellen a matematika tanításában (Struggle against formalism in teaching mathematics). *A középiskolai matematikatanítás kérdései*. Szocialista Nevelés Kiskönyvtára. 4. sz. Közoktatásügyi Kiadó Vállalat, Budapest, 1950, 24–28.
38. Remarks concerning the zeros of certain integral functions. *C. R. Acad. Bulg. Sci.*, 3 (1950), Nos. 2–3, 9–10.
39. On composed Poisson distributions. I (with L. Jánossy and J. Aczél). *Acta Math. Acad. Sci. Hung.*, 1 (1950), 209–224.
40. *Valószínűségszámítás* (Probability theory; lecture notes). Egyetemi jegyzet. A Debreceni Tudományegyetem Matematikai Intézete, Debrecen, 1950. (Mimeographed.)
41. *Valószínűségszámítás* (Probability theory; lecture notes). Egyetemi jegyzet. Az Eötvös Loránd Tudományegyetem Természettudományi Kara, Budapest, 1950. (Mimeographed.)
42. A valószínűségszámítás központi határértéktételének egy új általánosításáról (On a new generalization of the central limit theorem). *MTA III. Osz. Közl.*, 1 (1951), 351–355.
43. A Magyar Tudományos Akadémia Alkalmazott Matematikai Intézetének feladatairól (On the tasks of the Mathematical Institute of the Hungarian Academy of Sciences). *Akad. Ért.*, 58 (1951), No. 483, Jan.-Febr., 1951, 20–26.
44. A Poisson-eloszlás problémaköréről (On problems connected with the Poisson distribution). *MTA III. Osz. Közl.*, 1 (1951), 202–212.
45. On some problems concerning Poisson processes. *Publ. Math. Debrecen*, 2 (1951), 66–73.
46. Sur l'indépendance des domaines simples dans l'espace euclidien à n dimensions (with Kató Rényi and J. Surányi). *Colloqu. Math.*, 2 (1951), 130–135.
47. Összetett Poisson-eloszlásokról. I. (On composed Poisson distributions. I.; with L. Jánossy and J. Aczél). *MTA III. Osz. Közl.*, 1 (1951), 315–328.
48. Об основах теории вероятностей. *Annuaire Fac. Sci. Phys. Math., Univ. Sofia*, Livre 1, Partie 1, 47 (1951), 227–236.
49. *Základy theorie pravděpodobnosti* (Foundation of the probability theory). *Mat. Ustav Československe Akad. Ved.*, Praha, 1951, 10 pp. (Mimeographed.)
50. On composed Poisson distributions. II. *Acta Math. Acad. Sci. Hung.*, 2 (1951), 83–98.
51. Összetett Poisson-eloszlásokról. II. (On composed Poisson distributions. II.). *MTA III. Osz. Közl.*, 1 (1951), 329–341.
52. Két bizonyítás Jánossy Lajos egy tételére (Two proofs of a theorem of L. Jánossy; with P. Turán). *MTA III. Osz. Közl.*, 1 (1951), 369–370.
53. Hozzászólás (Remarks) (to Hőmunkások víz- és sóanyagcseréje. — A matematikai statisztika módszereinek alkalmazása az orvostudományban [Water and salt metabolism of people working under hot conditions. — The application of mathematical

- statistical methods in medicine]. *Orvosi Hetilap*, **92** (1951), No. 29, 20). *Orvosi Hetilap*, **92** (1951), No. 29, 6.
54. On the approximation of measurable functions (with L. Pukánszky). *Publ. Math. Debrecen*, **2** (1951), 146–149.
 55. *Komplex függvénytan* (Complex analysis; lecture notes). Egyetemi jegyzet. Tankönyvkiadó, 1. Jegyzetsokszorosító, Budapest, 1951, 34 pp.
 56. *Komplex függvénytan* (Complex analysis; lecture notes). Egyetemi jegyzet. VKM 2. Jegyzetsokszorosító, Budapest, 1951, 59 pp.
 57. Sztochasztikus függetlenség és teljes függvényrendszerek (Stochastic independence and complete system of functions). *Az Első Magyar Matematikai Kongresszus Közleményei*. 1950. augusztus 27–szeptember 2. Akadémiai Kiadó, Budapest, 1952, 299–308.
 58. Стохастическая независимость и полные системы функций. *Az Első Magyar Matematika Kongresszus Közleményei*. 1950. augusztus 27–szeptember 2. Akadémiai Kiadó, Budapest, 1952, 309–316.
 59. On a conjecture of H. Steinhaus. *Annales Soc. Polon. Math.*, **25** (1952), 279–287.
 60. Hozzászólás (Remarks) (to L. Kalmár: A matematika alapjaival kapcsolatos újabb eredmények [New results concerning the foundation of mathematics]. *MTA III. Oszt. Közl.*, **2** (1952), 89–103). *MTA III. Oszt. Közl.*, **2** (1952), 104–107.
 61. Újabb eredmények a valószínűségszámítás terén (New results in the theory of probability). *MTA III. Oszt. Közl.*, **2** (1952), 125–139.
 62. Ismertetés A. Ja. Hinchin "A statisztikai mechanika analitikus módszerei" c. könyvéről (Review of the book A. Ya. Khinchin: Analytical methods of statistical mechanism; with I. Fényes). *MTA III. Oszt. Közl.*, **2** (1952), 275–280.
 63. A valószínűségszámítás elvi kérdései a dialektikus materializmus megvilágításában (Basic problems of the theory of probability in the light of dialectical materialism). *Filozófiai Évkönyv*, 1952. Akadémiai Kiadó, Budapest, 1952, 63–97.
 64. On projections of probability distributions. *Acta Math. Acad. Sci. Hung.*, **3** (1952), 131–142.
 65. Jordan Károly matematikai munkásságáról (On the mathematical work of K. Jordan). *Mat. Lapok*, **3** (1952), 111–121.
 66. Gépkatrészek és felszerelési tárgyak törzskészletének valószínűségszámítási meghatározása (Probabilistic determination of basic reserve of parts and of mountings; with T. Szentmártony). *Mat. Lapok*, **3** (1952), 129–139.
 67. Gépipari üzemek elektromos energiaszükségletének és egyidejűségi, illetőleg szükségleti tényezőjének valószínűségszámítási meghatározása (Probabilistic determination of the electricity need of machine-industrial plants and that of their coefficient of simultaneity and their coefficient of necessity (energy-need); with T. Szentmártony). *MTA Alk. Mat. Int. Közl.*, **1** (1952), 85–104.
 68. Kompresszorok és légtartályok racionális méretezése üzemek sűrített levegővel való ellátására (Rational dimensioning of compressors and airtanks to provide compressed air for plants). *MTA Alk. Mat. Int. Közl.*, **1** (1952), 105–138.
 69. Poisson-folyamatok által származtatott történet-folyamatokról és azok technikai és fizikai alkalmazásairól (On processes generated by Poisson process and on their technical and physical applications; with L. Takács). *MTA Alk. Mat. Int. Közl.*, **1** (1952), 139–146.
 70. Megjegyzések Gombás Pál és Gáspár Rezső egy dolgozatához (Remarks on a paper of P. Gombás and R. Gáspár). *MTA Alk. Mat. Int. Közl.*, **1** (1952), 393–397.
 71. On the zeros of polynomials (with P. Turán). *Acta Math. Acad. Sci. Hung.*, **3** (1952), 275–284.
 72. Bolyai János, a tudomány nagy forradalmára (J. Bolyai, the great revolutionist of science). *Mat. Lapok*, **3** (1952), 173–178.
 73. *Valószínűségszámítás* (Probability theory; lecture notes). Egyetemi jegyzet. Felsőoktatási Jegyzetellátó Vállalat, Budapest, 1952.
 74. H. Steinhaus egy sejtéséről (On a conjecture of H. Steinhaus). *MTA III. Oszt. Közl.*, **3** (1953), 37–44.
 75. Укрепление связи математики с практикой. *Природа*, 1953, 69–73.
 76. Poznámka u uhlech monouhelníka (Remarks on the angles of a polygon). *Časopis Pěst. Mat.*, **78** (1953), 305–306.
 77. Valószínűség-eloszlások vetületeiről (Projections of probability distributions). *MTA III. Oszt. Közl.*, **3** (1953), 59–69.
 78. Bolyai János felfedezésének tudományos és világnézeti jelentősége (On the scientific and ideological significance of the discovery of János Bolyai). *Természet és Technika*, **112** (1953), 1–3.

79. A Bolyai–Lobacsevszkij geometria világnézeti jelentősége (The ideological significance of the Bolyai–Lobachevsky geometry). *MTA III. Oszt. Közl.*, **3** (1953), 253–273.
80. Ideologický význam geometrie Bolyai–Lobačevského (The ideological significance of the Bolyai–Lobachevsky geometry). *Časopis Pěst. Mat.*, **78** (1953), 149–168.
81. Hozzászólás (Remarks) (to L. Jánossy: Beszámoló a berlini fizikus kongresszus egyes problémáiról [Report on some problems of the congress of physicists in Berlin]. *MTA III. Oszt. Közl.*, **3** (1953), 323–325). *MTA III. Oszt. Közl.*, **3** (1953), 326–327.
82. Hozzászólás (Remarks) (to P. Gombás: Elméleti fizikai kutatásokban alkalmazott matematikai módszerek különös tekintettel a kvantummechanikai közelítő módszerekre [Applied mathematical methods in theoretical physics with respect to numerical methods in quantum mechanics]. *MTA III. Oszt. Közl.*, **3** (1953), 329–340). *MTA III. Oszt. Közl.*, **3** (1953), 344–347.
83. Az Alkalmazott Matematikai Intézet munkája a valószínűségszámítás ipari alkalmazásai terén (On the activity of the Mathematical Institute of the Hungarian Academy of Sciences in the industrial application of the theory of probability). *MTA III. Oszt. Közl.*, **3** (1953), 363–372.
84. On the theory of order statistics. *Acta Math. Acad. Sci. Hung.*, **4** (1953), 191–231.
85. A rendezett minták elméletéről (On the theory of order statistics). *MTA III. Oszt. Közl.*, **3** (1953), 467–503.
86. Eine neue Methode in der Theorie der geordneten Stichproben. *Bericht über die Mathematiker-Tagung in Berlin, Januar 1953*. Deutscher Verlag der Wissenschaften, Berlin, 1953, 203–212.
87. Hozzászólás (Remarks) (to Ankét O. J. Smidt „Négy előadás a Föld keletkezésének elméletéről” című könyvről [Conference on O. J. Smidt “Four talks on the genesis of the Earth”]. *MTA III. Oszt. Közl.*, **3** (1953), 579–601). *MTA III. Oszt. Közl.*, **3** (1953), 595–600.
88. Kémiai reakciók tárgyalása a sztochasztikus folyamatok elmélete segítségével (A discussion of chemical reactions using the theory of stochastic processes). *MTA Alk. Mat. Int. Közl.*, **2** (1953), 83–101.
89. Újabb kritériumok két minta összehasonlítására (New criteria for the comparison of two samples). *MTA Alk. Mat. Int. Közl.*, **2** (1953), 243–265.
90. A valószínűségszámítás alapfogalmairól (Basic concepts of the theory of probability). A Mérnöki Továbbképző Intézet előadássorozatából. Felsőoktatási Jegyzetellátó Vállalat, Budapest, 1953, 51 pp.
91. A raktárkészlet pótlásáról. I. (On the replacement policy of stocks; with Ilona Palásti, T. Szentmártony and L. Takács). *MTA Alk. Mat. Int. Közl.*, **2** (1953), 187–201.
92. Valószínűségszámítás (Probability theory; lecture notes). Egyetemi jegyzet. Felsőoktatási Jegyzetellátó Vállalat, Budapest, 1953.
93. Základní problémy počtu pravděpodobnosti ve světle dialektického materialismu (Basic problems of the calculus of probabilities in the light of dialectical materialism). *Časopis Pěst. Mat.*, **79** (1954), 189–218.
94. Elementary proofs of some basic facts concerning order statistics (with Gy. Hajós). *Acta Math. Acad. Sci. Hung.*, **5** (1954), 1–6.
95. Идеологическое значение геометрии Бойан–Лобачевского. *Acta Math. Acad. Sci. Hung.*, **5** (1954), Supplementum, 21–42.
96. A valószínűségszámítás új axiomatikus felépítése (A new axiomatic foundation of the theory of probability). *MTA III. Oszt. Közl.*, **4** (1954), 369–427.
97. A valószínűségszámítás történetének rövid áttekintése (A short survey of the history of the theory of probability). *MTA III. Oszt. Közl.*, **4** (1954), 447–466.
98. Valószínűségszámítás (Probability theory). Tankönyvkiadó, Budapest, 1954.
99. Elemi bizonyítások a rendezett minták elméletének néhány alapvető összefüggésére (Elementary proofs of some basic facts in the theory of order statistics; with Gy. Hajós). *MTA III. Oszt. Közl.*, **4** (1954), 467–472.
100. A kémiai frakcionáló megosztás matematikai tárgyalása nem-teljes diffúzió esetében (Mathematical investigation of chemical counter-current distribution in the case of non-complete diffusion; with P. Medgyessy, K. Tettamanti and I. Vincze). *MTA Alk. Mat. Int. Közl.*, **3** (1954), 81–97.
101. A komplex potenciál egyértékűségéről. I. (On the univalence of the complex potentials. I.; with Kató Rényi). *MTA Alk. Mat. Int. Közl.*, **3** (1954), 353–367.
102. Die prinzipiellen Fragen der Wahrscheinlichkeitsrechnung im Lichte des dialektischen Materialismus. *Philosophisches Jahrbuch*, 1952. Zusammenfassung. Akadémiai Kiadó, Budapest, 1954, 7–8.

103. Hozzászólás (Remarks) (to Kurt Sedlmayer: Nagyobb termések elérésének tudományos alapjai [Scientific basis to reaching greater yields]. *MTA IV. Oszt. Közl.*, 5 (1954)). *MTA IV. Oszt. Közl.*, 5 (1954), 138–200.
104. Egy lucerna nemesítésével kapcsolatos kombinatorikai problémáról (On a combinatorial problem in connection with the improving of alfalfa; a lecture on *Matematikai Statisztikai Kollokvium*. 1954. szeptember hó 27–29., Jósvafő). Bolyai János Matematikai Társulat, Budapest, 1954, 13–15. (MS).
105. Megoldatlan problémák a rendezett minták elméletében (Unsolved problems in the theory of order statistics; a lecture on *Matematikai Statisztikai Kollokvium*. 1954. szeptember hó 27–29., Jósvafő). Bolyai János Matematikai Társulat, Budapest, 1954, 18–20. (MS).
106. Egy kombinatorikai probléma, amely a lucerna nemesítésével kapcsolatban merült fel (On a combinatorial problem arising in connection with the improving of alfalfa). *Mat. Lapok*, 6 (1955), 151–164.
107. Bizonyos trigonometrikus rendszerek teljességéről (On the completeness of certain trigonometric systems; with J. Czipser). *MTA III. Oszt. Közl.*, 5 (1955), 391–410.
108. A matematika fejlődése hazánkban a felszabadulás óta (The development of mathematics in our country since the liberation; with Gy. Alexits and Gy. Hajós). *A magyar tudomány tíz éve. 1945–1955*. Akadémiai Kiadó, Budapest, 1955, 87–106.
109. Generalization of an inequality of Kolmogorov (with J. Hájek). *Acta Math. Acad. Sci. Hung.*, 6 (1955), 281–283.
110. On a new axiomatic theory of probability. *Acta Math. Acad. Sci. Hung.*, 6 (1955), 285–335.
111. A sztochasztikus folyamatok elméletéről és annak néhány műszaki alkalmazásáról (On the theory of stochastic processes and some technical applications). Felsőoktatási Jegyzetellátó Vállalat, Budapest, 1955, 78 pp.
112. On the density of certain sequences of integers. *Publ. Inst. Math. Math. Acad. Serbe Sci., Beograd*, 8 (1955), 157–162.
113. *Matematikai Statisztika* (Mathematical statistics; lecture notes). Egyetemi jegyzet. Jegyzetsokszorosító, Budapest, 1955.
114. Szakkörökben végezhető valószínűségszámítási kísérletekről (On probabilistic experiments which may be carried out in high-school study circles). *Előadások az iskolai matematika köréből*. A Bolyai János Matematikai Társulat Kiadványa. Tankönyvkiadó, Budapest, 1956, 135–150.
115. Axiomatischer Aufbau der Wahrscheinlichkeitsrechnung. *Bericht über die Tagung Wahrscheinlichkeitsrechnung und mathematische Statistik in Berlin, Oktober, 1954*. Deutscher Verlag der Wissenschaften, Berlin, 1956, 7–15.
116. An inequality for uncorrelated random variables (with Erzsébet Zergényi). *Czech. Math. Jour.*, 6/81 (1956), 415–419.
117. A számjegyek eloszlása valós számok Cantor-féle előállításában (On the distribution of the digits in Cantor's series). *Mat. Lapok*, 7 (1956), 77–100.
118. On some combinatorial problems (with P. Erdős). *Publ. Math. Debrecen*, 4 (1955/56), 398–405.
119. О предельном распределении для сумм независимых случайных величин на бикомпактных коммутативных топологических группах (with K. Urbanik and A. Prékopa). *Acta Math. Acad. Sci. Hung.*, 7 (1956), 11–16.
120. On conditional probability spaces generated by a dimensionally ordered set of measures. *Теория вероятностей, и прим.* 1 (1956), 61–71.
121. Az entrópia fogalmáról (On the notion of entropy; with J. Balatoni). *MTA Mat. Kut. Int. Közl.*, 1 (1956), 9–40.
122. Az ingerületátvitel valószínűsége egy egyszerű konvergens kapcsolású interneuronáli synapsis-modellben (The probability of synaptic transmission in simple models of interneuronal synapses with convergent coupling; with J. Szentágothai). *MTA Mat. Kut. Int. Közl.*, 1 (1956), 83–91.
123. On the number of zeros of successive derivatives of analytic functions (with P. Erdős). *Acta Math. Acad. Sci. Hung.*, 7 (1956), 125–144.
124. Az árrendezés problémájáról (On the regulation of prices; with A. Bródy). *MTA Mat. Kut. Int. Közl.*, 1 (1956), 325–335.
125. A Monte-Carlo módszer mint minimax stratégia (Monte Carlo methods as minimax strategies; with Ilona Palásti). *MTA Mat. Kut. Int. Közl.*, 1 (1956), 529–545.
126. Discussion on Dr. David's and Dr. Johnson's paper (on Some tests of significance with ordered variables. *Jour. Roy. Stat. Soc. Ser. B*, 18 (1956), 1–20). *Jour. Roy. Stat. Soc. Ser. B*, 18 (1956), 29.

127. A Poisson-folyamat egy jellemzése (A characterization of the Poisson process). *MTA Mat. Kut. Int. Közl.*, 1 (1956), 519–527.
128. On the independence in the limit of sums depending on the same sequence of independent random variables (with A. Prékopa). *Acta Math. Acad. Sci. Hung.*, 7 (1956), 319–326.
129. On a new axiomatic foundation of the theory of probability. *Proceedings of the International Congress of Mathematicians*, 1954, Amsterdam, September 2–September 9. Vol. I. Noordhoff N. V., Groningen–North-Holland Publishing Co., Amsterdam, 1957, 506–507.
130. On the theory of order statistics. *Proceedings of the International Congress of Mathematicians*, 1954, Amsterdam, September 2–September 9. Vol. I. Noordhoff N. V., Groningen–North-Holland Publishing Co., Amsterdam, 1957, 508–509.
131. A new deduction of Maxwell's law of velocity distribution. *Изв. Мат. Инст., БАН, София*, 2 (1957), 45–53.
132. Probabilistic proof of a theorem on the approximation of continuous functions by means of generalized Bernstein polynomials (with M. Arató). *Acta Math. Acad. Sci. Hung.*, 8 (1957), 91–98.
133. On the asymptotic distribution of the sum of a random number of independent random variables. *Acta Math. Acad. Sci. Hung.*, 8 (1957), 193–199.
134. On the number of zeros of successive derivatives of entire functions of finite order (with P. Erdős). *Acta Math. Acad. Sci. Hung.*, 8 (1957), 223–225.
135. A probabilistic approach to problems of diophantine approximation (with P. Erdős). *Illinois Jour. Math.*, 1 (1957), 303–315.
136. Mathematical Notes. II. On the sequence of generalized partial sums of a series. *Publ. Math. Debrecen*, 5 (1957/58), 129–141.
137. A remark on the theorem of Simmons. *Acta Sci. Math. Szeged*, 18 (1957), 21–22.
138. Valós számok előállítására szolgáló algoritmusokról (On algorithms for the representation of real numbers). *MTA III. Oszt. Közl.*, 7 (1957), 265–293.
139. Representations for real numbers and their ergodic properties. *Acta Math. Acad. Sci. Hung.*, 8 (1957), 477–493.
140. Az $L(z)$ valószínűség-eloszlásfüggvényről (On the distribution function $L(z)$). *MTA Mat. Kut. Int. Közl.*, 2 (1957), 43–50.
141. Szénszemcsés ellenállások vizsgálata valószínűségszámítási módszerrel (Investigating the conductivity of certain resistances by means of probability theory). *MTA Mat. Kut. Int. Közl.*, 2 (1957), 247–256.
142. Über den Begriff der Entropie in der Wahrscheinlichkeitsrechnung (lecture at the IV. Österreichischer Mathematikerkongress Wien, 17–22. IX. 1956). Summary in *Österr. Math. Ges. Beilage zu "Internat. Math. Nachr."*, 11 (1957), April, Nr. 47/48, Sondernummer, 83.
143. Über den Begriff der Entropie (with J. Balatoni). *Arbeiten zur Informationstheorie*. Deutscher Verlag der Wissenschaften, Berlin, 1957; pp. 117–134.
144. On a theorem of Erdős–Kac (with P. Turán). *Acta Arith.*, 4 (1958), 71–84.
145. Some remarks on univalent functions. *Изв. Мат. Инст., БАН, София*, 3 (1958/59), 111–121.
146. Some remarks on univalent functions. II. *Ann. Acad. Sci. Fennicae, Series A. I. Mathematica*. 250/29. Suomalainen Tiedekatemia, Helsinki, 1958, 7 p.
147. Quelques remarques sur les probabilités d'événements dépendants. *Jour. Math. Pures Appl.* (9), 37 (1958), 393–398.
148. On mixing sequences of sets. *Acta Math. Acad. Sci. Hung.*, 9 (1958), 215–228.
149. Egy egydimenziós véletlen térkitöltési problémáról (On a one-dimensional random space-filling problem). *MTA Mat. Kut. Int. Közl.*, 3 (1958), 109–127.
150. On Engel's and Sylvester's series (with P. Erdős and P. Szűsz). *Annales Univ. Sci. Budapest, Sect. Math.*, 1 (1958), 7–32.
151. Probabilistic methods in number theory (in Chinese). *Shuxue Jinzhan*, 4 (1958), 465–510.
152. On Cantor's products. *Colloqu. Math.*, 6 (1958), 135–139.
153. On mixing sequences of random variables (with P. Révész). *Acta Math. Acad. Sci. Hung.*, 9 (1958), 389–393.
154. On singular radii of power series (with P. Erdős). *MTA Mat. Kut. Int. Közl.*, 3 (1958), 159–169.
155. On the probabilistic generalization of the large sieve of Linnik. *MTA Mat. Kut. Int. Közl.*, 3 (1958), 199–206.
156. *Matematikai statisztika IV. éves alkalmazott matematika szakos hallgatók számára*

- (Mathematical statistics for university students of the fourth form; lecture notes). Egyetemi jegyzet. Felsőoktatási Jegyzetellátó Vállalat, Budapest, 1958, 211 pp.
157. Some further statistical properties of the digits in Cantor's series (with P. Erdős). *Acta Math. Acad. Sci. Hung.*, **10** (1959), 21–29.
 158. On random graphs. I. (with P. Erdős). *Publ. Math. Debrecen*, **6** (1959), 290–297.
 159. On a theorem of P. Erdős and its application in information theory. *Mathematica, Cluj*, **1** (24) (1959), 341–344.
 160. On the dimension and entropy of probability distributions. *Acta Math. Acad. Sci. Hung.*, **10** (1959), 193–215.
 161. New version of the probabilistic generalization of the large sieve. *Acta Math. Acad. Sci. Hung.*, **10** (1959), 217–226.
 162. On the central limit theorem for samples from a finite population (with P. Erdős). *MTA Mat. Kut. Int. Közl.*, **4** (1959), 49–61.
 163. Some remarks on the theory of trees. *MTA Mat. Kut. Int. Közl.*, **4** (1959), 73–85.
 164. On Cantor's series with convergent $\sum 1/q_n$ (with P. Erdős). *Annales Univ. Sci. Budapest, Sect. Math.*, **2** (1959), 93–109.
 165. Autoklávok soros és párhuzamos kapcsolásáról és a keverés elméletéről (On serial and parallel coupling of autoclaves and on the theory of mixing). *MTA Mat. Kut. Int. Közl.*, **4** (1959), 155–165.
 166. On measures of dependence. *Acta Math. Acad. Sci. Hung.*, **10** (1959), 441–451.
 167. On connected graphs. I. *MTA Mat. Kut. Int. Közl.*, **4** (1959), 385–388.
 168. Summation methods and probability theory. *MTA Mat. Kut. Int. Közl.*, **4** (1959), 389–399.
 169. On the central limit theorem for the sum of a random number of independent random variables. *Acta Math. Acad. Sci. Hung.*, **11** (1960), 97–102.
 170. Additive properties of random sequences of positive integers (with P. Erdős). *Acta Arithm.*, **6** (1960), 83–110.
 171. Bolyongási problémákra vonatkozó határeloszlástételek (Limit theorems of random walks). *MTA III. Oszt. Közl.*, **10** (1960), 149–169.
 172. On the evolution of random graphs (with P. Erdős). *MTA Mat. Kut. Int. Közl.*, **5** (1960), 17–61.
 173. Probabilistic methods in number theory. *Proceedings of the International Congress of Mathematicians*, 14–21 August, 1958, Edinburgh. Cambridge University Press, London, 1960, 529–539.
 174. Az információelmélet néhány alapvető kérdése (Some fundamental questions of information theory). *MTA III. Oszt. Közl.*, **10** (1960), 251–282.
 175. Dimension, entropy and information. *Transactions of the Prague Conference on information theory, statistical decision functions, random processes*. Held at Libice near Prague, from June 1 to 6, 1959. Publ. House of the Czech. Acad. Sci., Prague, 1960; pp. 545–556.
 176. Bemerkungen zur Arbeit "Über gewisse Elementenfolgen des Hilbertischen Raumes" von K. Koncz. *MTA Mat. Kut. Int. Közl.*, **5** (1960), 265–267.
 177. Üzletek áruellátásával kapcsolatos szélsőértékfeladatok (On some inventory problems; with Margit Ziermann). *MTA Mat. Kut. Int. Közl.*, **5** (1960), 495–506.
 178. Turán Pál matematikai munkásságáról (On the mathematical work of Pál Turán). *Mat. Lapok*, **11** (1960), 229–263.
 179. On the evolution of random graphs (with P. Erdős). *Bull. Inst. Internat. Stat.*, **38** (1961), 4^e Livraison, 343–347.
 180. On measures of entropy and information. *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability*. Held at the Statistical Laboratory, University of California, June 20–July 30, 1960. Vol. 1. University of California Press, Berkeley-Los Angeles, 1961; pp. 547–561.
 181. Egy általános módszer valószínűségszámítási tételek bizonyítására és annak néhány alkalmazása (A general method for proving theorems in probability theory and some applications). *MTA III. Oszt. Közl.*, **11** (1961), 79–105.
 182. On random generating elements of a finite Boolean algebra. *Acta Sci. Math. Szeged*, **22** (1961), 75–81.
 183. On the strength of connectedness of a random graph (with P. Erdős). *Acta Math. Acad. Sci. Hung.*, **12** (1961), 262–267.
 184. On a classical problem of probability theory (with P. Erdős). *MTA Mat. Kut. Int. Közl.*, **6A** (1961), 215–220.
 185. On Kolmogoroff's inequality. *MTA Mat. Kut. Int. Közl.*, **6A** (1961), 411–415.

186. Legendre polynomials and probability theory. *Annales Univ. Sci. Budapest, Sect. Math.*, **3** - **4** (1960/61), 247-251.
187. Egy információelméleti problémáról (On a problem of information theory). *MTA Mat. Kut. Int. Közl.*, **6B** (1961), 505-516.
188. On random subsets of a finite set. *Mathematica, Cluj*, **3** (26) (1961), 355-362.
189. Über verschiedene Masszahlen von Entropie und Informationsgewinn (lecture at V. Österreichischer Mathematikerkongress, Innsbruck, 12-17. IX. 1960). Summary in *Nachr. Österr. Math. Ges. Beilage zu "Internat. Math. Nachr."*, **15** (1961) Jänner, Nr. 66, Sondernummer, 79-80.
190. On different measures of information (lecture at Második Magyar Matematikai Kongresszus, Budapest, 1960. augusztus 24-31). Summary in *Deuxième Congrès Mathématique Hongrois*, Budapest, 24-31. August, 1960, II. Akadémiai Kiadó, Budapest, 1961, 26-28.
191. Gondolatok a matematikus képzés továbbfejlesztéséről (Thoughts on developing the teaching of mathematics). *Magyar Tudomány*, **6** (1961), 593-600.
192. Statistical laws of accumulation of information. *Bull. Inst. Internat. Stat.*, **39** (1962), 2^e Livraison, 311-316.
193. Az információ-akkumuláció statisztikus törvényszerűségeiről (On statistical laws of accumulation of information). *MTA Mat. Kut. Int. Közl.*, **12** (1962), 15-33.
194. Egy megfigyeléssorozat kiemelkedő elemeiről (On the extreme elements of observations). *MTA III. Oszt. Közl.*, **12** (1962), 105-121.
195. Three new proofs and a generalization of a theorem of Irving Weiss. *MTA Mat. Kut. Int. Közl.*, **7A** (1962), 203-214.
196. Théorie des éléments saillants d'une suite d'observations. *Annales Fac. Sci. Univ. Clermont-Ferrand*, **2** (1962), No. 8, 7-12.
197. Dialógus a matematikáról (Dialogue on mathematics). *Valóság*, 1962, No. 3, 40-55.
198. On a problem of A. Zygmund (with P. Erdős). *Studies in mathematical analysis and related topics. Essays in honor of George Pólya*, Stanford University Press, Stanford, Cal., 1962, 110-116.
199. A new approach to the theory of Engel's series. *Annales Univ. Budapest, Sect. Math.*, **5** (1962), 25-32.
200. On the representation of an even number as the sum of a prime and of an almost prime. *American Mathematical Society. Translations. Series 2, Vol. 19.* American Mathematical Society, Providence, 1962, 299-321.
201. Egy gráfelméleti problémáról (On a problem in the theory of graphs; with P. Erdős). *MTA Mat. Kut. Int. Közl.*, **7B** (1962), 623-641.
202. A matematika alkalmazásairól tartandó vita tézisei (Theses of the discussion on the applications of mathematics). *Magyar Tudomány*, **7** (1962), 553-559.
203. On the theory of outstanding observations (lecture at International Congress of Mathematicians, Stockholm, 1962). Summary in *International Congress of Mathematicians. Abstracts of short communications.* Stockholm, 1962. Almqvist and Wiksells, Uppsala, 1962, 165-166.
204. Théorie des éléments saillants d'une suite d'observations. *Colloquium on Combinatorial Methods in Probability Theory.* August 1-10, 1962. Matematisk Institut, Aarhus Universitet, Danmark, 1962, 104-117.
205. *Wahrscheinlichkeitsrechnung, mit einem Anhang über Informationstheorie.* VEB Deutscher Verlag der Wissenschaften, Berlin, 1962.
206. *Sur les graphes aléatoires (I). L'évolution des graphes aléatoires. — Sur les graphes aléatoires (II). Symétrie et asymétrie des graphes aléatoires.* Institut H. Poincaré, Paris, 1962, 20 pp. (Mimeographed.)
207. Remarks on a problem of Obreanu (with P. Erdős). *Canadian Math. Bull.*, **6** (1963), 267-273.
208. Über die konvexe Hülle von n zufällig gewählten Punkten (with R. Sulanke). *Z. Wahrscheinlichkeitstheorie*, **2** (1963/64), 75-84.
209. On stable sequences of events. *Sankhya, Ser. A*, **25** (1963), 293-302.
210. On the distribution of values of additive number-theoretical functions. *Publ. Math. Debrecen*, **10** (1963), 264-273.
211. A study of sequences of equivalent events as special stable sequences (with P. Révész). *Publ. Math. Debrecen*, **10** (1963), 319-325.
212. On "small" coefficients of the power series of entire functions (with Kató Rényi). *Annales Univ. Budapest, Sect. Math.*, **6** (1963), 27-38.

213. On two problems of information theory (with P. Erdős). *MTA Mat. Kut. Int. Közl.*, **8A** (1963), 229–243.
214. On random matrices (with P. Erdős). *MTA Mat. Kut. Int. Közl.*, **8A** (1963), 455–461.
215. An elementary inequality between the probabilities of events (with P. Erdős and J. Neveu). *Math. Scand.*, **13** (1963), 99–104.
216. Asymmetric graphs (with P. Erdős). *Acta Math. Acad. Sci. Hung.* **14** (1963), 295–315.
217. Un dialogue. *Les cahiers rationalistes*, **33** (1963), janvier-février, Nos. 208–209, 4–32.
218. Blaise Pascal. 1623–1666. *Magyar Tudomány*, **8** (70) (1963), 102–108.
219. Megjegyzések egyes “megjegyzések”-hez (Remarks on certain “Remarks”) (to K. Tekse: Néhány megjegyzés Rényi A. “A matematika alkalmazásairól tartandó vita téziseiről” című cikkéhez [Some remarks on A. Rényi’s Theses of the discussion on the application of mathematics]. *Magyar Tudomány*, **8** (70) (1963), 46–50). *Magyar Tudomány*, **8** (1963), 419–429.
220. Über stabile Folgen von Ereignissen und Zufallsveränderlichen (lecture at Tagung über Mathematische Statistik und Wahrscheinlichkeitstheorie. Oberwolfach, 4–8. März, 1963). Summary in *Tagungsbericht. Mathematische Statistik und Wahrscheinlichkeitstheorie, Oberwolfach, 4–8. März, 1963*. Mathematisches Forschungsinstitut, Oberwolfach, 1963. (Mimeographed.)
221. Dialógus a matematikáról. (Részletek.) (Dialogue on mathematics; parts.) *A matematika tanítása*. Szemelvénygyűjtemény (ed. T. Varga). Tankönyvkiadó, Budapest, 1963, 381–415.
222. Dialógus a matematika tanításáról (Dialogue on the teaching of mathematics). *A matematika tanítása*. Szemelvénygyűjtemény (ed. T. Varga). Tankönyvkiadó, Budapest, 1963, 365–380.
223. Über die konvexe Hülle von n zufällig gewählten Punkten. II. (with R. Sulanke). *Zeitschr. Wahrscheinlichkeitstheorie*, **3** (1964/65), 138–147.
224. Információelmélet a nyelvészetben (Information theory in linguistics). *Általános nyelvészeti tanulmányok. II. A matematikai nyelvészet és a gépi fordítás kérdései*. Akadémiai Kiadó, Budapest, 1964, 245–251.
225. *Additive and multiplicative number-theoretical functions*. University of Michigan, Ann Arbor, 1964, 23 pp. (Mimeographed.)
226. *Dialógus a matematika alkalmazásairól* (Dialogue on the applications of mathematics). Az MTA Matematikai Kutatóintézete, Budapest, 1964, 20 pp. (Mimeographed.)
227. *A természet könyvének nyelve. Dialógus* (The language of the book of nature. Dialogue). Az MTA Matematikai Kutatóintézete, Budapest, 1964. (MS.)
228. On an extremal property of the Poisson process. *Annals Inst. Stat. Math. Tokyo*, **16** (1964), 129–133.
229. A generalization of a theorem of E. Vincze (with R. G. Laha and E. Lukács). *MTA Mat. Kut. Int. Közl.*, **9A** (1964), 237–239.
230. On two mathematical models of the traffic on a divided highway. *Jour. Appl. Prob.*, **1** (1964), 311–320.
231. On the amount of information concerning an unknown parameter in a sequence of observations. *MTA Mat. Kut. Int. Közl.*, **9A** (1964), 617–625.
232. Hervorragende Elemente von Beobachtungsreihen (lecture at Internationale Tagung über Mathematische Statistik und ihre Anwendungen, Berlin vom 8. September, 1962). Summary in *Abh. Deutsch. Akad. Wissensch. Berlin, Klasse Math. Phys. Technik*, 1964, No. 4, 101.
233. A Socratic dialogue on mathematics. *Canadian Math. Bull.*, **7** (1964), 441–462.
234. Mathematics. A Socratic dialogue. *Physics Today*, **17** (1964), December, 24–36.
235. A Socratic dialogue on mathematics. “Simon Stevin”, **38** (1963/64), 125–144.
236. On the amount of information in a frequency-count. *Bull. Inst. Internat. Stat.*, **41** (1964), 623–626.
237. Sur les espaces simples des probabilités conditionnelles. *Annales Inst. H. Poincaré, Nouvelle série, Sect. B*, **1** (1964), No. 1, 3–21.
238. A dialogue on the application of mathematics. *Ontario Mathematical Gazette*, **3** (1964), 28–40.
239. *Dialogue on the applications of mathematics*. University of Michigan, Ann Arbor, 1964. (Mimeographed.)
240. Discussion on Mr. Lewis’s paper (to P. A. W. Lewis: A branching Poisson process model for the analysis of computer failure patterns. *Jour. Roy. Stat. Soc., Series B*, **26** (1964), 398–456). *Jour. Roy. Soc., Series B*, **26** (1964), 445–446.

241. Eine Extremaleigenschaft des Poissonschen Processes (lecture at Tagung über Mathematische Statistik und Wahrscheinlichkeitstheorie, Oberwolfach, 2–7. August, 1964). Summary in *Tagungsbericht. Mathematische Statistik und Wahrscheinlichkeitstheorie, Oberwolfach, 2–7. August, 1964*. Mathematisches Forschungsinstitut, Oberwolfach, 1964. (Mimeographed.)
242. On the foundations of information theory. *Rev. Inst. Internat. Stat.*, **33** (1965), 1–14.
243. Probabilistic methods in group theory (with P. Erdős). *Jour. Analyse Mathématique*, **14** (1965), 127–138.
244. Some remarks on periodic entire functions (with Kató Rényi). *Jour. Analyse Mathématique*, **14** (1965), 303–310.
245. On some problems in the theory of order statistics. 36th Session of the ISI, Sydney, 1965, 17 pp. (Mimeographed.)
246. On some problems in the theory of order statistics. *Bull. Inst. Internat. Stat.*, **43** (1965), 165–176.
247. On certain representations of real numbers and on sequences of equivalent events. *Acta Sci. Math. Szeged*, **26** (1965), 63–74.
248. *Dialogusok a matematikáról* (Dialogues on mathematics). Akadémiai Kiadó, Budapest, 1965.
249. On the theory of random search. *Bull. Amer. Math. Soc.*, **71** (1965), 809–828.
250. On the mean value of nonnegative multiplicative number-theoretical functions (with P. Erdős). *Michigan Math. Jour.*, **12** (1965), 321–338.
251. A new proof of a theorem of Delange. *Publ. Math. Debrecen*, **12** (1965), 323–329.
252. *The language of the Great Book of Nature*. Az MTA Matematikai Kutatóintézete, Budapest, 1965, 39 pp. (Mimeographed.)
253. A természet könyvének nyelve (The language of the book of nature). *Fizikai Szemle*, **15** (1965), 129–138.
254. A Matemática — Um Diálogo Socrático. *Gazeta de Matemática*, 1965, No. 100, Julho-Dezembro, 59–71.
255. On the amount of information concerning an unknown parameter in a sequence of observations. Lectures to the Fifth Summer Research Institute of the Australian Mathematical Society. Preprint. Australian Mathematical Society, 1965, 1–3.
256. On the theory of random search. Lectures to the Fifth Summer Research Institute of the Australian Mathematical Society. Preprint. Australian Mathematical Society, 1965, 14–16.
257. On an extremal property of the Poisson process. Lectures to the Fifth Summer Research Institute of the Australian Mathematical Society. Preprint. Australian Mathematical Society, 1965, 17–20.
258. *Véges geometriák kombinatorikai alkalmazásai. I.* (Combinatorial analysis of finite geometries. I.). Az MTA Matematikai Kutatóintézete, Budapest, 1965, 67 pp. (Mimeographed.)
259. *Új módszerek és eredmények a kombinatorikus analízisben. I.* (New methods and results in combinatorial analysis. I.). Az MTA Matematikai Kutatóintézete, Budapest, 1965, 89 pp. (Mimeographed.)
260. On a problem of graph theory (with P. Erdős and Vera T. Sós). *Studia Sci. Math. Hung.*, **1** (1966), 215–235.
261. *Véges geometriák kombinatorikai alkalmazása. I.* (Combinatorial analysis of finite geometries. I.). *Mat. Lapok*, **17** (1966), 33–76.
262. *Probability theory. Lecture notes*. Stanford University, Stanford, 1966, 110 pp.
263. On the existence of a factor of degree one of a connected random graph (with P. Erdős). *Acta Math. Acad. Sci. Hung.*, **17** (1966), 359–368.
264. *Új módszerek és eredmények a kombinatorikus analízisben. I.* (New methods and results in combinatorial analysis. I.). *MTA III. Osz. Közl.*, **16** (1966), 77–105.
265. On the amount of missing information and the Neyman–Pearson lemma. *Research papers in statistics*. Festschrift for J. Neyman. Wiley, London, 1966, 281–288.
266. On the amount of information in a random variable concerning an event. *Jour. Math. Sci. Delhi*, **1** (1966), 30–33.
267. *Statistics based on information theory*. European Meeting of Statisticians, London, 1966, 17 pp. (Mimeographed.)
268. *Mathematics. A Socratic dialogue* (a mimeographed form of A. Rényi's Mathematics. A Socratic dialogue. Physics Today, 17 (1964), December, 24–36). Mathematics Department of Ohio University, 1966, 16 pp.
269. Sokratischer Dialog. *Neue Sammlung*, **6**. (1966), 284–304.
270. A dialogue on the applications of mathematics. “Simon Stevin”, **39** (1965/66), 3–17.

271. Új módszerek és eredmények a kombinatorikus analízisben. II. (New methods and results in combinatorial analysis. II.). *MTA III. Oszt. Közl.*, **16** (1966), 159–177.
272. Levelek a valószínűségről (Letters on probability). *Fizikai Szemle*, **16** (1966), 278–288.
273. A Matematikai Kutató Intézet 10 éve (Ten years of the Mathematical Institute). *Magyar Tudomány*, **11** (73) (1966), 81–91.
274. *Valószínűesszámtás* (Probability theory). Tankönyvkiadó, Budapest, 1966.
275. *Wahrscheinlichkeitsrechnung, mit einem Anhang über Informationstheorie*. 2., berichtigte Auflage. VEB Deutscher Verlag der Wissenschaften, Berlin, 1966.
276. *Calcul des probabilités. Avec un appendice sur la théorie de l'information*. Dunod, Paris, 1966.
277. *Dialogusok a matematikáról*. 2. kiadás (Dialogues on mathematics; 2nd edition). Akadémiai Kiadó, Budapest, 1966.
278. *Valószínűesszámtási módszerek az analízisben* (Probabilistic methods in analysis). Az MTA Matematikai Kutatóintézete, Budapest, 1966, 65 pp. (Mimeographed.)
279. Eine Ungleichung zwischen der Irrtumswahrscheinlichkeit und der fehlenden Information. (Lecture at Tagung über Mathematische Statistik und Wahrscheinlichkeitstheorie. Oberwolfach, 17–24. April, 1966). Summary in *Tagungsbericht. Mathematische Statistik und Wahrscheinlichkeitstheorie*. Oberwolfach, 17–24. April, 1966. Mathematisches Forschungsinstitut, Oberwolfach, 1966. (Mimeographed.)
280. *On the mathematical theory of trees*. "Rouse Ball" lectures, Cambridge, 1966. (MS.)
281. *Levelek a valószínűségről* (Letters on probability). Akadémiai Kiadó, Budapest, 1967.
282. *Valószínűesszámtási módszerek az analízisben*. I. (Probabilistic methods in analysis. I.). *Mat. Lapok*, **18** (1967), 5–35.
283. *Valószínűesszámtási módszerek az analízisben*. II. (Probabilistic methods in analysis. II.). *Mat. Lapok*, **18** (1967), 175–194.
284. Remarks on the Poisson process. *Studia Sci. Math. Hung.*, **2** (1967), 119–123.
285. Statistics and information theory. *Studia Sci. Math. Hung.*, **2** (1967), 249–256.
286. On the height of trees (with Gy. Szekeres). *Jour. Australian Math. Soc.*, **7** (1967), 497–507.
287. Remarks on the Poisson process. *Symposium on probability methods in analysis*. Lectures delivered at a symposium at Loutraki, Greece, 22. 5–4. 6, 1966. Lecture Notes in Mathematics. 31. Springer, Berlin, 1967, 280–286.
288. On some basic problems of statistics from the point of view of information theory. *Proceedings of the Fifth Berkeley symposium on mathematical statistics and probability*. Held at the Statistical Laboratory, University of California, June 21–July 18, 1965 and December 27, 1965–January 7, 1966. Vol. I. University of California Press, Berkeley and Los Angeles, 1967, 531–543.
289. Játék és matematika (I) (Games and mathematics, I). *Természettudományi Közlöny*, **11** (98) (1967), 61–63.
290. Játék és matematika (II) (Games and mathematics, II). *Természettudományi Közlöny*, **11** (98) (1967), 116–119.
291. Játék és matematika (III) (Games and mathematics, III). *Természettudományi Közlöny*, **11** (98) (1967), 211–213.
292. "Az ember gúnnyal – tudjuk – arra támad, amit meg nem ért!" ("Wir sind gewohnt, dass die Menschen verhöhnen, was sie nicht verstehen, . . . ; Goethe: Faust). (A televízióban elhangzott "Játék és matematika" c. sorozat befejező része [Last part of a lecture series given in the television on "Games and mathematics"].) *Természettudományi Közlöny*, **11** (98) (1967), 296–298.
293. *Dialogues on mathematics*. Holden-Day, Inc., San Francisco, 1967.
294. *Dialoge über Mathematik*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1967.
295. *Dialoge über Mathematik*. Birkhäuser, Basel, 1967.
296. Probabilistic methods in combinatorial mathematics (lecture at Symposium on combinatorial mathematics, Chapel Hill, 1967). Mimeographed text: *Symposium on combinatorial mathematics*, Chapel Hill. University of North Carolina, Monographs series, 1967, 13 pp.
297. Probabilistic methods in combinatorial mathematics. *Combinatorial mathematics and its applications*. Proceedings of the Conference held at the University of North Carolina at Chapel Hill, April 10–14, 1967, 13 pp.
298. *Letters on probability*. 4th letter. Az MTA Matematikai Kutatóintézete, Budapest, 1967, 18 pp. (Mimeographed.)
299. *Dialoguri despre matematică*. Editura Științifică, București, 1967.

300. Kerekasztal-konferencia szovjet matematikusokkal a matematika elvi kérdéseiről (Round-table conference on the fundamental problems of mathematics with mathematicians from the Soviet Union). *Mat. Lapok*, 19 (1968), 3–8.
301. A rendezett minták elméletének egy problémaköréről (On some problems in the theory of order statistics). *MTA III. Ösz. Közl.*, 18 (1968), 23–30.
302. Zufällige konvexe Polygone in einem Ringgebiet (with R. Sulanke). *Zeitschr. Wahrscheinlichkeitstheorie*, 9 (1968), 146–157.
303. On quadratic inequalities in the theory of probability (with J. Galambos). *Studia Sci. Math. Hung.*, 3 (1968), 351–358.
304. On random matrices. II. (with P. Erdős). *Studia Sci. Math. Hung.*, 3 (1968), 459–464.
305. Information and statistics. *Studies in mathematical statistics*. Theory and applications. Akadémiai Kiadó, Budapest, 1968, 129–131.
306. Sur la théorie de la recherche aléatoire. *Colloques internationaux du Centre National de la Recherche Scientifique*. No. 165. Programmation en mathématiques numériques. Besançon, 7–14 Septembre, 1966. Éditions du Centre National de la Recherche Scientifique, Paris, 1968, 281–287.
307. On the distribution of numbers prime to n . *Abhandlungen aus Zahlentheorie und Analysis*. Zur Erinnerung an Edmund Landau (1877–1938). VEB Deutscher Verlag der Wissenschaften, Berlin, 1968, 269–278.
308. On the distribution of numbers prime to n . *Number theory and Analysis*, a Collection of Papers in Honor of Edmund Landau (1877–1938). Plenum Press, New York, 1968, 269–278.
309. Vázlatok egy Fibonacci-témára (Variations to a Fibonacci theme). *Természet Világa*, 1968, 22–27.
310. Vázlatok egy Fibonacci-témára. II. (Variations to a Fibonacci theme. II.). *Természet Világa*, 1968, 87–90.
311. *Ars Mathematica*. *Fizikai Szemle*, 18 (1968), 60–61.
312. *Ars Mathematica*. *Élet és Tudomány*, 14 (1968), 654–655.
313. *Valószínűségszámítás* (Probability theory). Második kiadás (2nd edition). Tankönyvkiadó, Budapest, 1968.
314. Die Sprache des Buches der Natur. *Neue Sammlung*, 8 (1968), 117–123.
315. Some remarks on the large sieve of Yu. V. Linnik (with P. Erdős). *Annales Univ. Sci. Budapest, Sect. Math.*, 11 (1968), 3–13.
316. On some problems of statistics from the point of view of information theory (lecture at Információelméleti Kollokvium. Kossuth Lajos Tudományegyetem, Debrecen, 1967, szeptember 19–24). *Summary in Információelméleti Kollokvium. Kossuth Lajos Tudományegyetem, Debrecen, 1967. szeptember 19–24. Előadáskivonatok*. Bolyai János Matematikai Társulat, Budapest, 1968, 87–90.
317. Stochastische Prozesse in der Biologie (lecture at A Nemzetközi Biometria Társaság Magyar Csoportjának Biometria Konferenciája. Magyar Tudományos Akadémia, Budapest, 1968. március 19–22.). *Summary in A Nemzetközi Biometria Társaság Magyar Csoportjának Biometria Konferenciája. Magyar Tudományos Akadémia, Budapest, 1968. március 19–22. Előadáskivonatok. Az MTA Biológiai Tudományok Osztálya, Budapest, 1968, 50 pp.*
318. On random entire functions (with P. Erdős). *Zastosowania Matematyki*, 10 (1969), 47–55.
319. Measures in denumerable spaces (with A. Hanisch and W. M. Hirsch). *American Math. Monthly*, 76 (1969), 494–502.
320. *Lectures on the theory of search*. Department of Statistics. University of North Carolina at Chapel Hill. Institute of Statistics, Mimeo Series, No. 600. 7 May, 1969, 78 pp.
321. A szerencsejátékok és a valószínűségszámítás (Gambling and the theory of probability). *Matematikai érdekességek*. Gondolat, Budapest, 1969, 197–220.
322. A Barkochba játék és az információelmélet (The Barkochba game and information theory). *Matematikai érdekességek*. Gondolat, Budapest, 1969, 269–286.
323. *Dialógusok a matematikáról* (Dialogues on mathematics). 3. kiadás (3rd edition). Akadémiai Kiadó, Budapest, 1969.
324. *Диалоги о математике*. Мир, Москва, 1969.
325. *Briefe über die Wahrscheinlichkeit*. Akadémiai Kiadó, Budapest, 1969.
326. *Briefe über die Wahrscheinlichkeit*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1969.
327. *Briefe über die Wahrscheinlichkeit*. Birkhäuser, Basel, 1969.
328. On some problems of statistics from the point of view of information theory. *Proceedings of the Colloquium on Information Theory*, organized by the Bolyai Mathematical

- Society, Debrecen (Hungary), 1967. Bolyai János Matematikai Társulat, Budapest, 1969, 343–357.
329. Lezioni sulla probabilità e l'informazione. *Lezioni e conferenze*. Università di Trieste, Istituto di Meccanica. Trieste, 1969.
 330. Remarks on the teaching of probability. *1st CSMP International Conference on the Teaching of Probability and Statistics at the Pre-College Level*. — Sponsored by Southern Illinois University, March 17–27, 1969. Carbondale, 1969. (Mimeographed.)
 331. *On Cayley's polynomials for counting trees*. International Conference on Combinatorial Structures and their Applications, Calgary, 1969. (Mimeographed.)
 332. On the enumeration of trees. *Proceedings of the Calgary International Conference on Combinatorial Structures and their Applications*. Calgary, 1969. (Mimeographed.)
 333. *Gondolatok a valószínűségszámítás tanításáról* (Remarks on the teaching of probability). Az MTA Matematikai Kutatóintézete, Budapest, 1969. (Mimeographed.)
 334. *Mathematical models of biological processes* (a lecture). Kingston, 1969. (MS.)
 335. Application of probability theory to other areas of mathematics. Lectures held at the 12th Biennial International Seminar of the Canadian Mathematical Congress at Vancouver, August, 1969. Preprint. Canadian Mathematical Society, Vancouver, 1969.
 336. *Gondolatok a valószínűségszámítás tanításáról* (Remarks on the teaching of probability). *Mat. Lapok*, 21 (1970).
 337. *Valószínűségszámítási feladatgyűjtemény* (Mathematical exercises in probability theory; with collaborators). Tankönyvkiadó, Budapest, 1970.
 338. *Probability theory*. Akadémiai Kiadó, Budapest – North-Holland Publishing Co., Amsterdam, 1970.
 339. *Foundations of probability*. Holden-Day, Inc., San Francisco, 1970.
 340. *On the mathematical theory of trees*. North-Holland Publishing Co., Amsterdam, 1970.
 341. *Stochastische Prozesse in der Biologie*. Vorträge der II. Ungarischen Biometrischen Konferenz (Budapest, von 19. bis 22. März, 1968). Akadémiai Kiadó, Budapest, 1970, 27–33.
 342. On a new law of large numbers (with P. Erdős). *Jour. Analyse Mathématique*, 22 (1970), 103–111.
 343. The Prüfer code for k -trees (with Kató Rényi). *Combinatorial theory and its applications III*. Bolyai János Matematikai Társulat, Budapest – North-Holland Publishing Co., Amsterdam – London, 1970, 945–971.
 344. On the enumeration of search-codes. *Acta Math. Acad. Sci. Hung.*, 21 (1970), 27–33.
 345. *Probability theory* (in Czech). Praha, 1970.
 346. *Uniform flow in cascade graphs*. (edited by M. Behara Springer, Berlin, 1970.
 347. On the number of endpoints of a k -tree. *Studia Sci.)Math. Hung.*, 5 (1970), 5–10.
 348. *Naplójegyzetek az információelméletről* (Notes on the theory of information). 1970. (MS.)
 349. *Dialogusok a matematikáról*. 3. rész (Dialogues on mathematics; 3rd part; in Italian). Sapere, 1970.
 350. Application of probability theory to other areas of mathematics. Publication of the 12th Biennial International Seminar of the Canadian Mathematical Congress (Vancouver, 1969). Vancouver, 1970.
 351. *Ars Mathematica* (in English). (in press) Akadémiai Kiadó
 352. *Napló az információelméletről* (Diary on the theory of information). *Fizikai Szemle*, 20 (1970), 161–172.
 353. Remarks on the teaching of probability. *The teaching of probability and statistics*. Proceedings of First CSMP International Conference on Teaching of Mathematics at the Pre-college Level. Jointly sponsored by Southern Illinois University and CEMREL. March, 1969. (Edited by Lenmart Råde.) John Wiley, Inc., New York, 1969, 273–281.
 354. *Письма о вероятности*. Мир, Москва, 1971.
 355. A sztochasztikus gejzír (The stochastic geyser). *MTA Mat. Kut. Int. Közl.* 7 (1962), 643

SELECTED PAPERS

1962 – 1970

ON STATISTICAL LAWS OF ACCUMULATION
OF INFORMATION

A. RÉNYI

INTRODUCTION

It often happens both in scientific research and in our everyday life that we receive some information on a subject (interesting us) not at once but bit by bit; the whole picture is reconstructed from small details, like a mosaic from its pieces. So, *the complete information is the result of the accumulation of partial informations*. During such a procedure of collecting information the new information is often partly contained by the earlier ones. In other words, generally, a “redundance” of information can be observed in an information accumulating process. This redundancy could be eliminated in the vast majority of the cases only by collecting the information according to a very careful and thorough plan, which would complicate the whole procedure so much that it would not be worth using it.

The process of information collection generally contains some random features, as well. E.g. the order of the partial data received is often casual.¹

To illustrate this let us consider the following examples. First we take the problem of qualitative chemical analysis. We would like to determine the components of some chemical compound. Therefore we submit it to different tests. Each test narrows the set of possibilities, and finally, after having tested the compound sufficiently many times there remains only one possibility. The bits of information received from different tests will be partly overlapping. The order of tests influences how fast can the compound be identified. Of course, if we have a beforehand hypothesis, that can facilitate the analysis. However, we are interested in the question where we know nothing about the compound beforehand and hence the order of tests is random to a certain extent.

A similar situation is faced by a doctor when he wishes to diagnose an illness. He examines the patient in various ways, then compares the results and on this basis he decides the diagnosis. Of course, the intuition and experience of the doctor are important in this case, they help to reduce the number of possibilities he has to take into consideration. However, the intuition and experience can be counted in this case as a beforehand information the source of which can be the complaints of the patient, the doctor's impressions and also his knowledge due to an earlier treatment of the patient; anyway, the information-collection starts not with the laboratory tests but in the very moment the doctor meets the patient first. (Therefore, the laboratory tests are quite

¹ In reality the situation is even more complicated, since the received information is often faulty, thus e.g. it can be influenced by random misprints or misunderstandings. In information theory we would say in this case that the information is transmitted by a noisy channel. Though the elimination of the faulty information — e.g. by finding contradictions — is often the most difficult part of data processing, this point of view will be neglected here; we return to it another time.

often unnecessary.) For us the important feature of this example is that the doctor diagnoses on the basis of a great many bits of information. Which bits of information and in which order are obtained by the doctor that is very casual. (For example, the patient can forget to mention some symptoms *at random* when listing his complaints just because they do not disturb him too much and he does not attribute significance to them.)

Our third example is the work of a judge, trying to detect the truth in a dispute at law. He tries to reconstruct the facts from the testimony of the witnesses. The testimony of the witnesses concerns mostly only a small part of the case and at the same time, they are often overlapping.² The task of the judge is to find a certain person in a set H of persons who has committed a certain crime. Again, it can be fairly random, who will be the witnesses and in which order they will be questioned. (For example, it can happen that some of the summoned witnesses can come only later or not at all.)

A further example is the so-called Bar—Kochba game which is such an oversimplified case of the situations interesting us, that it yields also the mathematical model of them immediately. Namely, the mathematical problem we are interested in occurs almost in "laboratory" purity in this game. The game Bar—Kochba is played by two participants; let us call them A and B . A thinks of something and B must guess what it is by putting questions.³ The rules of the game have no restriction on what A can think of: it can be a certain person, an object, and abstract notion, and so on. B must ask only such questions which can be answered by "yes" or "no" and A must answer them according to his best knowledge. A is allowed not to answer only if the question cannot be answered or he does not know the answer.⁴

In the Bar—Kochba game a good player generally asks according to a certain system, the questions, however, and their order is strongly influenced by random factors, while in the case of an inexperienced player they can be considered entirely casual.

The following modification of the Bar—Kochba game, which could be called "*multivalued Bar—Kochba game*" is also worth mentioning. This differs from the usual one in that the answers for the questions can be not only "yes" and "no": the number of possible answers can also be more than two. In this case B asks a question and lists the answers he means possible and A must tell, which one is right (it is supposed that only one of the answers can be correct). It is advisable to limit the number of alternatives in the case of the "multivalued Bar—Kochba game" (e.g. to allow at most 3 or 4 alternatives).

In order to obtain a mathematically suitable, simplified model of our problem from the Bar—Kochba game we have only to fix the set of things A can think of. This means that we fix a finite set H even before starting the game and A must choose an element of it. The finiteness of H — if the number of elements is not limited — practically means no restriction. (One reasonable restriction

² As we have mentioned, we shall neglect the fact that the witnesses, sometimes willingly, sometimes by mistake misinform the judge. Of course, this cannot be neglected in the real life.

³ The player A is often replaced by a group of people thinking of the same thing and answering the questions of B alternatively. Now this is irrelevant.

⁴ The faulty informations (which we generally disregard to simplify the mathematical model) are prohibited by the rules of the game.

is e.g. that A is allowed to think of an entry of an encyclopaedia, or, say, it can be defined using at most five words of a dictionary, and so on.)

In this case each question is equivalent to a subset H' of H , i.e. instead of asking a question we can ask whether the selected element belongs to H' or not.

Now, one can easily describe a theoretically optimal strategy, which, however from other points of view should not be played. Namely, if n is the number of elements in H and $2^{s-1} < n \leq 2^s$ ($s = 1, 2, \dots$) and the elements of H are enumerated by $0, 1, \dots, n-1$ (by both players in the same way), then it is enough to guess the index of the element. In other words, we can suppose that H is the set of the integers $0, 1, \dots, n-1$ and B would like to find the integer selected by A . Now, these integers have at most s digits in binary form and therefore B can always identify the selected integer by the following s questions: "Writing the index of the thing you have chosen in binary form, is its j th digit zero? ($j = 1, 2, \dots, s$)."

Hence the selected element of the n -element set H can always be found in $s = \{\log_2 n\}$ steps; here $\{x\}$ denotes the least integer not smaller than x . To show that fewer questions are not enough we argue in the following way. If B can ask only questions with answers "yes" or "no", then each question can be characterized by the set of the elements for which the answer is affirmative. Now, if $f(n)$ denotes the minimum number of questions needed to find an element of a set of n elements, then $f(n)$ is a non-decreasing function and if the set corresponding to the first question has m elements, then we need either $f(m)$ or $f(n-m)$ further question depending on whether the answer for the first question is affirmative or not. Therefore,

$$f(n) \geq 1 + \min_{0 \leq m \leq n} [\max(f(m), f(n-m))].$$

Hence

$$f(n) \geq 1 + f\left(\left\lfloor \frac{n}{2} \right\rfloor\right).$$

Now, from $2^{s-1} < n \leq 2^s$ it follows that $\left\lfloor \frac{n}{2} \right\rfloor > 2^{s-2}$. Repeating the argument above $(s-1)$ times we get

$$f(n) \geq s-1 + f(2)$$

and, obviously, $f(2) = 1$; therefore

$$f(n) \geq s.$$

As we have seen, s questions are enough, thus $f(n) = s$ if $2^{s-1} < n \leq 2^s$.

It can similarly be proven that in the case of the "multivalued Bar-Kochba game" the minimum number of questions needed to identify an element is $\left\lceil \frac{\log_2 n}{\log_2 r} \right\rceil$ if r is the maximum number of possible answers for a question.

Further, an optimal system of questions is the following: written the index of the selected element in r -ary form is its j th digit i ($j = 1, 2, \dots; i = 0, 1, \dots, r-1$)?

We can see that if r different answers can be given for each question then we can suppose without loss of generality that n , the number of elements

in H , is a power of r . Indeed, if $r^{s-1} < n \leq r^s$, we lose nothing adding $r^s - n$ new elements to H . Hence, let us suppose that $n = r^s$. Now, the system of questions given above is optimal by two reasons: a) the information given by an answer is completely new, there is no redundancy, since the j th digit of the index can equally be any integer from 0 to $r - 1$, independently of other digits; b) according to the theory of information a question, which can be answered in r ways contains at most $\log_2 r$ "bits" of information and using the system of questions given above we really receive this amount of information for each question. Indeed, writing the numbers $0, 1, \dots, r^s - 1$ in r -ary scale we shall have exactly r^{s-1} numbers with j th digit i ($j = 1, \dots, s$; $i = 0, 1, \dots, r - 1$). Hence, if A selects any of the numbers $0, 1, 2, \dots, r^s - 1$ with the same probability (what can be supposed, since we have no prior information on the number selected), then on the question, whether the j th digit of the selected number (in r -ary scale) is i or not we receive affirmative answer with probability $\frac{1}{r}$.

Therefore the information contained in each answer is $\log_2 r$, s answers yield $s \log_2 r = \log_2 n$ information and this is just the information needed to characterize the elements of an n -element set.

Here let us notice that the optimal system of questions mentioned above has the following property: It does not matter at all, whether the questions are asked simultaneously, or one by one. This is interesting because in playing the actual Bar-Kochba game we ask a question only having received the answer for the previous one and this seems to be advantageous, that is, one would worth selecting a question dependently on the answers received earlier; nevertheless, the advantage is a mere illusion, since in the case of the optimal system of questions they were completely independent from the answers and therefore could have been asked at once. (For example, if $r = 2$, the first question is, whether the selected number is even or odd and the second one is, whether the half of the difference of this number and its residue mod 2 is even or odd.) Now, knowing the answer for the first question we can ask "Is the half of the number even?" or "Denoting the number by x , is $\frac{x-1}{2}$ even or odd?" depending on the answer. However, this changes nothing but the formulation of the second question.

In other words, it is all the same whether we sum up the information received after each answer or only after having received all the answers.

An optimal system of questions for $r = 2$ and $n = 2^s$ can be characterized as follows. If $H_1, \dots, H_s$ are the sets corresponding to the questions, i.e. the j th question decides whether the selected element of H belongs to H_j or not, and $\bar{H}_j = H - H_j$, then each H_j and $\bar{H}_j$ has 2^{s-1} elements, further each intersection $H_i H_j, H_i \bar{H}_j, \bar{H}_i H_j, \bar{H}_i \bar{H}_j$ has 2^{s-2} elements and, in general, if $\tilde{H}_j$ denotes one of H_j and $\bar{H}_j$, then the intersection $\tilde{H}_{j_1} \tilde{H}_{j_2} \dots \tilde{H}_{j_k}$ has 2^{s-k} elements for any $j_1 < j_2 < \dots < j_k$. In particular, each set of form $\tilde{H}_{j_1} \tilde{H}_{j_2} \dots \tilde{H}_{j_s}$ has exactly one element, further, different ones contain different elements. Hence there exists a one to one correspondence between the 2^s sets of this form and the 2^s elements. It is also easily seen that each one to one correspondence between the elements of H and the set of expressions of form $\tilde{H}_{j_1} \tilde{H}_{j_2} \dots \tilde{H}_{j_s}$ induces an optimal system of questions. Thus the number of optimal systems is 2^s !

However, in playing the actual Bar—Kochba game, our optimal system of questions cannot be utilized, except, if the number of elements of H is very small. One reason for this is that it would be very tiresome a task to enumerate the objects for a large n , to keep the indices in mind and, even, if we could manage this, the game would become uninteresting. Therefore, it would be interesting to know, how many more questions are needed if we do not apply the optimal strategy. This problem will be answered under the extreme assumption that we do not apply any strategy at all, that is, our answers are chosen entirely at random. We shall obtain the following surprising result: chosen the questions at random the number of questions is almost never essentially greater than in the optimal case. Thus, for example, for an arbitrary (sufficiently large) n in 99 per cent of the cases we need at most 7 extra questions. In § 1 we shall investigate the model of the ordinary Bar—Kochba game, while in § 2, the model of the multivalued Bar—Kochba game.

We shall also consider the more general case, when the different answers for the questions have different probabilities. If each question has r answers and the probability distribution of the answers is $\mathcal{P} = (p_1, \dots, p_r)$ then, according to the Shannon formula the information yielded by an answer is

$$I_1(\mathcal{P}) = \sum_{i=1}^r p_i \log_2 \frac{1}{p_i} \text{ and, therefore, we expect that at least } \{\log_2 n / I_1(\mathcal{P})\}$$

questions should be asked. We shall calculate the number of extra questions needed when the questions are chosen at random for this case as well.

In §§ 3—4 we shall investigate a problem which could be called the problem of “simultaneous Bar—Kochba game”. In this game the player A is replaced by many players denoted by $A_1, \dots, A_l$ each of which thinks of one element of H , different players select different elements. B asks questions and each A_i answers the same questions according to the element selected by him; B must find the element selected by A_i for each $i = 1, 2, \dots, l$. Here again, we have two variants, the ordinary simultaneous and the multivalued simultaneous Bar—Kochba game, according to the number of the answers for a question. It is an essential difference from mathematical point of view, whether l is fixed when n tends to infinity, or l can also be very large, say $l = n$. Thus e.g., if $l = n$, each player A_i selected an element of H , thus B must find, as a matter of fact, an unknown permutation of H . In general, the player B must find a function which maps one finite set (the set of the players) into another finite set (namely, into H). In the case $l = n$ that is, when each element is chosen by somebody, A should ask questions concerning all the elements.⁵ Since a question having r possible answers corresponds to a partitioning of H into r subsets, B will be able to guess all the elements the players thought of exactly when the partitions corresponding to his questions separate each pair of elements of H , that is, when no two elements of H belong to the same class at each partition.⁶

⁵ The optimal system of questions given for the ordinary Bar—Kochba game is also optimal for the simultaneous one; however, if we ask the questions at random the ordinary and simultaneous Bar—Kochba games will differ essentially from each other: in the second case, if $l = n$, we need approximately twice as many questions than in the first case, i.e., when $l = 1$.

⁶ For the sake of brevity we shall use the following terminology: if the partial informations correspond to cutting H into two parts, we shall say that the information is obtained from *dichotomies* (dichotomy = cutting into two parts); if there are allowed more than two classes, we shall speak about *general classifications*.

In this way the problem of the simultaneous Bar—Kochba game is essentially equivalent to the following one: The books of a library are classified according to different points of view; under which conditions will these different classifications together characterize each book of the library? Or, let us consider the example of the qualitative chemical analysis. This example, already mentioned above can be modified so that it will correspond to the simultaneous Bar—Kochba game. Namely, if we would like to identify not one but many chemical compounds at the same time, using the same tests, then we submit them to these tests, register the results which give a classification of all the possible chemical compounds. Now, the problem is, how should we plan a sequence of tests so that we could determine the chemical structure of all the samples we have. Similar problems arise in connection with the I.Q. tests as well.

An interesting feature of these problems is that instead of $I_1(\mathcal{S}) = \sum_{i=1}^p p_i \log_2 \frac{1}{p_i}$, the Shannon entropy of the probability distribution $\mathcal{S}(p_1, \dots, p_r)$, another measure of information plays a role in their solution, namely $I_2(\mathcal{S}) = -\log_2 \sum_{i=1}^r p_i^2$, the so-called *information measure of order 2*. This $I_2(\mathcal{S})$ is a special case of measures of information introduced by the author in [1] and [2]. In these papers the measure of information of order α of the probability distribution $\mathcal{S} = (p_1, \dots, p_r)$ is defined as follows: Let $\alpha > 0$ and $\alpha \neq 1$; then

$$I_\alpha(\mathcal{S}) = \frac{1}{1-\alpha} \log_2 \left(\sum_{i=1}^r p_i^\alpha \right).$$

It is also remarked that if $\alpha \rightarrow 1$, then $I_\alpha(\mathcal{S})$ tends to $I_1(\mathcal{S}) = \sum_{i=1}^r p_i \log_2 \frac{1}{p_i}$. Thus the Shannon entropy can also be considered as measure of information of order α for $\alpha = 1$.

Here we remark that the case $r = 2$, $p_1 = p_2 = \frac{1}{2}$ was investigated by the author in [3] and [4]. In [3] the problem was formulated in the terminology of Boolean algebras. The problem of the multivalued simultaneous Bar—Kochba game can be translated into this language as follows: under which conditions do the partitions (corresponding to the questions of B) generate the Boolean algebra of all the subsets of H with respect to the set-theoretical operations?

The results of the paper were also given in my lectures at a seminar at the Michigan State University. From the participants of the seminar Professor H. Rubin joined in the investigation of these problems. I would like to thank him for his valuable and inspiring remarks. Another participant of the seminar, J. Fox, suggested the following modification of the ordinary simultaneous Bar—Kochba game: it is allowed to ask only questions giving some new information for *each* element not identified by the previous questions. In other words: each set of at least two elements of the Boolean algebra generated by the first $j-1$ questions must be split into two non-empty subsets by the j th question. H. Rubin has proved interesting results in connection with this modified version of the problem.

§ 1. ACCUMULATION OF INFORMATION IN CASE OF DICHOTOMIES CONCERNING ONE UNKNOWN ELEMENT

First we shall solve the following problem:

Let H be an n -element set. Let us choose k subsets of H at random so that each subset of H (including the empty set and H itself, as well) be selected with the same probability, i.e., with probability $\frac{1}{2^n}$.⁷ The sets will be denoted by

$H_1, \dots, H_k$. What is the probability P_{nk} that a fixed element $x \in H$ is determined by knowing which H_j 's contain it and which do not. We are also interested in the question, how large k must be to assure that $P_{nk} > \alpha$, where $0 < \alpha < 1$ is given.

Let us denote the elements of H by $x_1, \dots, x_n$ and let

$$(1.1) \quad \varepsilon_{jh} = \begin{cases} 1 & \text{if } x_h \in H_j \\ 0 & \text{if } x_h \notin H_j \end{cases} \quad (j = 1, 2, \dots, k; h = 1, 2, \dots, n).$$

According to our assumption, H_j will be a given subset of H with probability $\frac{1}{2^n}$. Since H has 2^{n-1} subsets containing x_h and also 2^{n-1} subsets not containing it,

$$(1.2) \quad \mathbf{P}(\varepsilon_{jh} = 1) = \mathbf{P}(\varepsilon_{jh} = 0) = \frac{2^{n-1}}{2^n} = \frac{1}{2}.$$

The proof that the random variables ε_{jh} ($j = 1, 2, \dots, k; h = 1, 2, \dots, n$) are independent is similar; first of all, the vectors $(\varepsilon_{j1}, \varepsilon_{j2}, \dots, \varepsilon_{jn})$ are independent, since, according to our assumptions, the sets $H_1, H_2, \dots, H_k$ are chosen independently from each other; further, if $\delta_1, \delta_2, \dots, \delta_n$ is an arbitrary sequence of 0's and 1's, then

$$(1.3) \quad \mathbf{P}(\varepsilon_{j1} = \delta_1, \varepsilon_{j2} = \delta_2, \dots, \varepsilon_{jn} = \delta_n) = \frac{1}{2^n} = \prod_{h=1}^n \mathbf{P}(\varepsilon_{jh} = \delta_h)$$

since H has exactly one subset containing those elements for which $\varepsilon_{jh} = 1$ and not containing those ones for which $\varepsilon_{jh} = 0$. Therefore the random variables ε_{jh} ($j = 1, 2, \dots, k; h = 1, 2, \dots, n$) are independent and each of them is equal to 0 (or 1) with probability $\frac{1}{2}$. Let us arrange these variables into a matrix

of $k \times n$ elements so that ε_{jh} be the h th element of the j th row. Let us denote this matrix by E_{kn} . It is easily seen that the requirement that the element x can be uniquely determined by knowing which of the sets $H_1, \dots, H_k$ contain it, in the case $x = x_i$ means that the i th column of the matrix E_{kn} differs from each other one. Since the column vectors of the matrix E_{kn} are independent

⁷ In this way it can also happen that the same subset is selected more than once. However, since n will be large and k will be of order $\log n$, the probability that a subset occurs at least twice is negligible. Moreover, this probability tends to 0 whenever $k/\sqrt{2^n}$ tends to 0.

and have k coordinates and since they are equal to a fixed vector with probability $\frac{1}{2^k}$, thus

$$(1.4) \quad P_{nk} = \left(1 - \frac{1}{2^k}\right)^{n-1}$$

independently of i and of the i th column of E_{kn} . From the inequality $e^{-\frac{x}{1-x}} < 1 - x < e^{-x}$ ($0 < x < 1$) we get

$$e^{-\frac{n-1}{2^k-1}} < P_{nk} < e^{-\frac{n-1}{2^k}}.$$

If $2^k \geq n$, then $\frac{n-1}{2^k-1} < \frac{n}{2^k}$, therefore

$$(1.5) \quad e^{-\frac{n}{2^k}} < P_{nk} < e^{-\frac{n-1}{2^k}} \quad \text{unless } 2^k < n.$$

In other words, if $\frac{1}{e} < \alpha < 1$ and $k \geq \log_2 n + \log_2 \frac{1}{\log \frac{1}{\alpha}}$ then $P_{nk} > \alpha$, while,

on the other hand, if $k \leq \log_2(n-1) + \log_2 \frac{1}{\log \frac{1}{\alpha}}$, then $P_{nk} < \alpha$. Thus we

have proved the following theorem:

Theorem 1.a. *Let us select k subsets of the n -element set H at random, choosing each subset independently from each other and with the same probability. Let P_{nk} denote the probability that a fixed element $x \in H$ is uniquely determined by knowing which ones of the selected subsets do contain it. If $\frac{1}{e} < \alpha < 1$ and*

$k > \log_2 n + \log_2 \frac{1}{\log \frac{1}{\alpha}}$, then $P_{nk} \geq \alpha$, while if $k < \log_2(n-1) + \log_2 \frac{1}{\log \frac{1}{\alpha}}$,

then $P_{nk} < \alpha$.

Remark. If $\alpha = 0.99$, then $\log_2 \frac{1}{\log \frac{1}{\alpha}} < \log_2 100 < 7$ therefore, we can win

the Bar-Kochba game in $\{\log_2 n\} + 7$ steps in more than 99 percent of the games (if the number of elements the other player could think of was n). It is surprising that, independently of how large n is, the number of questions needed putting the questions at random will be greater only by 7 than the minimum number of questions. Thus, e.g., if the players agreed to think of a 6-digit telephone-number, then, in 99 percent of the games the second player will succeed by 27 random questions.

It is easily seen that our conditions on the way of selecting the subsets imply that almost all the sets will have approximately $\frac{n}{2}$ elements.⁸

The following question arises: will it make any difference if we change the rule of selecting the sets so that most of the sets contain approximately p^n elements for a given $p \neq 1/2$, ($0 < p < 1$).

Such a rule can be obtained by supposing that the random variables ε_{jh} remain independent but changing their distribution as follows:

$$(1.6) \quad \mathbf{P}(\varepsilon_{jh} = 1) = p \quad \text{and so} \quad \mathbf{P}(\varepsilon_{jh} = 0) = q = 1 - p.$$

This will be the case if for every $x_h \in H$ we decide by lot whether it should belong to H_j or not and the probability of belonging to H_j is p independently of j and h . Again, we construct the matrix E_{kn} from the numbers ε_{jh} and the fact that the unknown element can be identified by knowing which of the sets $H_1, \dots, H_k$ contain it is equivalent (in the case $x = x_i$) to the fact that the i th column of the matrix E_{kn} differs from all the others. However, now the probability P_{nk} of this event does depend on the number of 1's in the i th column. Clearly

$$(1.7) \quad P_{nk} = \sum_{v=0}^k \binom{k}{v} p^v q^{k-v} (1 - p^v q^{k-v})^{n-1}$$

where v is the number of 1's. The application of the Moivre—Laplace theorem and a short computation yield the following theorem:

Theorem 2.a. *Let us select subsets of an n -element set H independently from each other in the following way: for each element of H we decide by an (independent) draw whether this element belongs to the set or not and the probabilities of these events are p and $q = 1 - p$ respectively $\left(0 < p < 1, p \neq \frac{1}{2}\right)$. Let P_{nk} denote the probability that an arbitrary but fixed element is characterized by the information, which of the selected subsets contain it. In this case, introducing the notation $I_1(\{p, q\}) = p \log_2 \frac{1}{p} + q \log_2 \frac{1}{q}$, if $n \rightarrow \infty$ and*

$$(1.8) \quad k = k(n) = \frac{\log_2 n + y \sqrt{\log_2 n} + o(\sqrt{\log_2 n})}{I_1(\{p, q\})}$$

then

$$(1.9) \quad \lim_{n \rightarrow \infty} P_{n, k(n)} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y/\sigma} e^{-t^2/2} dt$$

where

$$(1.10) \quad \sigma = \sqrt{\frac{pq}{I_1(\{p, q\})}} \cdot \left| \log \frac{p}{q} \right|.$$

⁸ More exactly, with probability near to one, the cardinality of each set will be between the bounds $\frac{n \pm \sqrt{(2 + \delta) n \log \log n}}{2}$ where $\delta > 0$ is arbitrary, and $n \geq n_0(\delta)$.

Remark. If in (1.10) $p = \frac{1}{2}$, then $\sigma = 0$; in this case the theorem remains valid if $y \neq 0$ and y/σ means $+\infty$ or $-\infty$ according whether $y > 0$ or $y < 0$.

§ 2. ACCUMULATION OF INFORMATION IN CASE OF GENERAL CLASSIFICATIONS CONCERNING ONE UNKNOWN ELEMENT

In this paragraph we shall investigate the following generalization of the problem considered in the previous paragraph:

The n -element set H is subdivided at random into r (enumerated) parts s times, independently. Hence, each subdivision will coincide with a fixed subdivision of H with the same probability $\frac{1}{r^n}$. Find the probability — denoted by P_{nk} — that fixing an arbitrary element x of H it can be identified by knowing for each partition, which of the r parts contains it.

It is obvious that such a partition can be characterized by the function the value of which is l on the elements of the l th subset of the partition. The number of these functions and consequently, of the partitions, is r^n . Let ε_{jk} denote the function belonging to the j th subdivision, i.e. let

$$(2.1) \quad \varepsilon_{jh} = l$$

if x_h belongs to the l th class in the j th partition ($l = 1, 2, \dots, r; j = 1, 2, \dots, k; h = 1, 2, \dots, n$). Similarly as in § 1, we can show that the random variables ε_{jh} are independent and

$$(2.2) \quad \mathbf{P}(\varepsilon_{jh} = l) = \frac{1}{r} \quad (j = 1, 2, \dots, k; h = 1, 2, \dots, n; l = 1, 2, \dots, r).$$

Let us consider again the matrix E_{kn} of the numbers ε_{jh} . If $x = x_i$, then P_{nk} equals to the probability that the i th column differs from the others. Thus we obtain that

$$(2.3) \quad P_{nk} = \left(1 - \frac{1}{r^k}\right)^{n-1},$$

that is, if $r^k > n$, then

$$(2.4) \quad e^{-\frac{n}{r^k}} < P_{nk} < e^{-\frac{n-1}{r^k}}.$$

In this way we obtain the following generalization of Theorem 1:

Theorem 1b. *If we choose k partitions of an n -element set H into r subsets at random, independently from each other and so that each of the r^n possible partitions is chosen with the same probability and if P_{nk} denotes the probability that an arbitrarily fixed element x of H is uniquely determined by giving the subset containing*

it for each of the k partitions, further, if $\frac{1}{e} < \alpha < 1$ and $k \geq \frac{\log_2 n + \log_2 \left(\log \frac{1}{\alpha}\right)^{-1}}{\log_2 r}$,

then $P_{nk} \geq \alpha$, while, if $k \leq \frac{\log_2 n + \log_2 \left(\log \frac{1}{a} \right)^{-1}}{\log_2 r}$, then $P_{nk} \leq \alpha$.

Remark. Putting $r = 2$ we obtain Theorem 1a as a special case of Theorem 1b.

Under these conditions on the selection of the partitions each subset of each partition will contain $\frac{n}{r} + O\left(\frac{\sqrt{n \log \log n}}{r}\right)$ elements with probability near to 1. If we would like to have partitions where the cardinalities of the subsets are not approximately constants, say, if we wanted to get subdivisions where the cardinalities of the l th parts are asymptotically equal to P_l^n for an arbitrarily given probability distribution $\mathfrak{P} = (p_1, \dots, p_r)$ then the random selection of the partitions should be modified so that

$$(2.5) \quad \mathbf{P}(\varepsilon_{jh} = l) = p_l \quad (l = 1, 2, \dots, r; j = 1, 2, \dots, k; h = 1, 2, \dots, n)$$

would hold.

In this case, in a way similar to the one used in the previous paragraph we obtain the following formula:

$$(2.6) \quad P_{nk} = \sum_{k_1+k_2+\dots+k_r=k} \frac{k!}{k_1! k_2! \dots k_r!} p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} (1 - p_1^{k_1} p_2^{k_2} \dots p_r^{k_r})^{n-1}.$$

From this by some computation we obtain the following

Theorem 2b. If we subdivide the n -element set H k times, independently into r enumerated subclasses so that each element of H for each of the subdivisions belongs to the l th class with probability p_l $\left(p_l > 0, l = 1, 2, \dots, r; \sum_{l=1}^r p_l = 1\right)$ and P_{nk} denotes the probability that an arbitrary but fixed element x of H can uniquely be determined by knowing for each of the partitions, which class contains x , further, if

$$(2.7) \quad k = k(n) = \frac{\log_2 n + y \sqrt{\log_2 n} + o(\sqrt{\log n})}{I_1(\mathfrak{P})}$$

where $\mathfrak{P} = (p_1, \dots, p_r)$ denotes a probability distribution not all the elements of which are equal, and

$$(2.8) \quad I_1(\mathfrak{P}) = \sum_{l=1}^r p_l \log_2 \frac{1}{p_l},$$

then

$$(2.9) \quad \lim_{n \rightarrow \infty} P_{n,k(n)} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y/\sigma} e^{-t^2/2} dt$$

where

$$(2.10) \quad \sigma = \sqrt{\frac{\sum_{l=1}^r p_l \cdot \log_2^2 p_l - \left(\sum_{l=1}^r p_l \cdot \log_2 \frac{1}{p_l} \right)^2}{I_1(\mathfrak{P})}}.$$

Remark. If $r = 2$, $p_1 = p$, $p_2 = q$ ($p + q = 1$, $p \neq 1/2$) then the value of σ defined by (2.10) is just $\sqrt{pq/I_1(\{p, q\})} \log \frac{p}{q}$; thus for $r = 2$ Theorem 2b reduces to Theorem 2a. If, on the other hand, r is arbitrary but $p_1 = p_2 = \dots = p_r = \frac{1}{r}$, then $\sigma = 0$; the assertion of Theorem 2 remains valid in this case as well if $y \neq 0$ and y/σ is taken by definition to be $+\infty$ or $-\infty$ according to the sign of y .

§ 3. SIMULTANEOUS ACCUMULATION OF INFORMATION IN CASE OF RANDOM DICHOTOMIES

In this paragraph first we shall consider the following problem: We would like to find l unknown elements of an n -element set H by choosing independently k subsets of H (where each subset is chosen with the same probability) and learning about each unknown element which of the selected subsets contain it. Let us denote by P_{nkl} the probability that these data are sufficient to find the l unknown elements of H . Let again denote by $x_1, \dots, x_n$ the elements of H , by $H_1, \dots, H_k$ the selected sets and let $\varepsilon_{jh} = 1$ or 0 according whether x_h belongs to H_j or not, ($j = 1, \dots, k$; $h = 1, \dots, n$). Obviously, P_{nkl} equals to the probability that the l columns of the matrix $E_{kn} = (\varepsilon_{jh})_{j \leq k; h \leq n}$ corresponding to the unknown elements will differ from each other and from the others. Thus we obtain that

$$(3.1) \quad P_{nkl} = \prod_{r=0}^{l-1} \left(1 - \frac{r}{2^k}\right) \left(1 - \frac{l}{2^k}\right)^{n-l}$$

It follows easily from (3.1) that if n , k and l tend to infinity so that $l = o(n)$

and $k = \log_2 nl + \log_2 \frac{1}{\log \frac{1}{\alpha}} + o(1)$ where $0 < \alpha < 1$ then

$$(3.3) \quad \lim P_{nkl} = \alpha.$$

On the other hand, if n and l tend to infinity so that

$$(3.4) \quad l \sim \vartheta n \quad (0 < \vartheta \leq 1)$$

then (3.3) holds in that case when

$$(3.5a) \quad k = \log_2 nl + \log_2 \frac{1 - \frac{\vartheta}{2}}{\log \frac{1}{\alpha}} + o(1),$$

that is, if

$$(3.5b) \quad k = 2 \log_2 n + \log_2 \frac{\vartheta(2 - \vartheta)}{2 \log \frac{1}{\alpha}} + o(1).$$

In particular, if

$$(3.6) \quad l = n$$

then

$$(3.7) \quad k = 2 \log_2 n + \log_2 \frac{1}{2 \log \frac{1}{\alpha}} + o(1)$$

is needed to ensure (3.3).

Hence, the following theorem holds:

Theorem 3a. *If we choose k subsets of an n -element set H at random, independently of each other and so that each of the k subsets of H are chosen with the same probability, and P_{nk} denotes the probability that the selected k subsets separate each pair of elements of H (that is, for any two elements x and y at least one of the k subsets contains exactly one of them) and n and k tend to infinity so that*

$$k = 2 \log_2 n + \log_2 \frac{1}{2 \log \frac{1}{\alpha}} + o(1),$$

where $0 < \alpha < 1$, then

$$\lim_{n \rightarrow \infty} P_{nk} = \alpha.$$

Comparing Theorems 1a and 3a we observe that we need roughly twice as much random sets to separate all the elements than to separate just one. Actually, we had to find an unknown permutation in Theorem 3a. This requires at least $\log_2 n! = n \log_2 n$ "bits" of information, while one dichotomy gives at most one "bit" for each element of H , that is, at most n "bits" altogether. In other words, if an unknown permutation is determined by using random dichotomies, the redundancy will be approximately 100 per cent.⁹

§ 4. SIMULTANEOUS ACCUMULATION OF INFORMATION IN CASE OF GENERAL CLASSIFICATIONS

Let us consider now the case when l different elements of an n -element set H are to be found on the basis of the following information: we select a subdivision of the set H into r parts at random (so that any partition has the same probability) and then we are told about each of the unknown elements, which of the r parts they belong to; then we again select a partition at random, independently of the first selection, and so on . . . Let P_{nkl} denote the proba-

⁹ If $l > n$, but — using the terminology of the simultaneous Bar—Kochba game — it is allowed to choose the same thing by more than one player, then the same number of dichotomies will be needed as for $l = n$, since $2 \log_2 n + \log_2 \frac{1}{2 \log \frac{1}{\alpha}}$ dichotomies will

separate all the elements of H with probability $\sim \alpha$ and it makes no difference, how many players had chosen a given element. (Indeed, these players will give the same answers and therefore B knowing that one of them has thought of a given element will also know that the others have chosen the same element.)

bility that k partitions are sufficient to identify all the unknown elements. Similarly as above it is easily seen that

$$(4.1) \quad P_{nkl} = \prod_{v=0}^{l-1} \left(1 - \frac{v}{r^k}\right) \left(1 - \frac{l}{r^k}\right)^{n-l}.$$

Therefore, if

$$(4.2) \quad l = o(n)$$

then

$$(4.3) \quad k = \frac{\log_2 nl + \log_2 \frac{1}{\log \frac{1}{\alpha}} + o(1)}{\log_2 r}$$

will imply

$$(4.4) \quad \lim P_{nkl} = \alpha \quad (0 < \alpha < 1).$$

On the other hand, if

$$(4.5) \quad l \sim \vartheta n \quad (0 < \vartheta \leq 1)$$

then

$$(4.6) \quad k = \frac{2 \log_2 n + \log_2 \frac{\vartheta(2-\vartheta)}{2 \log \frac{1}{\alpha}} + o(1)}{\log_2 r}$$

will imply (4.4).

In the view of these results we could think that if the cardinalities of the parts in a partition are approximately $p_1 n, p_2 n, \dots, p_r n$ (where $\sum p_i = 1$) then the only change in the results above is that $\log_2 r$ must be replaced by $I_1(\mathcal{P})$. However, a more detailed investigation disproves this conjecture: it turns out

that $\log_2 r$ must be replaced not by the Shannon entropy $I_1(\mathcal{P}) = \sum_{i=1}^r p_i \log \frac{1}{p_i}$,

but by the second order information measure $I_2(\mathcal{P}) = -\log_2 \left(\sum_{i=1}^r p_i^2 \right)$. (Of

course, if $p_1 = p_2 = \dots = p_r = \frac{1}{r}$ then $I_1(\mathcal{P}) = I_2(\mathcal{P})$.) This can be proved as

follows: Let $\pi_1, \pi_2, \dots, \pi_{r^k}$ denote in some fixed order all the possible products of k not necessarily different p_i 's where the order of factors is also counted.

Clearly, each of these products is of the form $p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ where $\sum_{i=1}^r k_i = k$

and this product occurs $\frac{k!}{k_1! k_2! \dots k_r!}$ times in the sequence $\pi_1, \pi_2, \dots, \pi_{r^k}$.

For the sake of simplicity, let us restrict our considerations to the most interesting case $l = n$.

If P_{nk} denotes the probability that the k partitions separate each element of H , then

$$(4.7) \quad P_{nk} = \sum' \pi_{i_1} \pi_{i_2} \dots \pi_{i_n}$$

where the summation is extended over all the n -tuples $(i_1, i_2, \dots, i_n)$ consisting of n different numbers.

To describe the asymptotic behavior of the sum on the left side of (4.7) we need that very sieve formula which was proved by the author in [5]. Let B_{ij} denote the event that the i th and j th column of the matrix E_{kn} are equal. Then P_{nk} is just the probability that none of the events B_{ij} ($1 \leq i < j \leq n$) occurs. Let G denote a graph the vertices of which are the pairs (i, j) ($1 \leq i < j \leq n$) and two pairs (i, j) and (i', j') are joined by an edge if not all the numbers i, i', j, j' are different (i.e., if either $i = i'$ or $i = j'$ or $j = i'$ or $j = j'$; clearly, since $i < j$ and $i' < j'$, at most one of the four equalities can hold). Let Γ^* denote the family of independent subsets of this graph (i.e. the family of those subsets no two elements of which are joined) and let Γ^{**} denote the family of those subsets of the vertices of G which contain at most one pair of vertices joined in the graph. Let

$$(4.8) \quad S_d^* = \sum^* P(B_{i_1 j_1} B_{i_2 j_2} \dots B_{i_d j_d})$$

and

$$(4.9) \quad S_d^{**} = \sum^{**} P(B_{i_1 j_1} B_{i_2 j_2} \dots B_{i_d j_d})$$

where $\sum^*$ and $\sum^{**}$ denote a summation over the d -tuples of pairs belonging to Γ^* or Γ^{**} respectively. In this case, according to a theorem of [5] for any non-negative integer s

$$(4.10) \quad 1 - S_1^{**} + S_2^* - S_3^{**} + \dots - S_{2s+1}^{**} \leq P_{nk} \leq 1 - S_1^* + S_2^{**} - \dots + S_{2s}^{**}$$

Now, it is obvious that

$$(4.11) \quad S_d^* = \left(\sum_{i=1}^r \pi_i^2 \right)^d \frac{n(n-1) \dots (n-2d+1)}{d! 2^k}$$

and

$$(4.12) \quad S_d^{**} = S_d^* \left(1 + \frac{8 \left(\sum_{i=1}^r \pi_i^3 \right) d(d-1)}{3 \left(\sum_{i=1}^r \pi_i^2 \right)^2 (n-2d+1)} \right).$$

Therefore, if

$$(4.13) \quad k = \frac{2 \log_2 n + \log \frac{1}{2 \log \frac{1}{\alpha}} + o(1)}{\log_2 \frac{1}{\sum_{v=1}^r p_v^2}}$$

then, since

$$(4.14) \quad \sum_{i=1}^{r^k} \pi_i^2 = \left(\sum_{v=1}^r p_v^2 \right)^k$$

we obtain, that for arbitrary fixed d

$$(4.15) \quad S_d^* \sim \frac{\left(\log \frac{1}{\alpha} \right)^d}{d!}.$$

Further, taking into account that

$$(4.16) \quad \sum_{i=1}^{r^k} \pi_i^3 = \left(\sum_{v=1}^r p_v^3 \right)^k$$

and therefore, if $\bar{p} = \max_{1 \leq v \leq r} p_v$ then

$$(4.17) \quad \sum_{i=1}^{r^k} \pi_i^3 < \bar{p}^k \left(\sum_{v=1}^r p_v^2 \right)^k$$

thus we obtain, that

$$(4.18) \quad S_d^{**} = S_d^* (1 + o(n^{-e}))$$

where

$$(4.19) \quad e = \frac{\log_2 \frac{\sum_{v=1}^r p_v^2}{\bar{p}^2}}{\log_2 \frac{1}{\sum_{v=1}^r p_v^2}} > 0.$$

Therefore, for every non-negative integer s

$$(4.20) \quad \sum_{d=0}^{2s+1} \frac{(-1)^d \left(\log \frac{1}{\alpha} \right)^d}{d!} \leq \underline{\lim} P_{nk} \leq \overline{\lim} P_{nk} \leq \sum_{d=0}^{2s} \frac{(-1)^d \left(\log \frac{1}{\alpha} \right)^d}{d!}.$$

If $n \rightarrow +\infty$, we obtain that

$$(4.21) \quad \lim P_{nk} = e^{-\log \frac{1}{\alpha}} = \alpha.$$

Thus we have proved the following theorem:

Theorem 3b. *If we partition the elements of an n -element set H k times independently into r classes so that each element of H at any partitioning will belong to the j th class with the probability p_j and if P_{nk} denotes the probability that the k considered partition separate each element of H , that is, for any two elements*

there is a partition in which the two elements belong to different classes, and if n and k tend to infinity so that

$$(4.22) \quad k = \frac{2 \log_2 n + \log_2 \frac{1}{\log \frac{1}{\alpha}} + o(1)}{-\log \left(\sum_{v=1}^r p_v^2 \right)}$$

where $0 < \alpha < 1$, then

$$(4.23) \quad \lim P_{nk} = \alpha.$$

Clearly, Theorem 3b contains Theorem 3a as a special case (when $r = 2$ and $p_1 = p_2 = \frac{1}{2}$).

REFERENCES

- [1] Rényi, A.: Az információelmélet néhány alapvető kérdése. *MTA III. Oszt. Közl.*, 10 (1960), 251–282.
- [2] Rényi, A.: On measures of entropy and information. *Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability*, University of California Press, 1961, Vol. I, 547–561.
- [3] Rényi, A.: On random generating elements of a finite Boolean algebra. *Acta Sci. Math. Szeged*, 22 (1961), 75–81.
- [4] Rényi, A.: Statistical laws of accumulation of information. *Bulletin of the International Statistical Institute*, 33rd Session of the ISI in Paris, 1961, 1–7.
- [5] Rényi, A.: Egy általános módszer valószínűségszámítási tételek bizonyítására és annak néhány alkalmazása. *MTA III. Oszt. Közl.*, 11 (1961), 79–105.

182, 187, 192, 213, 249, 256, 320, 340, 344

ON THE EXTREME ELEMENTS OF OBSERVATIONS

A. RÉNYI

INTRODUCTION

Let us perform independent observations concerning a random quantity. Let ξ_k ($k = 1, 2, \dots$) be the k th observation. In other words assume that the random variables are independent and identically distributed. Denote their common distribution function by $F(x)$. Assume that $F(x)$ is continuous for all values of x (i.e. the variables ξ_k take each real value x with probability 0). In other words: let ξ_k be the k th element of the sample in an infinite sampling concerning a population having continuous distribution. An observation ξ_k is called an extreme element of the sampling if $\xi_k > \xi_j$ for $j < k$. In other words an observation is extreme if it is larger than any of the preceding observations. By this definition ξ_1 is always (trivially) extreme. Let $\nu_0 = 1$; write ν_1 for the index of the first extreme observation having an index greater than 1 (i.e. non-trivial), ν_2 for the index of the first extreme observation having an index greater than ν_1 (i.e. the second non-trivial), in general ν_n for the index of the n th non-trivial extreme observation ($n = 1, 2, 3, \dots$). The aim of this paper is to study limit- and limit distribution theorems concerning the random variables ν_n .

Before stating the theorems concerning the sequence of random variables ν_n ($n = 1, 2, 3, \dots$) we make some general remarks. First of all it is obvious that the behaviour of the variables ν_n cannot depend on the distribution function $F(x)$. As a matter of fact, if ξ_{ν_n} is the n th extreme element of the sequence ξ_k , then $F(\xi_{\nu_n})$ is the n th extreme element of the sequence $F(\xi_k)$. Now the variables $F(\xi_k)$, $k = 1, 2, \dots$ are uniformly distributed on the interval $(0, 1)$, thus we can assume, without restricting generality, that our variables are uniformly distributed on the interval $(0, 1)$. All the limit theorems proved for the variables ν_n under this condition keep holding true without this condition for any choice of the continuous distribution function $F(x)$. The properties of the sequence of variables ν_n are thus "distribution-free". This implies that every statistical test based on the variables will also be "distribution-free". This area is similar to that of the order statistics; the main difference is that here we start from an infinite sequence of observations.

In § 1 we investigate the dependence of the variables ν_n and we show that the variables ν_n form a homogeneous Markov chain. In § 2 we determine the probability that the first N elements of the sequence ξ_k contain a given number of extreme elements. In § 3 we prove the surprising fact that if A_k denotes the event that the element ξ_k is extreme, then the events A_k ($k = 1, 2, \dots$) are mutually independent (in spite of the fact that A_k depends on all the variables $\xi_1, \xi_2, \dots, \xi_k$). This fact forms the basis of our further investigations. It will also give another way for proving the results of §§ 1 and 2. In § 4 we

prove that $\lim_{n \rightarrow \infty} \sqrt[n]{\nu_n} = e$ with probability 1; this can be considered as a strong law of large numbers for the weakly dependent variables $\log \frac{\nu_n}{\nu_{n-1}}$.

In § 5 we prove that $\log v_n$ is normally distributed in limit with expectation n and standard deviation $\sqrt{n}$; this can be considered as a central limit theorem for the weakly dependent variables $\log \frac{v_n}{v_{n-1}}$. § 6 deals with the iterated logarithm theorem for the variables v_n , while in § 7 we point to some interesting relations between the variables v_n and the representation of permutations as products of cycles. Finally in § 8 we investigate the surprising relation between the variables v_n and the representation of real numbers by modified Engel series.

§ 1. THE JOINT DISTRIBUTION OF THE INDICES OF EXTREME ELEMENTS

We prove that the variables v_n form a homogeneous Markov chain and determine the transition probabilities of this Markov chain. To this, we need to determine the joint distribution of the variables $v_1, v_2, \dots, v_n$. As shown in the introduction, we can assume without restricting generality that the variables ξ_k are uniformly distributed in the interval $(0, 1)$. Let $1 < k_1 < \dots < k_n$, where $k_1 < \dots < k_n$ are integers. It is easy to see that if¹

$$\begin{aligned} G(k_1, \dots, k_n; x_0, x_1, \dots, x_n) = \\ (1.1) \quad = \mathbf{P}(v_1 = k_1, \dots, v_n = k_n, \xi_1 < x_0, \xi_{k_1} < x_1, \dots, \xi_{k_n} < x_n) \end{aligned}$$

and

$$(1.2) \quad g(k_1, \dots, k_n; x_0, \dots, x_n) = \frac{\partial^{n+1} G(k_1, \dots, k_n; x_0, x_1, \dots, x_n)}{\partial x_0 \partial x_1 \dots \partial x_n}$$

then

$$(1.3) \quad g(k_1, \dots, k_n; x_0, x_1, \dots, x_n) = x_0^{k_1-2} x_1^{k_1-k_1-1} \dots x_{n-1}^{k_n-k_{n-1}-1}$$

if only $0 < x_0 < x_1 < \dots < x_n$;

and thus

$$\begin{aligned} \mathbf{P}(v_1 = k_1, \dots, v_n = k_n) = \\ (1.4) \quad = \int \int \dots \int_{0 < x_0 < x_1 < \dots < x_n < 1} x_0^{k_1-2} x_1^{k_1-k_1-1} \dots x_{n-1}^{k_n-k_{n-1}-1} dx_0 dx_1 \dots dx_n \end{aligned}$$

Therefore

$$(1.5) \quad \mathbf{P}(v_1 = k_1, \dots, v_n = k_n) = \frac{1}{(k_1 - 1)(k_2 - 1) \dots (k_{n-1} - 1)(k_n - 1)k_n}.$$

Thus

$$(1.6) \quad \mathbf{P}(v_n = k_n \mid v_1 = k_1, \dots, v_{n-1} = k_{n-1}) = \frac{k_{n-1}}{(k_n - 1)k_n}.$$

¹ $\mathbf{P}(\dots)$ denotes the probability of the events in brackets.

(1.6) shows that the variables v_n ($n = 0, 1, 2, \dots$) form a homogeneous Markov chain with transition probabilities

$$(1.7) \quad \mathbf{P}(v_n = k | v_{n-1} = l) = \frac{l}{(k-1)k}, \quad k \geq l+1 \geq n+1, \quad n = 1, 2, \dots$$

In particular (since $v_0 \equiv 1$) in case $n = 1$ (1.7) implies that

$$(1.8) \quad \mathbf{P}(v_1 = k) = \frac{1}{(k-1)k}, \quad k \geq 2.$$

As a consequence of (1.8) we see that *the expectation of v_1 is infinite*. This paradox fact has been remarked first by S. S. Wilks [12] and analyzed in details by E. J. Gumbel [13].

(1.5) and (1.7) help in answering several questions concerning the sequence v_n . We can, for instance, determine the distribution of v_n . Obviously, for $k \geq n+1$ we have

$$(1.9) \quad \mathbf{P}(v_n = k) = \sum_{1 < k_1 < \dots < k_{n-1} < k} \frac{1}{(k_1 - 1) \dots (k_{n-1} - 1) (k - 1) k}.$$

Let us now determine for fixed $k \geq 2$ the generating function of the sequence of numbers $\mathbf{P}(v_n = k)$, $n = 1, 2, \dots, k-1$, i.e. the polynomial

$$(1.10) \quad G_k(z) = \sum_{n=1}^{k-1} \mathbf{P}(v_n = k) z^n \quad (k = 2, 3, \dots).$$

It is easy to see that

$$(1.11) \quad G_k(z) = \frac{z}{k(k-1)} \prod_{j=1}^{k-2} \left(1 + \frac{z}{j}\right) = (-1)^k \frac{\binom{1-z}{k}}{z-1}.$$

Evidently

$$(1.12) \quad G_k(1) = \sum_{n=1}^{k-1} \mathbf{P}(v_n = k)$$

is the probability of the occurrence of the number k in the sequence of numbers v_n . (1.11) yields

$$(1.13) \quad G_k(1) = \frac{1}{k(k-1)} \prod_{j=1}^{k-2} \left(\frac{j+1}{j}\right) = \frac{1}{k}.$$

Thus we have the following

Lemma 1. *The probability of the event that the k th element of an infinite sample drawn from a population having continuous distribution be extreme, equals $\frac{1}{k}$.*

Using relation (1.11) we can determine for arbitrary fixed n the generating function of the sequence of numbers $\mathbf{P}(v_n = k)$, $k = n+1, n+2, \dots$

Setting

$$(1.14) \quad H(z, w) = \sum_{n=0}^{\infty} \sum_{k=n+1}^{\infty} \mathbf{P}(v_n = k) z^n w^k$$

we have

$$(1.15) \quad H(z, w) = w + \sum_{k=2}^{\infty} G_k(z) w^k = \frac{(1-w)^{1-z} - 1}{z-1}.$$

Therefore

$$H(z, w) = \frac{1-w}{z-1} \sum_{n=0}^{\infty} \frac{z^n \left(\log \frac{1}{1-w} \right)^n}{n!} - \frac{1}{z-1},$$

thus for $n \geq 1$

$$(1.16) \quad \sum_{k=n+1}^{\infty} \mathbf{P}(v_n = k) w^k = (w-1) \sum_{l=0}^n \frac{\left(\log \frac{1}{1-w} \right)^l}{l!} + 1.$$

§ 2. THE DISTRIBUTION OF THE NUMBER OF EXTREME ELEMENTS IN A SEQUENCE OF OBSERVATIONS OF GIVEN NUMBER OF ELEMENTS

In this § we deal with the following question: write μ_N for the number of extreme elements in the sequence $\xi_1, \xi_2, \dots, \xi_N$; we are to determine the distribution of μ_N . It can be seen, the same way as (1.1), that defining

$$(2.1) \quad G_N(k_1, \dots, k_n; x_0, x_1, \dots, x_n) = \\ = \mathbf{P}(v_1 = k_1, \dots, v_n = k_n, v_{n+1} > N, \xi_1 < x_0, \xi_{v_1} < x_1, \dots, \xi_{v_n} < x_n$$

and

$$(2.2) \quad g_N(k_1, \dots, k_n; x_0, x_1, \dots, x_n) = \frac{\partial^{n+1} G_N(k_1, \dots, k_n; x_0, x_1, \dots, x_n)}{\partial x_0 \partial x_1 \dots \partial x_n}$$

for integers $1 < k_1 < \dots < k_n \leq N$, one has

$$(2.3) \quad g_N(k_1, \dots, k_n; x_0, \dots, x_n) = x_0^{k_1-2} x_1^{k_1-k_1-1} \dots x_{n-1}^{k_n-k_{n-1}-1} x_n^{N-k_n}$$

if $0 < x_0 < \dots < x_n$. This implies that

$$(2.4) \quad \mathbf{P}(v_1 = k_1, \dots, v_n = k_n, v_{n+1} > N) = \frac{1}{(k_1-1)(k_2-1)\dots(k_n-1)N}$$

for $1 < k_1 < k_2 < \dots < k_n \leq N$.

Therefore setting

$$(2.5) \quad Q_N(n) = \mathbf{P}(\mu_N = n)$$

we have $Q_1(1) = 1$ and for $N \geq 2$

$$(2.6) \quad Q_N(n) = \frac{1}{N} \sum_{1 < k_1 < \dots < k_n \leq N} \frac{1}{(k_1-1)\dots(k_n-1)}, \quad n = 1, 2, \dots$$

and thus

$$(2.7) \quad H_N(x) = \sum_{n=1}^N Q_N(n) x^n = \frac{x}{N} \prod_{r=1}^{N-1} \left(1 + \frac{x}{r}\right).$$

Thus we have determined the generating function of μ_N . One evidently has the identity

$$(2.8) \quad H_N(x) = \prod_{l=1}^N \left(1 + \frac{x-1}{l}\right).$$

Now we can determine the moments of μ_N . If $\mathbf{E}\zeta$ stands for the expectation of the random variable ζ and $\mathbf{D}\zeta$ for its standard deviation, then (2.7) yields

$$(2.9) \quad \mathbf{E}\mu_N = \sum_{s=1}^N \frac{1}{s}$$

and

$$(2.10) \quad \mathbf{D}^2 \mu_N = \sum_{s=1}^N \frac{1}{s} - \sum_{s=1}^N \frac{1}{s^2}.$$

Therefore

$$(2.11) \quad \mathbf{E}\mu_N = \log N + O(1)$$

and

$$(2.12) \quad \mathbf{D}^2 \mu_N = \log N + O(1).$$

The higher moments of μ_N can be calculated similarly.

Formula (2.7) can be rewritten as follows:

$$(2.13) \quad H_N(x) = \sum_{n=1}^N \frac{|S_N^{(n)}| x^n}{N!}$$

where $S_N^{(n)}$ stand for the Stirling numbers of first kind (cf. [1], p. 142). Thus

$$(2.14) \quad Q_N(n) = \frac{|S_N^{(n)}|}{N!}.$$

Thus we obtained a simple probabilistic interpretation of the Stirling numbers of first kind. (For another (more complicated) probabilistic interpretation see [1], pp. 166—167.)

§ 3. THE INDEPENDENCE OF EXTREMITY OF DIFFERENT OBSERVATIONS

Write A_k for the event that the k th element of an infinite sample of a population having a continuous distribution is extreme. In this § we prove the following simple but basic fact

Lemma 2. *If A_k ($k = 1, 2, \dots$) denotes the event that the k th element of a sample of a population having a continuous distribution, is extreme, then the events $A_1, A_2, \dots, A_k, \dots$ are independent.*

In view of the importance of this lemma we give three different proofs.

First proof. If $1 < j_1 < j_2 < \dots < j_k$ are arbitrary integers, then we get, similarly as in §§ 1 and 2, that

$$(3.1) \quad \mathbf{P}(A_{j_1} A_{j_2} \dots A_{j_k}) = \int \int \dots \int_{0 < x_1 < \dots < x_k < 1} x_1^{j_1-2} x_2^{j_2-j_1-1} \dots x_k^{j_k-j_{k-1}-1} dx_1 dx_2 \dots dx_k$$

whence

$$(3.2) \quad \mathbf{P}(A_{j_1} A_{j_2} \dots A_{j_k}) = \frac{1}{j_1 j_2 \dots j_k},$$

and since $\mathbf{P}(A_k) = \frac{1}{k}$ by Lemma 1, thus

$$(3.3) \quad \mathbf{P}(A_{j_1} A_{j_2} \dots A_{j_k}) = \mathbf{P}(A_{j_1}) \mathbf{P}(A_{j_2}) \dots \mathbf{P}(A_{j_k}).$$

Second proof. Let us arrange the random variables in order of magnitude. Let $\xi_{l_1^{(n)}}$ be the largest one, $\xi_{l_2^{(n)}}$ be the second largest and in general $\xi_{l_r^{(n)}}$ the r th in order ($r = 1, 2, \dots, n$). The sequence of numbers $(l_1^{(n)}, l_2^{(n)}, \dots, l_n^{(n)})$ is a permutation of the numbers $1, 2, \dots, n$ and since the variables are independent and identically distributed, each of the possible $n!$ permutations occurs with the same probability $\frac{1}{n!}$. The probability $\mathbf{P}(A_{j_1}, A_{j_2}, \dots, A_{j_k})$

($1 < j_1 < j_2 < \dots < j_k$) can be thus computed by determining at which permutations $(l_1^{(j_k)}, l_2^{(j_k)}, \dots, l_{j_k}^{(j_k)})$ the numbers $\xi_{j_1}, \xi_{j_2}, \dots, \xi_{j_k}$ are extreme and then dividing by $j_k!$. It is obvious that in order that $\xi_{j_1}, \xi_{j_2}, \dots, \xi_{j_k}$ are extreme, the fulfilment of the following conditions is necessary and sufficient: (a) among the numbers $\xi_1, \xi_2, \dots, \xi_{j_k}$ the largest one is ξ_{j_k} , i.e. $l_{j_k}^{(j_k)} = j_k$. (b) the numbers $j_k - 1, j_k - 2, \dots, j_{k-1} + 1$ can be placed arbitrarily in the sequence $(l_1^{(j_k)}, l_2^{(j_k)}, \dots, l_{j_k}^{(j_k)})$ but after having placed them j_{k-1} should be placed to the first one of the empty places (c) in general, after having placed the numbers $r \geq j_s$ ($1 \leq s \leq k$ the numbers $j_s - 1, j_s - 2, \dots, j_{s-1} + 1$) $j_0 = 1$) can be placed arbitrarily to the empty places, and then the number j_{s-1} should be placed to the first one of the still empty places.

The above said imply that there is no choice when placing the numbers $j_1, j_2, \dots, j_k$; if however $m < j_k$ and $m \neq j_i$ ($i = 1, 2, \dots, k$), then we have m choices for placing the number m . Thus the number of permutations $l_1^{(j_k)}, l_2^{(j_k)}, \dots, l_{j_k}^{(j_k)}$ at which the events $A_{j_1}, A_{j_2}, \dots, A_{j_k}$ occur, is $\frac{j_k}{j_1 j_2 \dots j_k}$ and thus

$$(3.4) \quad \mathbf{P}(A_{j_1} A_{j_2} \dots A_{j_k}) = \frac{j_k}{j_1 j_2 \dots j_k}.$$

Third proof. It is known in the theory of order-statistics that if $\xi_1, \xi_2, \dots, \xi_n$ are independent identically distributed random variables, then ξ_n falls with the same probability $\frac{1}{n}$ to any of the n intervals to which the values of the variables $\xi_1, \xi_2, \dots, \xi_{n-1}$ divide the real axis. Indeed, the event that ξ_n falls to the l th (from the right) of the above intervals ($l = 1, 2, \dots, n$ where the interval $x \geq \max(\xi_1, \xi_2, \dots, \xi_{n-1})$ is called the first one and the interval $x < \min(\xi_1, \xi_2, \dots, \xi_{n-1})$ is called the n th one) means that ξ_n is the l th term

of the sequence $\xi_1, \xi_2, \dots, \xi_n$ in order of magnitude, and since the numbers $1, 2, \dots, n$ have $(n-1)!$ such permutations where n stands at the l th place, thus the probability of our event is $\frac{(n-1)!}{n!} = \frac{1}{n}$. In particular, the probability

that ξ_n is extreme, is $\frac{1}{n}$, i.e. $\mathbf{P}(A_n) = \frac{1}{n}$. This is a new proof for Lemma 1.

On the other hand the above combinatorial argument shows that the conditional probability of the event A_n is $\frac{1}{n}$ under any condition which refers

only to the order of the variables $\xi_1, \xi_2, \dots, \xi_{n-1}$ and contains no restriction for the values of these variables. Indeed, writing B for such a condition and assuming that the event B occurs in $N \leq (n-1)!$ arrangements out of the all possible $(n-1)!$ arrangements (in order of magnitude) of the variables $\xi_1, \xi_2, \dots, \xi_{n-1}$, we have

$$(3.5) \quad \mathbf{P}(A_n | B) = \frac{N}{Nn} = \frac{1}{n}.$$

Now choosing the event $A_{j_1}, A_{j_2}, \dots, A_{j_k}$ for B and $n = j_k$ ($1 < j_1 < j_2 < \dots < j_k$) the statement of Lemma 2 follows immediately.

Using the third proof of Lemma 2 we can establish the following generalization of Lemma 2:

Lemma 3. *Let $\xi_1, \xi_2, \dots, \xi_k, \dots$ be independent random variables having the same continuous distribution, and write α_k for the index of ξ_k in the sequence obtained from the sequence of numbers $\xi_1, \xi_2, \dots, \xi_k$ by ordering them in decreasing order ($k = 1, 2, \dots$). Then the variables $\alpha_1, \alpha_2, \dots, \alpha_k, \dots$ are mutually independent, $\alpha_1 \equiv 1$, and for $n = 2, 3, \dots$*

$$(3.6) \quad \mathbf{P}(\alpha_n = l) = \frac{1}{n}, \quad l = 1, 2, \dots, n.$$

Proof. For all statements of the lemma it is sufficient to show that for any $n \geq 2$ and arbitrary integers $a_1, a_2, \dots, a_n$ with $1 \leq a_k \leq k$ ($k = 2, 3, \dots, n$) we have

$$(3.7) \quad \mathbf{P}(\alpha_2 = a_2, \alpha_3 = a_3, \dots, \alpha_n = a_n) = \frac{1}{n!}$$

Any admissible choice of the numbers $a_2, \dots, a_n$ determines the order of the sequence of numbers uniquely, thus corresponds to one of the permutations denoted above by $(l_1^{(n)}, l_2^{(n)}, \dots, l_n^{(n)})$; in fact a_k gives the number how many ξ_j with $j < k$ precede the number ξ_k in the sequence obtained by ordering the numbers $\xi_1, \xi_2, \dots, \xi_k$ in decreasing order. This implies the statement of Lemma 3.

Lemma 3 obviously contains Lemma 2 as a special case since (3.7) implies

$$(3.8) \quad \mathbf{P}(A_{j_1}, A_{j_2}, \dots, A_{j_k}) = \mathbf{P}(\alpha_{j_1} = j_1, \alpha_{j_2} = j_2, \dots, \alpha_{j_k} = j_k) = \frac{1}{j_1 j_2 \dots j_k}.$$

This can be considered as a new (fourth) proof for Lemma 2.

Actually the second, third and fourth proof of Lemma 2 are different variants of the same combinatorial idea. In fact there are two essentially different ways

leading to Lemma 2: we can establish it analytically (first proof) or using combinatorial arguments.

Using Lemma 2 we can get new proofs for the results of §§ 1 and 2. E.g. (1.5) can be established as follows: if $l_1, l_2, \dots, l_{k_n-n}$ denote the terms in the sequence $1, 2, \dots, k_n - 1$ different from $k_1, k_2, \dots, k_{n-1}$, then (writing $\bar{A}$ for the complement of the event A)

$$(3.9) \quad \mathbf{P}(v_1 = k_1, \dots, v_n = k_n) = \mathbf{P}(A_{k_1} \dots A_{k_n} \bar{A}_{l_1} \bar{A}_{l_2} \dots \bar{A}_{l_{k_n-n}})$$

and thus

$$(3.10) \quad \mathbf{P}(v_1 = k_1, \dots, v_n = k_n) = \frac{1}{k_1 \dots k_n} \prod_{j=1}^{k_n-n} \left(1 - \frac{1}{l_j}\right) = \\ = \frac{1}{(k_1 - 1) \dots (k_n - 1) k_n}.$$

The fact that the variables v_n form a Markov chain becomes obvious since, in general, if the variables η_k are independent and integer-valued and v_n denotes the n th index k for which $\eta_k = a$ (a is a fixed integer), then the variables v_n form a Markov chain.

(2.8) can be proved similarly (and also (2.6) being a corollary of (2.8)).

In fact, let

$$(3.11) \quad \varepsilon_k = \begin{cases} 1, & \text{if the event } A_k \text{ occurs} \\ 0 & \text{otherwise} \end{cases}$$

then

$$(3.12) \quad \mu_N = \varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_N.$$

And since the variables ε_k are independent by Lemma 2, the generating function of μ_N equals the product of the generating functions of the variables ε_k ($k = 1, 2, \dots, N$). Now

$$\mathbf{P}(\varepsilon_k = 1) = \frac{1}{k} \quad \text{and} \quad \mathbf{P}(\varepsilon_k = 0) = 1 - \frac{1}{k},$$

thus the generating function of ε_k is $1 + \frac{x-1}{k}$, therefore the generating function of μ_N is

$$(3.13) \quad H_N(x) = \prod_{k=1}^N \left(1 + \frac{x-1}{k}\right).$$

§ 4. A LAW OF LARGE NUMBERS FOR EXTREME OBSERVATIONS

In this § we prove the following theorem:

Theorem 1. *If v_n denotes the index of the n th extreme element of an infinite sample drawn from a population having a continuous distribution, then with probability 1*

$$(4.1) \quad \lim_{n \rightarrow \infty} \sqrt[n]{v_n} = e,$$

(e is the base of the natural logarithm).

Proof. We start from the obvious relation

$$(4.2) \quad \mathbf{P}(v_n \leq k) = \mathbf{P}(\mu_k \geq n)$$

whence

$$(4.3) \quad \mathbf{P}(v_n > k) = \mathbf{P}(\mu_k < n).$$

Choose an arbitrarily small positive number ε . Writing $\{x\}$ for the smallest integer not less than x and $[x]$ for the largest integer not exceeding x (the integer part of x) we have

$$(4.4) \quad \mathbf{P}(v_n > e^{n(1+\varepsilon)}) = \mathbf{P}(\mu_{\{e^{n(1+\varepsilon)}\}} < n)$$

and

$$(4.5) \quad \mathbf{P}(v_n \leq e^{n(1-\varepsilon)}) = \mathbf{P}(\mu_{[e^{n(1-\varepsilon)}]} \geq n).$$

According to the Chebyshev inequality

$$(4.6) \quad \mathbf{P}(|\mu_N - \mathbf{E}\mu_N| \geq \lambda \mathbf{D}\mu_N) \leq \frac{1}{\lambda^2},$$

thus by (2.11) and (2.12) we get

$$(4.7) \quad \mathbf{P}(|\mu_N - \log N| \geq \varepsilon \log N) = O\left(\frac{1}{\log N}\right).$$

(4.4), (4.5) and (4.7) imply that

$$(4.8) \quad \mathbf{P}(\sqrt[n]{v_n} > e^{1+\varepsilon}) + \mathbf{P}(\sqrt[n]{v_n} < e^{1-\varepsilon}) = O\left(\frac{1}{n}\right).$$

Thus the sequence

$$(4.9) \quad \sum_{k=1}^{\infty} (\mathbf{P}(\sqrt[k^2]{v_{k^2}} > e^{1+\varepsilon}) + \mathbf{P}(\sqrt[k^2]{v_{k^2}} < e^{1-\varepsilon}))$$

is convergent for any positive value of ε , and by the Borel—Cantelli lemma (cf. [2]) we get with probability 1

$$(4.10) \quad \lim_{k \rightarrow \infty} \sqrt[k^2]{v_{k^2}} = e.$$

Introducing the notation $\beta_n = \sqrt[n]{v_n}$, by the monotonicity of v_n we get for $k^2 < n < (k+1)^2$

$$(4.11) \quad (\beta_{k^2})^{\left(\frac{k}{k+1}\right)^2} < \beta < (\beta_{(k+1)^2})^{\left(\frac{k+1}{k}\right)^2}$$

Thus Theorem 1 follows immediately from (4.10). The assertion of Theorem 1 can be restated in the following equivalent form:

Theorem 1'. If μ_N denotes the number of extreme elements in the first N elements of an infinite sample of a continuous population, then with probability 1

$$(4.12) \quad \lim_{N \rightarrow \infty} \frac{\mu_N}{\log N} = 1.$$

Theorem 1' is a special case of a general form of the laws of large numbers (cf. [3], [4], [5]), which says that for independent non-negative random variables η_k ($k = 1, 2, \dots$) the conditions

$$a) \quad \lim_{n \rightarrow \infty} A_n = +\infty$$

and

b) the sequence $\sum_{n=1}^{\infty} \frac{D_n^2}{A_n^2}$ is convergent (here $M_k = \mathbf{E}\eta_k$, $D_k = \mathbf{D}\eta_k$ and $A_n = \sum_{k=1}^n M_k$) imply that

$$(4.13) \quad \lim_{N \rightarrow \infty} \frac{\sum_{k=1}^N \eta_k}{A_N} = 1$$

with probability 1.

Applying the theorem for the variables $\eta_k = \varepsilon_k$ Theorem 1' follows, taking into account that in this case $A_N \sim \log N$ and $D_N^2 = \frac{1}{N} - \frac{1}{N^2}$ thus

$$\frac{D_N^2}{A_N^2} \sim \frac{1}{N \log^2 N}$$

i.e. conditions a) and b) of the above theorem hold. We note that the way we proved Theorem 1 is also appropriate for proving the above mentioned theorem.

§ 5. A CENTRAL LIMIT THEOREM FOR THE EXTREME ELEMENTS

In this § we prove the following theorem:

Theorem 2. *If v_n is the index of the n th extreme element of an infinite sample of a continuous population, then for any real x*

$$(5.1) \quad \lim_{n \rightarrow \infty} \mathbf{P} \left(\frac{\log v_n - n}{\sqrt{n}} < x \right) = \Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du.$$

Proof. By (4.2) Theorem 2 is equivalent to the following

Theorem 2'. *If μ_N denotes the number of extreme elements in the first N elements of an infinite sample of a continuous population, then for any real x*

$$(5.2) \quad \lim_{N \rightarrow \infty} \mathbf{P} \left(\frac{\mu_N - \log N}{\sqrt{\log N}} < x \right) = \Phi(x).$$

Now (5.2) follows immediately from the Ljapunov form of the central limit theorem (cf. [2]) since

$$\mu_N = \varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_N$$

where

$$\mathbf{E} \varepsilon_k = \frac{1}{k}$$

$$\mathbf{D}^2 \varepsilon_k = \frac{1}{k} - \frac{1}{k^2}$$

$$\mathbf{E} \left| \varepsilon_k - \frac{1}{k} \right|^3 = \left(\frac{1}{k} - \frac{1}{k^2} \right) \left(1 - \frac{2}{k} + \frac{2}{k^2} \right) \leq \frac{1}{k}$$

thus

$$\frac{\sqrt[3]{\sum_{k=1}^N \mathbf{E} \left| \varepsilon_k - \frac{1}{k} \right|^3}}{\sqrt{\sum_{k=1}^N \mathbf{D}^2 \varepsilon_k}} = O \left(\frac{1}{\sqrt[6]{\log N}} \right).$$

§ 6. AN ITERATED LOGARITHM THEOREM FOR THE EXTREME ELEMENTS

Theorem 3. *If v_n denotes the index of the n th extreme element of an infinite sample of a continuous population, then with probability 1*

$$(6.1) \quad \limsup_{n \rightarrow \infty} \frac{\log v_n - n}{\sqrt{2n \log \log n}} = +1$$

and

$$(6.2) \quad \liminf_{n \rightarrow \infty} \frac{\log v_n - n}{\sqrt{2n \log \log n}} = -1.$$

Theorem 3 is equivalent to the following

Theorem 3'. *If μ_N denotes the number of extreme elements among the first N elements of an infinite sample of a continuous population then with probability 1*

$$(6.3) \quad \limsup_{N \rightarrow \infty} \frac{\mu_N - \log N}{\sqrt{2 \log N \cdot \log \log \log N}} = +1$$

and

$$(6.4) \quad \liminf_{N \rightarrow \infty} \frac{\mu_N - \log N}{\sqrt{2 \log N \cdot \log \log \log N}} = -1.$$

Now Theorem 3' simply means that the iterated logarithm theorem applies for the independent variables ε_k ($k = 1, 2, \dots$) which is a consequence of the facts that the variables are bounded and the variance of μ_N tends to $+\infty$ (cf. [6]).

§ 7. ON THE DISTRIBUTION OF THE NUMBER OF CYCLES OF A RANDOM PERMUTATION

The random variable μ_N can also be interpreted as follows: we choose at random a permutation of the numbers $1, 2, \dots, N$ (each permutation has the same probability $\frac{1}{N!}$ to be chosen) and count how many of the numbers in this

permutation has the property that it is not preceded by a larger element (thus makes no inversion with a larger number) and denote by μ_N the number of such elements — called extremes in the following. Our results on the distribution of the random variable μ_N (i.e. the explicit formula (2.15), formula (2.8) for the generating function of μ_N the interpretation of this formula given in § 3 and Theorem 2') give answer, at the same time, to another problem concerning random permutations, namely for the determination of the distribution of the number of cycles in a random permutation. As a matter of fact we have the following relation:

Lemma 4. *Write γ_N for the number of cycles in a random permutation of the numbers $1, 2, \dots, N$, and μ_N for the number of extreme elements in a random permutation of the numbers $1, 2, \dots, N$, then γ_N and μ_N have the same distribution, i.e.*

$$(7.1) \quad \mathbf{P}(\gamma_N = k) = \mathbf{P}(\mu_N = k) \quad (k = 1, 2, \dots, N)$$

Proof. In order to establish Lemma 4 it is sufficient to construct a one-to-one mapping of the set of permutations of N elements onto itself which assigns a permutation Π' having k extreme elements to a permutation Π having k cycles. Such a mapping can be obtained as follows: represent the permutation Π as products of cycles and order the cycles in such a way that finding the largest element of each cycle we order the cycles in such a manner that their largest elements form an increasing sequence. Then we order the elements within a cycle in such a way that the cycle starts with its largest number. Now omitting the brackets separating the cycles, we get the permutation Π' assigned to the permutation Π . For instance, if $N = 9$ and Π is the permutation

$$5 \ 1 \ 3 \ 2 \ 7 \ 9 \ 8 \ 4 \ 6$$

then the representation of Π as the product of cycles arranged as prescribed above, is

$$\Pi = (3) \ (842157) \ (96)$$

and thus Π' is the permutation

$$384215796$$

It is clear that the number of extreme elements of Π' will be equal to the number of cycles of Π , since the largest elements of the cycles of Π will be the only extreme elements in Π' . The mapping is one-to-one since the representation of Π as product of cycles determines Π uniquely and our rules for the cycle representation have also been unique.

Thus we have proved that the generating function of γ_N is $H_N(x)$ [cf. (2.8)] further γ_N is normally distributed in limit with expectation $\log N$ and standard deviation $\sqrt{\log N}$. These results for the distribution of the number of cycles of permutations have already been known (cf. [7] and [8]); the above said can also serve as new proofs for these results.

μ_N has been represented as the sum of N independent random variables, the question naturally arises whether γ_N can also be represented as the sum of independent random variables, the k th taking the value 1 with probability $\frac{1}{k}$ and the value 0 with probability $1 - \frac{1}{k}$, in a combinatorically meaningful way. That this is possible, has been shown by W. Feller (cf. [7]).

§ 8. ON THE REPRESENTATION OF REAL NUMBERS BY MODIFIED AND ORDINARY ENGEL'S SERIES

In this § we prove the following theorem:

Theorem 4. *Let us make an infinite sample from a population having a continuous distribution and let $v_0 = 1, v_1, v_2, \dots, v_n, \dots$ be the indices of the extreme elements of the sample. Let*

$$(8.1) \quad \alpha = \frac{1}{v_1} + \sum_{n=2}^{\infty} \frac{1}{(v_1 - 1)(v_2 - 1) \dots (v_{n-1} - 1)v_n}.$$

Then the random variable α is uniformly distributed in the interval $(0, 1)$.

For proving Theorem 4 we need the following auxiliary statement

Lemma 5. *Let x be a positive number in the interval $(0, 1]$, then x can be uniquely represented in the form*

$$(8.2) \quad x = \frac{1}{k_1} + \sum_{n=2}^{\infty} \frac{1}{(k_1 - 1)(k_2 - 1) \dots (k_{n-1} - 1)k_n}$$

where $k_1, k_2, \dots, k_n$, is a strictly increasing infinite sequence of integers greater than 1. The above sequence can be determined as follows: let k_1 be the smallest integer exceeding $\frac{1}{x}$, if the numbers $k_1, k_2, \dots, k_{N-1}$ have already been chosen ($N = 2, 3, \dots$), then let k_N be the smallest integer for which

$$\frac{1}{k_1} + \sum_{n=2}^N \frac{1}{(k_1 - 1)(k_2 - 1) \dots (k_{n-1} - 1)k_n} < x.$$

Remark 1. The representation (8.2) is similar to the representation of real numbers by Engel's series, i.e. in the form

$$(8.3) \quad x = \sum_{n=1}^{\infty} \frac{1}{q_1 q_2 \dots q_n}$$

where the integers $q_1, q_2, \dots, q_n, \dots$ are greater than 1 and form a non-decreasing infinite sequence. Here the numbers q_n can be obtained by the following algorithm: q_1 is the smallest integer exceeding $\frac{1}{x}$, if $q_1, q_2, \dots, q_{N-1}$ have already been chosen ($N = 2, 3, \dots$), then let q_N be the smallest integer for which

$$\sum_{n=1}^N \frac{1}{q_1 q_2 \dots q_n} < x.$$

Due to the resemblance of the two procedures we call representation (8.2) the modified Engel's series of the number x .

Remark 2. If x is rational then it can also be represented in a form (8.2) with a finite sequence.

The proof of lemma 5. Applying the algorithm described in the lemma first we have $k_N > k_{N-1}$, since in view of the identity $\frac{1}{k} + \frac{1}{(k-1)k} = \frac{1}{k-1}$ the

converse assumption would imply that k_{N-1} could have been chosen smaller contradicting to the algorithm; on the other hand

$$(8.4) \quad \left| x - \frac{1}{k_1} - \sum_{n=2}^N \frac{1}{(k_1-1)(k_2-1)\dots(k_{n-1}-1)k_n} \right| \leq \frac{1}{(k_1-1)\dots(k_N-1)k_N}$$

and since $k_N > N$, the right-hand side of (8.4) tends to 0 as $N \rightarrow \infty$, i.e. (8.2) holds.

It is not hard to see that the representation (8.2) with an infinite sequence k_n is unique.

The proof of theorem 4. Let $1 < k_1 < k_2 < \dots < k_N$,

$$(8.5) \quad q_N = \frac{1}{k_1} + \sum_{n=2}^N \frac{1}{(k_1-1)\dots(k_{n-1}-1)k_n}$$

and

$$(8.6) \quad b_N = a_N + \frac{1}{(k_1-1)\dots(k_N-1)k_N}.$$

The probability that α belongs to the interval $(a_N, b_N]$ equals the probability that $v_1 = k_1, \dots, v_N = k_N$ holds and thus by (1.5) this probability is equal to

$$(8.7) \quad \frac{1}{(k_1-1)\dots(k_N-1)k_N} = b_N - a_N,$$

i.e. the length of the interval $(a_N, b_N]$. This implies that for an arbitrary interval $(a, b]$, $0 \leq a < b \leq 1$

$$(8.8) \quad \mathbf{P}(a < \alpha \leq b) = b - a,$$

for, every interval is the union of a finite or countably infinite number of disjoint intervals of the form $(a_N, b_N]$. This proves Theorem 4.

Theorem 4 can be interpreted as follows: if the number x is chosen at random with a uniform distribution in the interval $(0, 1]$ and the sequence of numbers k_n is defined by (8.2), then the random variables k_n , $n = 1, 2, \dots$ obey the statistical laws proved in §§ 1, 4, 5 and 6 for the variables v_n , e.g. the probability that a positive integer k ($k \geq 2$) occurs in the sequence k_n , is equal to $\frac{1}{k}$, for

almost all number x we have $\lim_{n \rightarrow \infty} \sqrt[n]{k_n} = e$, further if $E_n(y)$ denotes the set of numbers x ($0 \leq x \leq 1$) for which $\frac{\log k_n - n}{\sqrt[n]{n}} < y$, then the Lebesgue measure of $E_n(y)$ converges to $\Phi(y)$ as $n \rightarrow \infty$, etc.

The corresponding theorems for Engel's series are known: e.g. the limit theorem $\lim_{n \rightarrow \infty} \sqrt[n]{q_n} = e$ for almost all x is due to R. Borel [9], while the statement that the Lebesgue measure of the set of numbers x satisfying $\frac{\log q_n - n}{\sqrt[n]{n}} < y$

tends to $\Phi(y)$, is due to P. Lévy [10]. Detailed proofs for these theorems and some sharpenings can be found in [10]. Slightly generalizing the method of the present paper we can get new and much simpler proofs in case of ordinary Engel's series for the Borel's and Lévy's theorems and for the results due to P. Erdős, T. Szűsz and the author.

In fact, write $\varepsilon_k(x)$ for the number *how many times* the number k occurs among the denominators in the ordinary Engel's series of the real number x , i.e. in the sequence $q_n = q_n(x)$, $n = 1, 2, \dots$ defined in (8.3). It is easy to see that if x is a random variable uniformly distributed in the interval $(0, 1]$ then

$$(8.9) \quad \mathbf{P}(\varepsilon_k(x) = r) = \frac{k-1}{k^{r+1}} \quad (r = 0, 1, 2, \dots)$$

(cf. [10], theorem 1). It is also easy to see that the random variables $\varepsilon_k(x)$, $k = 1, 2, \dots$ are independent. This is so since the probability that $q_1(x) = q_1$, $q_2(x) = q_2, \dots, q_n(x) = q_n$ (here $q_1, q_2, \dots, q_n$ is a non-decreasing sequence of positive integers), is equal to

$$(8.10) \quad \frac{1}{q_1 q_2 \dots q_n (q_n - 1)}$$

and thus the probability that in the sequence $q_n(x)$, $n = 1, 2, \dots$ the number 2 occurs r_2 times, the number 3 r_3 times, $\dots$, the number k (exactly) r_k times, is

$$(8.11) \quad \mathbf{P}(\varepsilon_2 = r_2, \dots, \varepsilon_k = r_k) = \frac{1}{2^{r_2} 3^{r_3} \dots k^{r_k} (k-1)} -$$

$$- \frac{1}{2^{r_2} 3^{r_3} \dots (k-1)^{r_{k-1}} k^{r_k+1} (k-1)}$$

and thus

$$(8.12) \quad \mathbf{P}(\varepsilon_2 = r_2, \dots, \varepsilon_k = r_k) = \prod_{l=2}^k \frac{1}{l^{r_l}} = \prod_{l=2}^k \frac{l-1}{l^{r_l+1}},$$

therefore in view of (8.9) we have

$$(8.13) \quad \mathbf{P}(\varepsilon_2 = r_2, \dots, \varepsilon_k = r_k) = \prod_{l=2}^k \mathbf{P}(\varepsilon_l = r_l),$$

i.e. the variables $\varepsilon_2, \dots, \varepsilon_k$ are independent. Set

$$(8.14) \quad \mu_N(x) = \sum_{k=1}^N \varepsilon_k(x)$$

i.e. $\mu_N(x)$ denotes the number of elements in the sequence $q_1(x), q_2(x), \dots$ not exceeding N . Then we evidently have the identity

$$(8.15) \quad \mathbf{P}(\mu_N(x) \geq n) = \mathbf{P}(q_n(x) \leq N)$$

which implies that the limit relation

$$(8.16) \quad \lim_{n \rightarrow \infty} \sqrt[n]{q_n(x)} = e$$

is equivalent to the limit relation

$$(8.17) \quad \lim_{n \rightarrow \infty} \frac{\mu_N(x)}{\log N} = 1.$$

Now the general form of the laws of large numbers mentioned in § 4 implies that (8.17) holds for almost all x the same way as in the case of theorem 1'. The central limit theorem and the iterated logarithm theorem for the sequence $q_n(x)$ can be established similarly (cf. [11]). Thus, surprisingly enough, our investigations on the extreme elements of infinite samples have led to considerable simplifications of the theory of Engel's series. Finally we wish to make the following remark. Write $q_n(x)$, $n = 1, 2, \dots$ for the denominators in the ordinary Engel's series of the number x and let k_n^* denote the n -th number in order of magnitude occurring in the sequence $q_n(x)$, i.e. we cancel the repetitions in the sequence of numbers $q_n(x)$ thus keeping each occurring number only once; then the sequence k_n^* possesses the same statistical properties than the denominators k_n in the modified Engel's series, resp. the indices ν_n of the extreme elements in an infinite sample of a continuous population. Thus the theory of extreme elements is in direct connection with the ordinary Engel's series.

REFERENCES

- [1] Jordan, Ch.: *Calculus of finite differences*. Budapest, 1939.
- [2] Rényi, A.: *Valószínűségszámítás*. Tankönyvkiadó, Budapest, 1954.
- [3] Loève, M.: *Probability theory*. Van Nostrand, New York, 1955, 238.
- [4] Rényi, A.: A számjegyek eloszlása valós számok Cantor-féle előállításában. *Matematikai Lapok*, 7 (1956), 77–100.
- [5] Rényi, A.: A new axiomatic theory of probability. *Acta Math. Acad. Sci. Hung.*, 6 (1955), 185–336.
- [6] Kolmogoroff, A.: Über das Gesetz des iterierten Logarithmus. *Math. Ann.* 1927.
- [7] Feller, W.: *An introduction to probability theory and its applications*. New York, 1950. Ch. 10. § 7.
- [8] Riordan, J.: *An introduction to combinatorial analysis*. Wiley, New York, 1958, 70–71.
- [9] Borel, É.: Sur les développements unitaires normaux. *Comptes Rendus*, 225 (1947), 51.
- [10] Lévy, P.: Remarques sur un théorème de M. Émile Borel. *Comptes Rendus*, 225 (1947), 918–919.
- [11] Erdős, P., Rényi, A. and Szűsz, P.: On Engel's and Sylvester's series. *Annales Univ. Sci. Budapest, Sect. Math.*, 1 (1958), 7–32.
- [12] Wilks, S. S.: Recurrence of extreme observations. *Jour. Australian Math. Soc.*, 1 (1959), 106–122.
- [13] Gumbel, E. J.: The return period of order statistics. *Annals Inst. Statist. Math.*, 12 (1961), 249–256.

121, 160, 174, 175, 196, 204

NOTES

The following generalizations are given. In [1] the record times (the locations of the largest values (outstanding elements)) of a Markov chain (instead of independent random variables) are investigated. In [2] the properties of the locations of the m th largest values (instead of the largest values) are studied. [3] gives a law of iterated logarithm for $\Delta_r = V_r - V_{r-1}$ (interrecord time). A generalization of Lemma 2 is given in [4]. A multivariate version of the problem is studied in [5].

No. 196 is a French version of No. 194, No. 204 is nearly the same as No. 194. (P. R.)

REFERENCES

- [1] Strawderman, W. E. and Holmes, P. T.: On the law of the iterated logarithm for inter-record times. *J. Appl. Prob.*, 7 (1970), 432—439.
- [2] Pickands, I. III.: The two-dimensional Poisson processes and extremal processes. *J. Appl. Prob.*, 8 (1971), 745—756.
- [3] Resnick, S. I.: Asymptotic location and recurrence properties of maxima of a sequence of random variables defined on a Markov chain. *Z. Wahrscheinlichkeitstheorie verw. Geb.*, 18 (1971), 197—217.
- [4] Barndorff-Nielsen, O.: On the limit behaviour of extreme order statistics. *Annals of Math. Stat.*, 34 (1963), 992—1002.
- [5] Barndorff-Nielsen, O. and Sobel, M.: On the distribution of the number of admissible points in a vector random sample. *Теория вероятностей* 11 (1966), 283—305.

THREE NEW PROOFS AND A GENERALIZATION OF A THEOREM OF IRVING WEISS

by
A. RÉNYI

Dedicated to Prof. P. Erdős, at
his 50th birthday.

Introduction

Let us suppose that N balls are distributed at random among n boxes, so that each ball may fall into any box with the same probability $\frac{1}{n}$, independently of what happens to the other balls. Let $\zeta_{n,N}$ denote the number of boxes which remain empty. I. WEISS [1] has proved that if $n \rightarrow +\infty$ and $N = N(n)$ is a function of n such that $\lim_{n \rightarrow +\infty} \frac{N}{n} = \alpha > 0$ then $\zeta_{n,N}$ is in the limit normally distributed, its expectation and variance being asymptotically equal to $ne^{-\frac{N}{n}}$ and $ne^{-\frac{N}{n}} \left[1 - \left(1 + \frac{N}{n} \right) e^{-\frac{N}{n}} \right]$ respectively; by other words we have (denoting by $\mathbf{P}(\dots)$ the probability of the event in the brackets) for any real x

$$(1) \quad \lim_{\substack{n \rightarrow +\infty \\ \frac{N}{n} \rightarrow \alpha}} \mathbf{P} \left(\frac{\zeta_{n,N} - ne^{-\frac{N}{n}}}{\sqrt{ne^{-\frac{N}{n}} \left[1 - \left(1 + \frac{N}{n} \right) e^{-\frac{N}{n}} \right]}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du.$$

WEISS used the method of moments, which in this case leads to rather cumbersome calculations. In view of the simplicity of the question (which is in striking contrast with the difficulties of the proof) and the importance of its various possible practical applications, we considered it worth while trying to find a simpler proof.

We succeeded in finding three new proofs for the result of Weiss all using the method of characteristic functions. All these proofs are definitely simpler than that of I. WEISS, though a certain amount of subtle asymptotic analysis is indispensable. Besides their simplicity, these proofs are of a certain methodological interest, as they may serve as patterns for the solution of other similar problems.

These proofs yields also a more general result, namely that (1) remains valid also if $\frac{N}{n} \rightarrow 0$ or $\frac{N}{n} \rightarrow +\infty$ provided that

$$ne^{-\frac{N}{n}} \left(1 - \left(1 + \frac{N}{n} \right) e^{-\frac{N}{n}} \right) \rightarrow +\infty$$

(this is equivalent in case $\frac{N}{n} \rightarrow 0$ with $\frac{N^2}{n} \rightarrow +\infty$ and in case $\frac{N}{n} \rightarrow +\infty$ with $\frac{N}{n} - \log n \rightarrow -\infty$) We prove the generalization of the theorem of WEISS to the case $\frac{N}{n} \rightarrow +\infty$ $\frac{N}{n} - \log n \rightarrow -\infty$ by the second method, and the generalization to the case $\frac{N}{n} \rightarrow 0$, $\frac{N^2}{n} \rightarrow +\infty$ by the third method.

The problem in question is essentially that of proving the central limit theorem for certain not independent but weakly (and symmetrically) dependent random variables.) The situation is similar to that of sampling from a finite population (see [2]). The variables in question are the indicators of the emptiness of the different boxes; as a matter of fact $\zeta_{n,N}$ can be written in the form

$$\zeta_{n,N} = \varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_n$$

where ε_k is 1 or 0 according to whether the k -th box is empty or not ($k = 1, 2, \dots, n$). The dependence is in this case not negligible in the limit, as is seen from the formula for the variance.

As a matter of fact, the mean value of ε_k being $\left(1 - \frac{1}{n}\right)^N \sim e^{-\frac{N}{n}}$ if the dependence would be in the limit negligible, the variance would be asymptotically equal to $ne^{-\frac{N}{n}}(1 - e^{-\frac{N}{n}})$; while as mentioned above, the variance is definitely smaller (by the factor $1 - \frac{N}{n(e^{N/n} - 1)} < 1$) which shows that there is a not negligible negative correlation among the variables ε_k .

As a matter of fact, the variance $\mathbf{D}^2(\zeta_{n,N})$ of $\zeta_{n,N}$ is

$$\mathbf{D}^2(\zeta_{n,N}) = n^2 \left[\left(1 - \frac{2}{n}\right)^N - \left(1 - \frac{1}{n}\right)^{2N} \right] + n \left[\left(1 - \frac{1}{n}\right)^N - \left(1 - \frac{2}{n}\right)^N \right]$$

and therefore

$$\mathbf{D}^2(\zeta_{n,N}) = ne^{-\frac{N}{n}} \left[1 - \left(1 + \frac{N}{n}\right) e^{-\frac{N}{n}} \right] \cdot \left(1 + O\left(\frac{N}{n^2}\right)\right).$$

In § 1 we give the first proof which is worked out only for the case when $\frac{N}{n} \rightarrow \alpha > 0$. In § 2 we present the second proof. In § 3 we give the third proof and in § 4 add some remarks.

This paper was written during the stay of the author, as a visiting professor, at the Department of Statistics of the Michigan State University during the summer term of the year 1961. The author is indebted to Prof. H. RUBIN for calling his attention to the paper of I. WEISS.

§ 1. The first proof

Let $P_{n,N}(k)$ denote the probability that there are exactly k empty boxes if n denotes the total number of boxes and N the number of balls. By other words we put

$$P_{n,N}(k) = \mathbf{P}(\zeta_{n,N} = k) \quad (k = 0, 1, \dots, n).$$

The following two recursion formulae hold:

$$(2) \quad P_{n,N+1}(k) = P_{n,N}(k) \left(1 - \frac{k}{n}\right) + P_{n,N}(k+1) \frac{k+1}{n}$$

and

$$(3) \quad P_{n,N}(k) = P_{n-1,N}(k-1) \cdot \left(1 - \frac{1}{n}\right)^N + \sum_{l=1}^N \binom{N}{l} \frac{1}{n^l} \left(1 - \frac{1}{n}\right)^{N-l} \cdot P_{n-1,N-l}(k).$$

We obtain (2) by considering what happens if after throwing N balls into the boxes, one ball more is added: this may fall in a box which already contains a ball, or into an empty box. The two terms on the right correspond to these two possibilities.

As regards the less evident recursion formula (3) this can be obtained by the following argument: Let us label the boxes by the numbers $1, 2, \dots, n$ and let us denote by l the number of balls which fall into the first box. We distinguish between the cases $l = 0$ and $l \geq 1$. If $l = 0$ (the probability of which is $\left(1 - \frac{1}{n}\right)^N$) then the N balls are distributed among the remaining $n - 1$ boxes so that among these $k - 1$ boxes remain empty. This gives the first term on the right of (3). If however l is some positive integer, $1 \leq l \leq n$ (the probability of which is $\binom{N}{l} \frac{1}{n^l} \left(1 - \frac{1}{n}\right)^{N-l}$) then the remaining $N - l$ balls are distributed among $n - 1$ boxes so that k boxes remain empty. Thus we obtain the sum on the right of (3).

Now let us introduce the characteristic function $\varphi_{n,N}(t)$ of $\zeta_{n,N}$, i.e. we put

$$(4) \quad \varphi_{n,N}(t) = \sum_{k=0}^n P_{n,N}(k) e^{ikt}.$$

We obtain from (3) the recursion formula

$$(5) \quad \varphi_{n,N}(t) = \left(1 - \frac{1}{n}\right)^N \cdot e^{it} \cdot \varphi_{n-1,N}(t) + \sum_{l=1}^N \binom{N}{l} \frac{1}{n^l} \left(1 - \frac{1}{n}\right)^{N-l} \cdot \varphi_{n-1,N-l}(t).$$

Let us now introduce the generating function

$$(6) \quad G_n(t, z) = \sum_{N=0}^{\infty} \frac{\varphi_{n,N}(t) \cdot (nz)^N}{N!}.$$

We obtain from (5) easily

$$(7) \quad G_n(t, z) = G_{n-1}(t, z) (e^{it} + e^z - 1). \quad (n = 2, 3, \dots).$$

As evidently

$$(8) \quad \varphi_{1,N}(t) = \begin{cases} e^{it} & \text{for } N = 0 \\ 1 & \text{for } N \geq 1 \end{cases}$$

and thus

$$(9) \quad G_1(t, z) = e^{it} + e^z - 1$$

we obtain by (7) the surprisingly simple formula

$$(10) \quad G_n(t, z) = (e^{it} + e^z - 1)^n.$$

One can deduce (10) also from (2); as a matter of fact from (2) we get for G_n the partial differential equation $\frac{\partial G_n}{\partial z} = nG_n + \frac{e^{-it} - 1}{i} \frac{\partial G_n}{\partial t}$; taking into account that $G_n(t, 0) = \varphi_{n,0}(t) = e^{int}$, we get (10).

Now to prove (1) we apply the method of Laplace to obtain from (10) an asymptotic formula for $\varphi_{n,N}(t)$. We have by Cauchy's formula

$$(11) \quad \varphi_{n,N}(t) = \frac{N!}{n^N \cdot 2\pi i} \oint \frac{(e^{it} + e^z - 1)^n}{z^{N+1}} dz$$

where the integration may be carried out on any circle around the point $z = 0$.

We shall prove that putting

$$(12) \quad \alpha_n = \frac{N}{n}$$

and

$$(13) \quad D_n^2 = e^{-\frac{N}{n}} \left(1 - \left(1 + \frac{N}{n} \right) \cdot e^{-\frac{N}{n}} \right)$$

we have

$$(14) \quad \lim_{\substack{n \rightarrow +\infty \\ \frac{N}{n} \rightarrow a}} \varphi_{n,N} \left(\frac{t}{D_n \sqrt{n}} \right) \cdot e^{-\frac{itn \cdot e^{-a_n}}{D_n \sqrt{n}}} = e^{-\frac{t^2}{2}}.$$

((14) is clearly equivalent to (1)).

Let us choose as the path of integration in (11) the circle $|z| = \alpha_n$, by putting $z = \alpha_n \zeta$ with $\zeta = e^{iu}$ ($-\pi \leq u \leq +\pi$). Then we obtain, by Stirling's formula, putting $u = \frac{v}{\sqrt{n\alpha_n}}$

$$(15) \quad \varphi_{n,N} \left(\frac{t}{D_n \sqrt{n}} \right) \sim \frac{1}{\sqrt{2\pi}} \int_{-\pi\sqrt{n\alpha_n}}^{+\pi\sqrt{n\alpha_n}} E_n^n \cdot e^{-iv\sqrt{n\alpha_n}} dv$$

where

$$(16) \quad E_n = \left(e^{\frac{it}{D_n \sqrt{n}}} - 1 \right) \cdot e^{-a_n} + e^{a_n} \left(e^{\frac{iv}{\sqrt{n\alpha_n}}} - 1 \right).$$

Clearly for $\left| \frac{v}{\sqrt{n\alpha_n}} \right| \geq \delta > 0$ we have for $n \geq n_1$ (D_n and α_n being bounded from below by a positive constant)

$$(17) \quad E_n \leq q < 1$$

where q depends only on δ and α . It follows that

$$(18) \quad \lim_{n \rightarrow +\infty} \int_{\delta \sqrt{n\alpha_n} \leq |v| \leq \pi \sqrt{n\alpha_n}} |E_n|^n dv = 0.$$

On the other hand for $\sqrt[n]{n\alpha_n} \leq |v| \leq \delta \sqrt{n\alpha_n}$, in view of

$$(19) \quad |E_n|^2 = e^{2\alpha_n \left(\cos \frac{v}{\sqrt{n\alpha_n}} - 1 \right)} + 2e^{-2\alpha_n} \left(1 - \cos \frac{t}{D_n \sqrt{n}} \right) - \\ - 4e^{\alpha \left(\cos \frac{v}{\sqrt{n\alpha_n}} - 2 \right)} \cdot \sin \frac{t}{2\sqrt{n}} \sin \left(\frac{t}{2\sqrt{n}} - \frac{v}{\sqrt{n\alpha_n}} \right),$$

we get

$$(20) \quad |E_n|^2 \leq 1 - C_\delta \frac{v^2}{n} + O\left(\frac{t^2 + |tv|}{n}\right)$$

where $C_\delta > 0$ depends only on δ , which implies

$$(21) \quad \lim_{n \rightarrow +\infty} \int_{\sqrt[n]{n\alpha_n}}^{\delta \sqrt{n\alpha_n}} |E_n|^n dv = 0.$$

Thus we obtain from (13), (18) and (21)

$$(22) \quad \varphi_{n,N} \left(\frac{t}{D_n \cdot \sqrt{n}} \right) e^{-\frac{itne^{-\alpha_n}}{D_n \sqrt{n}}} \sim \frac{1}{\sqrt{2\pi}} \int_{-\sqrt[n]{n\alpha_n}}^{+\sqrt[n]{n\alpha_n}} E_n^n \cdot e^{-iv\sqrt{n\alpha_n} - \frac{itne^{-\alpha_n}}{D_n \sqrt{n}}} dv.$$

Now we get by an elementary calculation

$$(23) \quad E_n^n \cdot e^{-iv\sqrt{n\alpha_n} - \frac{itne^{-\alpha_n}}{D_n \sqrt{n}}} = e^{-\frac{t^2}{2} - \frac{\left(v - \frac{t\sqrt{\alpha_n}}{D_n} e^{-\alpha_n} \right)^2}{2}} + O\left(\frac{v^3}{\sqrt{n}}\right).$$

Thus it follows from (22) that (14) holds. As mentioned already, this proves (1).

§ 2. The second proof

In this § we give a second proof for (1) which leads at the same time to the following more general

Theorem 1. *If we distribute at random N balls among n boxes where $N = N(n)$ is a function of n such that $\frac{N(n)}{n}$ is bounded from below and $\lim_{n \rightarrow +\infty} \frac{N(n)}{n} - \log n \rightarrow -\infty$, then we have, putting $\alpha_n = \frac{N(n)}{n}$ for any real x*

$$\lim_{n \rightarrow +\infty} \mathbf{P} \left(\frac{\zeta_{n,N(n)} - ne^{-\alpha_n}}{\sqrt{ne^{-\alpha_n} [1 - (1 + \alpha_n) e^{-\alpha_n}]}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du.$$

Remark. In case $\alpha_n \rightarrow +\infty$ of course the result can be written also in the simpler form

$$\lim_{n \rightarrow +\infty} \mathbf{P} \left(\frac{\zeta_{n,N(n)} - ne^{-\alpha_n}}{\sqrt{ne^{-\alpha_n}}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du.$$

Proof. The idea of the proof which will be given in this § is one already applied in the paper [3]. Let us put

$$(24) \quad S_r = \mathbf{M} \left(\sum_{1 \leq k_1 < k_2 < \dots < k_r \leq n} \varepsilon_{k_1} \varepsilon_{k_2} \dots \varepsilon_{k_r} \right)$$

where $\mathbf{M}(\dots)$ denotes the expectation of the random variable in the brackets. Then evidently

$$(25) \quad S_r = \sum_{j=r}^n P_{n,N}(j) \binom{j}{r}$$

and thus

$$(26) \quad \sum_{r=0}^n S_r (x-1)^r = \sum_{j=0}^n P_{n,N}(j) x^j.$$

Now we can give a simple formula for S_r ; in fact we have

$$(27) \quad S_r = \binom{n}{r} \left(1 - \frac{r}{n} \right)^N$$

Thus we get for the characteristic function $\varphi_{n,N}(t)$ defined by (4) the explicit formula

$$(28) \quad \varphi_{n,N}(t) = \sum_{r=0}^n \binom{n}{r} \left(1 - \frac{r}{n} \right)^N (e^{it} - 1)^r.$$

Of course (28) can be deduced also directly from (11).

In order to prove theorem 1 we consider the function

$$(29) \quad \psi_{n,N}(t) = \varphi_{n,N} \left(\frac{t}{D_n \sqrt{n}} \right) e^{-\frac{it \sqrt{n} e^{-\alpha_n}}{D_n} \left(1 - \frac{N - n\alpha_n}{n} \right)}$$

where N is now not identical with $N(n)$, but is an independent nonnegative integral-valued variable. Then we have by (28), putting $y = e^{\frac{it}{D_n \sqrt{n}}}$,

$$(30) \quad \psi_{n,N}(t) = y^{-ne^{-\alpha_n}(1+\alpha_n)} \sum_{r=0}^n \binom{n}{r} \left(1 - \frac{r}{n}\right)^N (y-1)^r y^{Ne^{-\alpha_n}}.$$

It follows that putting

$$(31) \quad K_n(t) = \sum_{N=0}^{\infty} \psi_{n,N}(t) \frac{(\alpha_n \cdot n)^N e^{-\alpha_n \cdot n}}{N!}$$

we have

$$(32) \quad K_n(t) = e^{\alpha_n \cdot n(y^{e^{-\alpha_n}} - 1)} y^{-ne^{-\alpha_n}(1+\alpha_n)} (1 + (y-1)e^{-\alpha_n}y^{e^{-\alpha_n}})^n.$$

Now if α_n is bounded from below and $\alpha_n - \log n \rightarrow -\infty$ the right hand side of (32) can be evaluated as follows

$$(33) \quad K_n(t) \sim e^{-\frac{t^2}{2} + O\left(\frac{1}{\sqrt{n}}\right)}.$$

Thus we obtain

$$(34) \quad \lim_{n \rightarrow +\infty} K_n(t) = e^{-\frac{t^2}{2}}.$$

Now evidently $|\psi_{n,N}(t)| \leq 1$ and thus by the central limit theorem, if $\omega_n = \log(n\alpha_n)$ then we have

$$(35) \quad \lim_{n \rightarrow +\infty} \left| \sum_{|N - n\alpha_n| > \omega_n \sqrt{n\alpha_n}} \psi_{n,N}(t) \frac{(n\alpha_n)^N e^{-n\alpha_n}}{N!} \right| = 0$$

and

$$(36) \quad \lim_{n \rightarrow +\infty} \sum_{|N - n\alpha_n| \leq \omega_n \sqrt{n\alpha_n}} \frac{(n\alpha_n)^N e^{-n\alpha_n}}{N!} = 1.$$

We shall show now that for

$$(37) \quad |N - n\alpha_n| \leq \omega_n \sqrt{n\alpha_n}$$

we have

$$(38) \quad |\psi_{n,N}(t) - \psi_{n,N(n)}(t)| = O\left(\frac{\log^3 n}{\sqrt{n}}\right).$$

This implies by virtue of (34), (35) and (36) that

$$(39) \quad \lim_{n \rightarrow +\infty} \psi_{n,N(n)}(t) = e^{-t^2/2}.$$

As we have

$$(40) \quad \psi_{n,N(n)}(t) = \varphi_{n,N(n)}\left(\frac{t}{D_n \sqrt{n}}\right) e^{-\frac{it \sqrt{n} e^{-\alpha_n}}{D_n}}$$

it will follow from (39) that (14), and thus Theorem 1 holds.

Thus it remains only to prove (38). In view of (2) we obtain,

$$(41) \quad \psi_{n,N+1}(t) - \psi_{n,N}(t) = \left(e^{\frac{it e^{-a_n}}{D_n \sqrt{n}}} - 1 \right) \psi_{n,N}(t) + \frac{\left(e^{-\frac{it}{D_n \sqrt{n}}} - 1 \right)}{n} \sum_{k=1}^{\infty} P_{n,N}(k) k \cdot e_k$$

where

$$e_k = e^{\frac{it}{D_n \sqrt{n}} (k - n e^{-a_n(1+a_n)} + (N+1)e^{-a_n})}$$

Thus we obtain

$$(42) \quad \begin{aligned} \psi_{n,N+1}(t) - \psi_{n,N}(t) = & \left[e^{\frac{it e^{-a_n}}{D_n \sqrt{n}}} - 1 - \left(e^{-\frac{it}{D_n \sqrt{n}}} - 1 \right) \left(1 - \frac{1}{n} \right)^N \right] \psi_{n,N}(t) + \\ & + \frac{\left(e^{-\frac{it}{D_n \sqrt{n}}} - 1 \right)}{n} \sum_{k=0}^{\infty} P_{n,N}(k) \left(k - n \left(1 - \frac{1}{n} \right)^N \right) \cdot e_k. \end{aligned}$$

Thus we get for $|N - n \alpha_n| = O(\omega_n \sqrt{n \alpha_n})$

$$(43) \quad \begin{aligned} |\psi_{n,N+1}(t) - \psi_{n,N}(t)| = & O\left(\frac{(\log n)^{1/2}}{n}\right) + \\ & + O\left(\frac{1}{D_n \cdot n^{1/2}} \sum_{k=0}^{\infty} P_{n,N}(k) \cdot \left| k - n \left(1 - \frac{1}{n} \right)^N \right| \right). \end{aligned}$$

As clearly

$$(44) \quad \sum P_{n,N}(k) \left| k - n \left(1 - \frac{1}{n} \right)^N \right| \leq \mathbf{D}(\zeta_{n,N})$$

where $\mathbf{D}^2(\zeta_{n,N})$ denotes the variance of $\zeta_{n,N}$ and we have

$$\mathbf{D}^2(\zeta_{n,N}) \sim n D_n^2$$

it follows

$$|\psi_{n,N+1}(t) - \psi_{n,N}(t)| = O\left(\frac{(\log n)^{1/2}}{n}\right).$$

Thus if $|N - n \alpha_n| \leq \omega_n \sqrt{n \alpha_n}$ we have

$$(45) \quad |\psi_{n,N}(t) - \psi_{n, N(n)}(t)| = O\left(\frac{\log^3 n}{\sqrt{n}}\right).$$

This proves (39), and thus Theorem 1.

§ 3. The third proof

In this § we shall prove the following

Theorem 2. *If we distribute N balls at random among n boxes, where $N = N(n)$ is a function of n such that for $n \rightarrow +\infty$ $\frac{N(n)}{n}$ is bounded from above and*

$$(46) \quad \lim_{n \rightarrow +\infty} \frac{N^2(n)}{n} = +\infty,$$

and $\zeta_{n,N(n)}$ denotes the number of empty boxes, then we have, putting $\alpha_n = \frac{N(n)}{n}$ for any real x

$$(47) \quad \lim_{n \rightarrow +\infty} \mathbf{P} \left(\frac{\zeta_{n,N(n)} - ne^{-\alpha_n}}{\sqrt{ne^{-\alpha_n} [1 - (1 + \alpha_n) e^{-\alpha_n}]}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du.$$

Remark. In case $\alpha_n \rightarrow 0$, the result can be written in the simpler form

$$(47a) \quad \lim_{n \rightarrow +\infty} \mathbf{P} \left(\frac{\zeta_{n,N(n)} - ne^{-\alpha_n}}{\alpha_n \sqrt{\frac{n}{2}}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du$$

or, putting $\zeta_{n,N(n)}^* = \zeta_{n,N(n)} - n(1 - \alpha_n)$

$$(47b) \quad \lim_{n \rightarrow +\infty} \mathbf{P} \left(\frac{\zeta_{n,N(n)}^* - \frac{n\alpha_n^2}{2}}{\alpha_n \sqrt{\frac{n}{2}}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du.$$

Proof. Let us note first that putting

$$(48) \quad D_n^2 = e^{-\alpha_n} (1 - (1 + \alpha_n) e^{-\alpha_n})$$

our conditions on $N(n)$ imply that

$$(49) \quad \lim_{n \rightarrow +\infty} nD_n^2 = +\infty.$$

Let us introduce the random variables ν_k ($k = 1, 2, \dots$) defined as follows: ν_k is the least number such that after distributing ν_k balls among the n boxes, exactly k boxes will be occupied. Let us put further $\delta_1 = \nu_1$, $\delta_k = \nu_k - \nu_{k-1}$ ($k = 2, 3, \dots$). The random variables δ_k are clearly independent, and we have $\delta_1 \equiv 1$ and

$$(50) \quad \mathbf{P}(\delta_k = j) = \left(\frac{k-1}{n} \right)^{j-1} \left(1 - \frac{k-1}{n} \right) \quad (k = 2, 3, \dots).$$

It follows that the characteristic function of δ_k is

$$(51) \quad f_k(t) = \mathbf{M}(e^{it\delta_k}) = \frac{e^{it} \left(1 - \frac{k-1}{n} \right)}{1 - \left(\frac{k-1}{n} \right) e^{it}}$$

and thus the characteristic function of ν_k is

$$(52) \quad g_k(t) = \prod_{j=1}^k f_j(t) = \prod_{j=0}^{k-1} \frac{e^{it} \left(1 - \frac{j}{n} \right)}{1 - \frac{je^{it}}{n}}.$$

Let us calculate now the expectation and the variance of ν_k . We have evidently

$$(53) \quad \mathbf{M}(\delta_k) = \frac{n}{n-k+1}$$

and thus

$$(54) \quad \mathbf{M}(\nu_k) = \sum_{j=0}^{k-1} \frac{n}{n-j} = n \log \frac{n}{n-k} + O(1)$$

further

$$(55) \quad \mathbf{D}^2(\delta_k) = \frac{1}{\left(1 - \frac{k-1}{n}\right)^2} - \frac{1}{\left(1 - \frac{k-1}{n}\right)}$$

and thus

$$(56) \quad \mathbf{D}^2(\nu_k) = \frac{k}{1 - \frac{k}{n}} - n \log \frac{n}{n-k} + O(1).$$

Now we calculate the third absolute moment of δ_k . We have

$$(57) \quad \mathbf{M}\left(\left|\delta_k - \frac{n}{n-k+1}\right|^3\right) = O\left(\frac{k}{n}\right).$$

Thus Liapounoff's theorem can be applied to $\nu_k = \delta_1 + \delta_2 + \dots + \delta_k$ if $\frac{k}{\sqrt{n}} \rightarrow +\infty$.

It follows that if $k = k(n)$ is a function of n such that $\frac{k(n)}{\sqrt{n}} \rightarrow +\infty$ then for any real x

$$(58) \quad \lim_{n \rightarrow +\infty} \mathbf{P}\left[\frac{\nu_k - n \log \frac{1}{1 - \frac{k}{n}}}{\sqrt{\frac{\frac{k}{1 - \frac{k}{n}} - n \log \frac{1}{1 - \frac{k}{n}}}{1 - \frac{k}{n}}}} < x\right] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du.$$

Now let us take into account that

$$(59) \quad \mathbf{P}(\nu_k \leq N) = \mathbf{P}(\zeta_{n,N} \leq n-k).$$

Let us suppose that

$$(60) \quad N = n \log \frac{1}{1 - \frac{k}{n}} + x \sqrt{\frac{\frac{k}{1 - \frac{k}{n}} - n \log \frac{1}{1 - \frac{k}{n}}}{1 - \frac{k}{n}}} + O(1)$$

and solve this approximate equation approximately for k .

It is easy to see that we get

$$(61) \quad k = n(1 - e^{-\alpha_n}) - x \sqrt{ne^{-\alpha_n}(1 - (1 + \alpha_n)e^{-\alpha_n})} + O(1)$$

further $\frac{N^2}{n} \rightarrow +\infty$ implies $\frac{k^2}{n} \rightarrow +\infty$. Thus it follows from (58) and (59) that

$$(62) \quad \lim_{n \rightarrow +\infty} \mathbf{P} \left(\frac{\zeta_{n,N} - ne^{-\alpha_n}}{\sqrt{ne^{-\alpha_n}(1 - (1 + \alpha_n)e^{-\alpha_n})}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du.$$

This proves Theorem 2.

§ 4. Some remarks

Theorems 1 and 2 settle the question of the asymptotic distribution of the number of empty boxes if there are n boxes at all, and denoting by $N = N(n)$ the number of balls, $\frac{N(n)}{\sqrt{n}} \rightarrow +\infty$ and $\frac{N(n)}{n} - \log n \rightarrow -\infty$.

In the limiting case $\frac{N(n)}{n} - \log n \rightarrow \gamma$ with some real γ it can be proved by much more elementary methods that the number of empty boxes is in the limit distributed according to Poisson's law, with mean value $e^{-e^{-\gamma}}$ (see e.g. [4] and also [5].) If $\frac{N(n)}{n} - \log n \rightarrow +\infty$ then with probability tending to 1

there will be no empty boxes at all. On the other hand if $N = o(\sqrt{n})$ then it is almost sure that all balls are in different boxes and thus with probability tending to 1 the number of empty boxes will be exactly equal to $n - N$. Finally for $N \sim \delta \sqrt{n}$ with $\delta > 0$ the quantity $\zeta_{n,N} - n + N$ will have in the limit a Poisson distribution with mean value $\frac{\delta^2}{2}$. As these results are quite ele-

mentary, we do not go into details. We wanted only to point out that from the results of the present paper a complete picture is obtained concerning the behaviour of the distribution of $\zeta_{n,N}$ in the limit if $N = N(n)$ tends to infinity with $n \rightarrow +\infty$ in an arbitrary manner.

REFERENCES

- [1] WEISS, I.: "Limiting distribution in some occupancy problems". *Applied Math. and Stat. Laboratory, Stanford University. Technical Report No. 28*, 1955.
- [2] ERDŐS, P.—RÉNYI, A.: "On the central limit theorem for samples from a finite population". *MTA Mat. Kut. Int. Közl.* **4** (1959) 49—61.
- [3] ERDŐS, P.—RÉNYI, A.: "On the evolution of random graphs." *MTA Mat. Kut. Int. Közl.* **5** (1960) 17—61.
- [4] BERNSTEIN, S. N.: *Теория вероятностей*. Москва, 1946. p. 75—76.
- [5] RÉNYI, A.: *Wahrscheinlichkeitsrechnung*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1962.

NOTE

In connection with the classical occupancy problem there are two types of questions: (i) If N balls are thrown into n boxes, what is the probability to achieve a certain situation, for example what is the probability that the number of empty cells is 0; (ii) What can be said about the number N of balls which are needed to achieve a certain situation (with a big probability)?

No. 184 of Erdős and Rényi investigates the second question, No. 195 of Rényi considers the first one and shows the strong connection between the two types of questions. A lot of papers generalize both of the problems in different directions.

[1] and [2] are studying the number of urns containing m balls (instead of 0) in both cases. In [6] and [12] only the first question is treated but a complete survey of the distribution of the balls is given. In [5] the number of empty urns is investigated in connection with the second question.

The most popular generalization of these questions is the following: suppose that a ball is thrown into the i th urn with probability p_i ($\sum_{i=1}^n p_i = 1$) and the first ball thrown into the i th urn yields a gain a_i (if a ball is thrown into a non-empty urn the gain is 0). The total gain after throwing N balls is called bonus sum. The limit distribution of the bonus sum and the limit distribution of the waiting time to collect a given bonus sum are treated in [3], [7], [9], [11], [13] and [16]. Some of these papers allow to vary p_i and a_i in time. Clearly we get the original problems if $a_i = 1$, $p_i = 1/n$.

A common generalization of the problem of [1] and [2] and of the problem of the bonus sum is given in [6]. (P. R.)

REFERENCES

- [1] Békéssy, A.: On classical occupancy problems I. *Publications of the Math. Inst. of the Hung. Acad. of Sci.*, **8** (1963), 59—71.
- [2] Békéssy, A.: On classical occupancy problems II. (Sequential occupancy). *Publications of the Math. Inst. of the Hung. Acad. of Sci.*, **9** (1964), 133—141.
- [3] Pathak, P. K. and Sethuraman, I.: On the asymptotic distribution of the mean of distinct units in sampling from a finite population. *Publications of the Math. Inst. of the Hung. Acad. of Sci.*, **9** (1964), 113—115.
- [4] Севастьянов, Б. А. и Чистяков, В. П.: Асимптотическая нормальность в классической задаче о дробниках. *Теория вероятностей*, **9** (1964), 223—237.
- [5] Baum, L. E. and Billingsley, P.: Asymptotic distributions for the coupon collector's problem. *Annals of Math. Stat.*, **36** (1965), 1835—1839.
- [6] Викторова, Н. Н. и Чистяков, В. П.: Асимптотическая нормальность в задаче о дробниках произвольными попадания в ящики. *Теория вероятностей*, **10** (1965), 162—167.
- [7] Rosén, B.: On the control limit theorem for sums of dependent random variables. *Z. Wahrscheinlichkeitstheorie verw. Geb.*, **7** (1967), 48—82.
- [8] Samuel, E.: Sequential maximum likelihood estimation of the size of a population. *Annals of Math. Stat.*, **39** (1968), 1057—1068.
- [9] Rosén, B.: Asymptotic normality in a coupon collector's problem. *Z. Wahrscheinlichkeitstheorie verw. Geb.*, **13** (1969), 256—279.
- [10] Ailam, G.: The asymptotic distribution of the measure of random sets with application to the classical occupancy problem and suggestions for curve filling. *Annals of Math. Stat.*, **41** (1970), 427—434.
- [11] Rosén, B.: On the coupon collector's waiting time. *Annals of Math. Stat.*, **41** (1970), 1952—1969.

- [12] Ивченко, Г. И.: О предельных распределениях порядковых статистик полиномиальной схемы. *Теория вероятностей*, **16** (1971), 94—107.
- [13] Holst, L.: Limit theorems for some occupancy and sequential occupancy problems. *Annals of Math. Stat.*, **42** (1971), 1671—1680.
- [14] Holst, L.: Asymptotic normality in a generalized occupancy problem. *Z. Wahrscheinlichkeitstheorie verw. Geb.*, **21** (1972), 109—120.
- [15] Park, C. I.: A note on the classical occupancy problem. *Annals of Math. Stat.*, **43** (1972), 1698—1701.
- [16] Holst, L.: Some limit theorems with applications in sampling theory. *Annals of Stat.*, **1** (1973), 644—658.

On a Problem of A. Zygmund

P. Erdős and A. Rényi

Dedicated to Professor G. Pólya on his 75th birthday

1. Introduction

We shall consider in the present paper the theory of lacunary power series (and also Fourier series), an area of study in which Professor Pólya has made a number of important contributions—see, for example, his beautiful and already classical paper [1]. Many results of this theory may be characterized (somewhat vaguely) as follows: The behavior of a function $f(z)$ having a “sufficiently” lacunary power series is essentially the same on every arc of its circle of convergence (if the series has a finite radius convergence), or in every angle $\alpha \leq \arg z \leq \beta$ as $|z| \rightarrow +\infty$ (if it is an entire function). Among results of this type we mention only one.

Wiener [2] proved that if a lacunary power series

$$f(z) = \sum_{k=1}^{\infty} C_k z^{\lambda_k} \quad (\lambda_{k+1} - \lambda_k \rightarrow +\infty),$$

satisfies $\lim_{r \rightarrow 1} f(re^{i\vartheta}) = f(e^{i\vartheta})$ for $\alpha < \vartheta < \beta$ and $f(e^{i\vartheta}) \in L^2$ on the interval (α, β) , then $\lim_{r \rightarrow 1} f(re^{i\vartheta}) = f(e^{i\vartheta})$ exists almost everywhere, and $f(e^{i\vartheta}) \in L^2$ on the interval $[-\pi, \pi]$. This result can be formulated in the language of Fourier series as follows: consider a lacunary trigonometric series with gaps tending to $+\infty$, i.e., a series of the form

$$(1.1) \quad \sum_{k=1}^{\infty} a_k \cos \lambda_k x + b_k \sin \lambda_k x,$$

where λ_k is an increasing sequence of positive integers such that

$$(1.2) \quad \lim_{k \rightarrow +\infty} (\lambda_{k+1} - \lambda_k) = +\infty.$$

If such a series is Abel-summable almost everywhere in some interval (α, β) to a function $f(\vartheta)$ which belongs to the class $L^2(\alpha, \beta)$ for $-\pi \leq \alpha < \beta \leq \pi$, then (1.1) is the Fourier series of a function $f(\vartheta)$ in $L^2(-\pi, \pi)$; i.e., the series $\sum_{k=1}^{\infty} (a_k^2 + b_k^2)$ is convergent. Wiener's inequality for trigonometric polynomials, from which he deduced this result, has been generalized by Ingham [3] and by Turán [4]. For an elementary proof of a somewhat

weaker inequality see [5]. It follows particularly from Wiener's theorem that if (1.1) is the Fourier series of an L -integrable function $f(\vartheta)$ and $f(\vartheta)$ belongs to L^2 in (α, β) , then it belongs to L^2 in the whole interval.

About 20 years ago Zygmund suggested to the first-named author that he consider the problem of whether a similar result holds for the space L^q with $q \neq 2$ ($q > 1$), instead of the space L^2 . In other words, he asked, if the Fourier series (1.1) of $f(\vartheta) \in L$ is lacunary in the sense of (2.2) and if $f(\vartheta)$ belongs in the subinterval (α, β) to the space L^q , then does it follow that $f(\vartheta)$ belongs to L^q in the whole interval $[-\pi, \pi]$? The problem has so far remained unsolved, and Zygmund mentions it in his book [6, vol. I, p. 380] as an open question.

In Sec. 3 of this paper we shall show that the answer to Zygmund's query is negative for $q > 2$; i.e., the theorem of Wiener cannot be generalized for the space L^q ($q > 2$). We shall prove even more: There exist functions $f(\vartheta) \in L^2$ having a lacunary Fourier series which do not belong to any class L^q ($q > 2$) in the full interval $[-\pi, \pi]$ but which, however, are bounded in every closed subinterval of the interval $[-\pi, \pi]$ not containing the point $\vartheta = 0$.

We shall prove this by the use of probability theory. We consider a class of random lacunary Fourier series and prove that almost all series of this class have the above-mentioned properties. Thus our proof is not constructive; only the existence of a function (as a matter of fact, of an infinity of functions) having the required properties will be proved. Such a method has often been used in similar situations. Usually in such proofs the coefficients a_k, b_k are taken as random variables and the exponents λ_k are explicitly given (not random) numbers. In our proof, however, the coefficients a_k, b_k will be given numbers and the exponents λ_k will be positive, integer-valued random variables.

Lacunary random power series in which the exponents are random variables have already been used for a similar purpose in a previous joint paper [7] of the authors. The method used in this paper is essentially the same as that developed in [7], only it has been modified to some extent. The proof is based on a lemma presented in Sec. 2, similar to the lemma of [7]. The modification of the method is as follows: In the lemma of [7] we considered random exponents, each of which is uniformly distributed on a set of consecutive integers; in the lemma of Sec. 3, the exponents are random integers having a binomial distribution.

In Sec. 4 we consider some additional questions. For another related problem where a probabilistic method was also applied with success, see [10].

2. A Lemma on Random Cosine Polynomials

In this section we prove the following

LEMMA. *Let $d > 2$ and let $s < m_1 < m_2 < \dots < m_d$ be arbitrary positive integers. Let $\nu_1, \nu_2, \dots, \nu_d$ be independent random variables, each of which takes on the values $0, \pm 1, \pm 2, \dots, \pm s$ with the corresponding probabilities**

* Here and in what follows $P(\)$ denotes the probability of the event in the brackets.

$$(2.1) \quad P(\nu_j = l) = \binom{2s}{s+l} \frac{1}{2^{2s}} \quad (l = 0, \pm 1, \dots, \pm s; j = 1, \dots, d).$$

Put

$$(2.2) \quad C = \sum_{j=1}^d \cos(m_j + \nu_j)\varphi,$$

where $0 < |\varphi| \leq \pi$. Let ε be an arbitrary positive number with $0 < \varepsilon < \frac{1}{2}$. Then we have

$$(2.3) \quad P(C \geq d^{(1/2)+\varepsilon}) \leq 2 \exp\{-d^{2\varepsilon}/16\},$$

provided that

$$(2.4) \quad s \geq \frac{8 \log d}{\varphi^2}$$

and

$$(2.5) \quad d^\varepsilon \geq 2.$$

PROOF. The proof can be carried out by the method of S. Bernstein [9, pp. 162-65] (see also [7] and [8], where this method has been similarly applied).

Let t be a real number, $|t| \leq 1$. Then we have

$$(2.6) \quad M(e^{itC}) = \prod_{j=1}^d M(\exp\{it \cos(m_j + \nu_j)\varphi\}),$$

where $M(\ast)$ denotes the mean value of the random variable enclosed in parentheses. Since $|e^x - 1 - x| \leq |x|^2$ for $|x| \leq 1$, we have

$$(2.7) \quad M(\exp\{it \cos(m_j + \nu_j)\varphi\}) \leq 1 + |t| \cdot |M(\cos(m_j + \nu_j)\varphi)| + t^2.$$

Since by (2.1) clearly

$$(2.8) \quad M(\cos(m_j + \nu_j)\varphi) = (\cos m_j\varphi) \cdot \left(\cos \frac{\varphi}{2}\right)^{2s},$$

we obtain

$$(2.9) \quad M(e^{itC}) \leq \left[1 + |t| \left(\cos \frac{\varphi}{2}\right)^{2s} + t^2\right]^d \leq \exp\left\{d \left[|t| \left(\cos \frac{\varphi}{2}\right)^{2s} + t^2\right]\right\}.$$

Clearly, for $0 < t < 1$,

$$(2.10) \quad \begin{aligned} P(C \geq d^{(1/2)+\varepsilon}) \\ = P(\exp\{Ct\} \geq \exp\{td^{(1/2)+\varepsilon}\}) \leq \exp\{-td^{(1/2)+\varepsilon}\} M[\exp\{Ct\}]. \end{aligned}$$

From (2.9) and (2.10), we obtain

$$(2.11a) \quad \left. \begin{aligned} P(C \geq d^{(1/2)+\varepsilon}) \\ P(C \leq -d^{(1/2)+\varepsilon}) \end{aligned} \right\} \leq \exp\{d(t(\cos \varphi/2)^{2s} + t^2) - td^{(1/2)+\varepsilon}\}.$$

Thus for any t with $0 \leq t < 1$ we have

$$(2.11b) \quad P(|C| > d^{(1/2)+\varepsilon}) \leq 2 \exp\{t(d(\cos \varphi/2)^{2s} - d^{(1/2)+\varepsilon}) + dt^2\}.$$

Let us now choose t so as to minimize the right-hand side of (2.11b); that is, choose $t = \frac{1}{2}(d^{t-1/2} - (\cos \varphi/2)^{2t})$. We obtain

$$(2.12) \quad P(|C| \geq d^{(1/2)+\epsilon}) \leq 2 \exp \{-\frac{1}{4}[d^t - \sqrt{d}(\cos \varphi/2)^{2t}]^2\}.$$

By the inequality $(\cos \varphi/2)^2 \leq \exp\{-\varphi^2/16\}$, valid for $|\varphi| \leq \pi$, and in view of (2.4) and (2.5), we have $\sqrt{d}(\cos \varphi/2)^{2t} \leq \sqrt{d} \exp\{-s\varphi^2/16\} \leq 1 \leq d^t/2$, and thus we have from (2.12)

$$(2.13) \quad P(|C| \geq d^{(1/2)+\epsilon}) \leq 2 \exp\{-d^{2\epsilon}/16\};$$

thus our Lemma is proved.

3. A Class of Random Lacunary Fourier Series

We shall prove the following

THEOREM. *There exist real, even functions $f(\vartheta)$ defined in the interval $[-\pi, \pi]$ that have the following four properties:*

- (a) *$f(\vartheta)$ belongs to the class $L^1(-\pi, \pi)$;*
- (b) *the Fourier series of $f(\vartheta)$ is of the form*

$$(3.1) \quad f(\vartheta) \sim \sum_{j=1}^{\infty} a_j \cos \lambda_j \vartheta,$$

where the λ_j are positive integers such that

$$(3.2) \quad \lim_{j \rightarrow +\infty} (\lambda_{j+1} - \lambda_j) = +\infty;$$

- (c) *$f(\vartheta)$ is bounded for $\delta \leq |\vartheta| \leq \pi$ for every $\delta > 0$;*
- (d) *$f(\vartheta)$ does not belong to any class $L^q(-\pi, \pi)$ with $q > 2$.*

PROOF. Put

$$(3.3) \quad C_k(\vartheta) = \sum_{j=1}^{d_k} \cos(n_k + m_{kj} + \nu_{kj})\vartheta,$$

and

$$(3.4) \quad f(\vartheta) \sim \sum_{k=4}^{\infty} \frac{C_k(\vartheta)}{d_k^{(1/2)+\epsilon_k}},$$

where n_k, d_k , and m_{kj} are positive integers, defined as follows: $n_1 = 4$, $n_{k+1} = 2^{n_k}$ ($k = 1, 2, \dots$); $d_k = n_k/n_{k-1}^5$ ($k = 4, 5, \dots$) [evidently d_k is an integer for each $k \geq 4$]; and $m_{kj} = (j-1)n_{k-1}^4$ ($j = 1, \dots, d_k$; $k = 4, 5, \dots$). Let ϵ_k be defined by

$$\epsilon_k = \frac{n_{k-2}}{n_{k-1}} \quad \text{for } k = 4, 5, \dots.$$

Suppose also that ν_{kj} ($k = 1, 2, \dots$; $j = 1, 2, \dots, d_k$) are independent random variables having the distribution

$$(3.5) \quad P(\nu_{kj} = l) = \binom{2s_k}{s_k + l} \frac{1}{2^{2s_k}} \quad (l = 0, \pm 1, \dots, \pm s_k),$$

where $s_k = n_{k-1}^3$. Clearly, we have

$$(3.6) \quad \frac{1}{\pi} \int_{-\pi}^{\pi} f^2(\vartheta) d\vartheta = \sum_{k=4}^{\infty} \frac{d_k}{d_k^{1+4\epsilon_k}} = \sum_{k=4}^{\infty} \frac{1}{\exp \{ \log 2(4n_{k-2}^2 - 20n_{k-2}/n_{k-1}) \}}.$$

Since $\lim_{k \rightarrow +\infty} n_{k-2}^2/n_{k-1} = 0$, it follows that $f(\vartheta) \in L^2(-\pi, \pi)$. Let us put

$$(3.7) \quad N_k = n_k^{3/2} = 2^{3 \cdot 2^{n_k-2-1}}$$

and consider the polynomial $C_k(\vartheta)$ for $\vartheta = \vartheta_h = \pi h/N_k$, where h is any integer such that $N_k \delta_k \leq |h| \leq N_k$ and $\delta_k = 1/n_{k-1}$. Clearly, $d_k^{\epsilon_k} \geq 2$. Since $\pi^2 > 8$, we have $8 \log d_k/\vartheta^2 \leq s_k$ for $k \geq 4$. Thus we may apply our Lemma and obtain

$$(3.8) \quad P(|C_k(\vartheta_h)| \geq d_k^{(1/2)+\epsilon_k}) \leq 2 \exp \{-d_k^{2\epsilon_k}/16\}$$

for $N_k \delta_k \leq |h| \leq N_k$, and therefore

$$(3.9) \quad P(\max_{N_k \delta_k \leq |h| \leq N_k} |C_k(\vartheta_h)| \geq d_k^{(1/2)+\epsilon_k}) \leq 4N_k \exp \{-d_k^{2\epsilon_k}/16\}.$$

Now evidently for $|\vartheta_h - \vartheta| \leq \pi/N_k$ we have, in view of $m_{kd_k} + s_k < n_k$,

$$(3.10) \quad |C_k(\vartheta) - C_k(\vartheta_h)| \leq \frac{\pi}{N_k} \max_{\vartheta} |C_k'(\vartheta)| \leq \frac{2\pi d_k n_k}{N_k} < d_k^{1/2},$$

and thus we obtain

$$(3.11) \quad P(\max_{\pi \delta_k \leq |\vartheta| \leq \pi} |C_k(\vartheta)| \geq \frac{1}{2} d_k^{(1/2)+\epsilon_k}) \leq 4N_k \exp \{-d_k^{2\epsilon_k}/16\}.$$

As the series $\sum_{k=4}^{\infty} N_k \exp \{-d_k^{2\epsilon_k}/16\}$ is clearly convergent, it follows by the Borel-Cantelli lemma that with probability 1 the inequalities

$$(3.12) \quad \max_{\pi \delta_k \leq |\vartheta| \leq \pi} |C_k(\vartheta)| < \frac{1}{2} d_k^{(1/2)+\epsilon_k}$$

are satisfied except for a finite number of values of k ; i.e., inequality (3.12) holds for almost all series of the form (3.2) (equally for almost all choices of the random integers ν_{kj}).

It follows, in view of the convergence of the series $\sum 1/d_k^{\epsilon_k}$ and of $\delta_k \rightarrow 0$, that the series (3.2) is convergent for every ϑ with $0 < |\vartheta| \leq \pi$, also that the series is uniformly convergent in every closed subinterval of $[-\pi, \pi]$ which does not contain the point $\vartheta = 0$, and that its sum is bounded in every such interval. Thus we have already shown that almost all functions $f(\vartheta)$ defined by (3.2) satisfy conditions (a) and (c) of our Theorem. It is easy to see that condition (b) is always satisfied; as a matter of fact, the gaps of $C_k(\vartheta)$ are all at least equal to $n_{k-1}^4 - 2n_{k-1}^3$, and the gap between the greatest exponent of $C_{k-1}(\vartheta)$ and the least exponent of $C_k(\vartheta)$ is at least

$n_k - 2n_{k-1}$, and thus (3.2) is evidently satisfied. We even have $\lambda_j - \lambda_{j-1} > c \log^4 \lambda_j$ ($c > 0$). It remains to show that $f(\vartheta)$ also has property (d).

To prove this let us consider $f(\vartheta)$ for $\pi/n_k \leq \vartheta \leq 5\pi/4n_k$. For such values of ϑ we obviously have

$$(3.13) \quad \sum_{j=1}^{k-1} \frac{C_j(\vartheta)}{d_j^{(1/2)+2\varepsilon_j}} < k d_{k-1}^{1/2} < n_{k-1}^{1/2}.$$

We have also in view of $\pi/n_k \geq \pi\delta_{j+1} = \pi/n_j$ for $j \geq k$, with probability 1 for k sufficiently large,

$$(3.14) \quad \sum_{j=k-1}^{\infty} \frac{C_j(\vartheta)}{d_j^{(1/2)+2\varepsilon_j}} < \sum_{j=k+1}^{\infty} \frac{1}{d_j^{\varepsilon_j}} < 1.$$

Finally, we have for $\pi/n_k \leq \vartheta \leq 5\pi/4n_k$ and for sufficiently large k

$$(3.15) \quad |C_k(\vartheta)| \geq \frac{d_k}{\sqrt{2}} - 2 \sum_{j=1}^{d_k} |\sin(m_{kj} + \nu_{kj})\vartheta| \geq \frac{d_k}{\sqrt{2}} - \frac{20\pi}{n_{k-1}} \geq \frac{d_k}{2}.$$

Thus we obtain from (3.13)–(3.15)

$$(3.16) \quad |f(\vartheta)| \geq \frac{1}{2} d_k^{(1/2)-2\varepsilon_k} - 1 - n_{k-1}^{1/2} > \frac{1}{4} d_k^{(1/2)-2\varepsilon_k}$$

for $\pi/n_k \leq \vartheta \leq 5\pi/4n_k$ and sufficiently large k .

Now let $q > 2$ be arbitrary but fixed. It follows that for sufficiently large k one has $q(\frac{1}{2} - 2\varepsilon_k) > 1 + \rho$, where $\rho = (q - 2)/4 > 0$, and thus

$$(3.17) \quad \int_{\pi/n_k}^{5\pi/4n_k} |f(\vartheta)|^q d\vartheta > \frac{\pi n_k^{\rho}}{4^{q+1} n_{k-1}^{5(1+\rho)}}.$$

As the right-hand side of (3.16) tends to $+\infty$ for $k \rightarrow +\infty$, it follows that

$$\int_{-\pi}^{\pi} |f(\vartheta)|^q d\vartheta = +\infty. \quad \text{Q.E.D.}$$

One can even prove somewhat more. As a matter of fact, it follows from (3.16) that if $\alpha > 9$,

$$\lim_{k \rightarrow +\infty} \int_{\pi/n_k}^{5\pi/4n_k} f^2(\vartheta) \log^{\alpha} |f(\vartheta)| d\vartheta = +\infty.$$

Thus not even $f^2(\vartheta) \log^{9+\varepsilon} |f(\vartheta)|$ is integrable if $\varepsilon > 0$.

4. Some Remarks on Additional Problems

It seems that our method is not applicable in the case $1 < q < 2$. As a matter of fact, to settle this case one has to consider series of the form (1.1) with $\sum (a_k^2 + b_k^2) = +\infty$, and in this case if we choose the exponents at random we cannot even be sure of obtaining a Fourier series.

Another open question is how rapidly the exponents of a series of the form (1.1) can increase so that the series will still have properties (a)–(d). As is well known (see [6]), if $\lambda_{k+1}/\lambda_k \geq \lambda > 1$, that is, if (1.1) is a series with Hadamard gaps, then if $f(\vartheta)$ belongs to L^2 (i.e., $\sum (a_k^2 + b_k^2) < +\infty$), it

also belongs to L^q for every q . Thus certainly λ_k cannot increase exponentially. By modifying our construction, we could get series having properties (a) – (d) with $\lambda_{j+1} - \lambda_j > (\log \lambda_j)^A$ with arbitrarily large A . Our method is not applicable in the case where $\lambda_{j+1} - \lambda_j > \lambda_j^B$ with $0 < B < 1$. It may be true, however, that if the function is bounded in a subinterval (α, β) , then it belongs to $L^q(-\pi, \pi)$ for some $q > 2$ if $\lambda_{j+1} - \lambda_j > \lambda_j^\alpha$ for some $\alpha > 0$. If $\lambda_{j+1} - \lambda_j > \lambda_j^\alpha$ for every $\alpha < 1$ if $j > j_0(\alpha)$, then perhaps it belongs to $L^q(-\pi, \pi)$ for every q .

Finally, we may ask whether for every function $\omega(x)$ tending monotonically to $+\infty$ for $x \rightarrow +\infty$ there exists a function $f(\vartheta)$ which has properties (a), (b), and (c) and is such that $f^2(\vartheta)\omega(|f(\vartheta)|)$ is not integrable. As we mentioned at the end of Sec. 3, our functions $f(\vartheta)$ are such that

$$\int_{-\pi}^{\pi} f^2(\vartheta) \log^\alpha |f(\vartheta)| d\vartheta$$

is divergent for $\alpha > 9$. By modifying the construction, the value 9 could be replaced by a smaller one, but our method is not suitable to deal with the case of arbitrarily slowly increasing functions $\omega(x)$.

REFERENCES

- [1] PÓLYA, G., Lücken und Singularitäten von Potenzreihen, *Math. Zeit.*, **29** (1929), 549–640.
- [2] WIENER, N., A Class of Gap Theorem, *Annali di Pisa*, **3** (1934), 367–72.
- [3] INGHAM, A. E., Some Trigonometric Inequalities with Applications to the Theory of Series, *Math. Zeit.*, **41** (1936), 367–69.
- [4] TURÁN, P., On an Inequality, *Annal. Univ. Sci. R. Eötvös*, Budapest, **1** (1958), 3–6.
- [5] MARCZINKIEWICZ, J., and A. ZYGMUND, Proof of a Gap Theorem, *Duke Math. J.*, **4** (1938), 469–72.
- [6] ZYGMUND, A., *Trigonometric Series*. Cambridge: Cambridge Univ. Press, 1959.
- [7] ERDÖS, P., and A. RÉNYI, On Singular Radii of Power Series, *Pub. Math. Inst. Hung. Acad. Sci.*, **3** (1958), 159–70.
- [8] ERDÖS, P., and A. RÉNYI, Probabilistic Approach to Some Problems of Diophantine Approximation, *Illinois J. Math.*, **1** (1957), 303–15.
- [9] BERNSTEIN, S., *Teoria Veroiatnostei* (Theory of probability), 4th ed. Moscow: 1946.
- [10] NORDLANDER, A., Studies in Exponential Polynomials (Ph.D. Dissertation), Univ. Uppsala, Sweden, 1961.

NOTE

The general problem mentioned in the first few lines of the paper is due to S. Mandelbrojt in 1935. As to the problem of lacunarity raised in 4. P. Turán solved in the same volume this problem positively for $q > 6$ at least by exhibiting an *explicit* example of the required type with $B = \frac{1}{q+6}$. His construction was modified afterwards by S. Knapowski to give a required explicit example for $q > 3$. This problem of Erdős—Rényi for $2 < q < 3$, further Zygmund's original problem for $1 < q < 2$ are unsolved sofar. As Rényi mentions in his paper No. 282, J. Katznelson has also communicated him another explicit example for all sufficiently large q 's. (P. T.)

A NEW APPROACH TO THE THEORY OF ENGEL'S SERIES

By

A. RÉNYI

Mathematical Institute of the Hungarian Academy of Sciences

(Received February 18, 1962)

Introduction

In a previous joint paper with P. ERDŐS and P. SZÜSZ in this journal ([1]) we have given detailed proofs of certain results on Engel's series for the representation of real numbers, due originally to É. BOREL [2] and P. LÉVY [3]. Recently I have found a new approach to these theorems which leads to a much simpler proof of these results. The new approach consists in introducing a certain sequence of independent random variables, by means of which all the quantities in question can be expressed in a simple way. The mentioned theorems are obtained as direct consequences of well known general theorems on the sum of independent random variables. This is an essential simplification compared with [1] where the same results have been obtained by the rather difficult technique of dealing with sums of almost independent random variables.

In § 1 we give the definition of Engel's series, and collect certain simple formulas, all of which have already been given in [1], which will be needed in the sequel. In § 2 we introduce the mentioned independent random variables. In § 3 we show how Theorems 2, 3 and 4 of [1] can be obtained as special cases of well known limit theorems of probability theory. In § 4 we prove by the same method some new results on Engel's series. These are obtained by combining the method of the present paper by some previous results of the author (see [4]). Finally in § 5 we discuss a modification of Engel's representation of real numbers, which we call *modified Engel's series*. For these series similar results hold as for ordinary Engel's series. A similar simple approach to the corresponding theory of Sylvester's series, given in [1] is still lacking.

§ 1. Engel's representation of real numbers

Let x be an arbitrary real number in the interval $(0, 1]$. Then x can be represented in the form of the infinite series

$$(1.1) \quad x = \frac{1}{q_1} + \frac{1}{q_1 q_2} + \dots + \frac{1}{q_1 q_2 \dots q_n} + \dots$$

where $q_1, q_2, \dots, q_n, \dots$ is a nondecreasing sequence of positive integers ≥ 2 , which can be obtained by the following algorithm: we choose for q_1 the least positive integer for which $\frac{1}{q_1} < x$; for q_2 the least positive integer for

which $\frac{1}{q_1} + \frac{1}{q_1 q_2} < x$, and in general (for $n=2, 3, \dots$) if $q_1, q_2, \dots, q_n$ have already been determined we choose for q_{n+1} the least positive integer for which $\frac{1}{q_1} + \frac{1}{q_1 q_2} + \dots + \frac{1}{q_1 q_2 \dots q_n q_{n+1}} < x$. This algorithm ensures that q_n is a non-decreasing sequence, further that

$$(1.2) \quad \left| x - \sum_{n=1}^N \frac{1}{q_1 q_2 \dots q_n} \right| < \frac{1}{q_1 q_2 \dots q_N (q_N - 1)},$$

which implies that (1.1) holds.

Clearly the n -th denominator q_n is a well defined function of x , that is $q_n = q_n(x)$. If we suppose now that x is a random variable, uniformly distributed in the interval $(0,1]$, then $q_n = q_n(x)$ is a random variable too ($n=1, 2, \dots$). It was shown in [1] that the sequence $\{q_n\}$ is a homogeneous Markov chain with transition probabilities

$$(1.3) \quad P(q_{n+1} = k | q_n = j) = \frac{j-1}{k(k-1)} \quad (n = 1, 2, \dots)$$

where k and j are arbitrary positive integers satisfying $k \geq j \geq 2$, and the (unconditional) distribution of q_1 is given by

$$(1.4) \quad P(q_1 = k) = \frac{1}{k(k-1)} \quad (k = 2, 3, \dots).$$

(Here and in what follows $P(A)$ denotes the probability of the event A and $P(A|B)$ the conditional probability of the event A under condition B).

§ 2. The basic independent variables

Let $\varepsilon_k = \varepsilon_k(x)$ ($k=2, 3, \dots$) denote the number of times the integer k occurs in the sequence $q_n = q_n(x)$ ($n=1, 2, \dots$). As the sequence q_n is non-decreasing, it follows that $\varepsilon_k = r$ means that there exists a nonnegative integer j such that

$$(2.1) \quad \begin{array}{lll} q_n < k & \text{for}^* & n \leq j, \\ q_n = k & \text{for} & n = j+1, j+2, \dots, j+r, \\ q_n > k & \text{for} & n > j+r. \end{array}$$

The probability distribution of ε_k can be easily obtained. As a matter of fact this has already been done in [1] (Theorem 1). We obtain by (1.3)

$$(2.2) \quad P(\varepsilon_k \geq r) = \frac{1}{k^r(k-1)} \prod_{i=2}^{k-1} \frac{1}{1 - \frac{1}{i}} = \frac{1}{k^r},$$

* if $j=0$ then there is of course no $n \leq j$ for which q_n is defined.

and as evidently

$$(2.3) \quad P(\varepsilon_k = r) = P(\varepsilon_k \geq r) - P(\varepsilon_k \geq r+1)$$

it follows

$$(2.4) \quad P(\varepsilon_k = r) = \frac{k-1}{k^{r+1}} \quad (r = 0, 1, 2, \dots; k = 2, 3, \dots).$$

Now what escaped our attention when writing the paper [1] is the fact that the random variables $\varepsilon_2, \varepsilon_3, \dots, \varepsilon_k, \dots$ are independent.

This can be shown as follows: Let $r_2, r_3, \dots, r_n$ be arbitrary nonnegative integers, then again by (1.3)

$$(2.5) \quad P(\varepsilon_2 = r_2, \varepsilon_3 = r_3, \dots, \varepsilon_{n-1} = r_{n-1}, \varepsilon_n \geq r_n) = \frac{1}{2^{r_2} \cdot 3^{r_3} \cdot \dots \cdot (n-1)^{r_{n-1}} n^{r_n}}$$

and thus

$$(2.6) \quad P(\varepsilon_2 = r_2, \varepsilon_3 = r_3, \dots, \varepsilon_n = r_n) = \frac{n-1}{n} \prod_{k=2}^n \frac{1}{k^{r_k}} = \prod_{k=2}^n \frac{(k-1)}{k^{r_k+1}}.$$

Compared with (2.4) it follows that

$$(2.7) \quad P(\varepsilon_2 = r_2, \dots, \varepsilon_n = r_n) = \prod_{k=2}^n P(\varepsilon_k = r_k)$$

which makes the independence of the variables $\varepsilon_2, \varepsilon_3, \dots, \varepsilon_k, \dots$ obvious.

Thus we have proved the following

THEOREM 1. *If ε_k ($k=2, 3, \dots$) denotes how many times the number k occurs in the sequence of denominators q_n ($n=1, 2, \dots$) of Engel's series of a random real number x , uniformly distributed in the interval $(0, 1]$, then the random variables ε_k are independent and the distribution of ε_k is given by (2.4).*

Let us calculate the mean value, the variance and the third absolute central moment of the random variable ε_k . (Here and in what follows we denote by $M(\zeta)$ the mean value and by $D^2(\zeta)$ the variance of the random variable ζ .)

We clearly have for $k=2, 3, \dots$

$$(2.8) \quad M(\varepsilon_k) = \frac{1}{k-1},$$

$$(2.9) \quad D^2(\varepsilon_k) = \frac{1}{k-1} + \frac{1}{(k-1)^2},$$

$$(2.10) \quad M[|\varepsilon_k - M(\varepsilon_k)|^3] \leq \frac{C}{k-1},$$

where C is a positive constant, not depending on k .

§ 3. Limit theorems on the denominators of Engel's series

Let $\mu_N = \mu_N(x)$ denote the number of terms of the sequence $q_n = q_n(x)$ which are $\leq N$. By other words, let us put

$$(3.1) \quad \mu_N = \sum_{k=2}^N \varepsilon_k.$$

Then clearly in view of (2.8), (2.9) and (2.10) and Theorem 1

$$(3.2) \quad M(\mu_N) = \sum_{j=1}^{N-1} \frac{1}{j} \sim \log N,$$

$$(3.3) \quad D^2(\mu_N) = \sum_{j=1}^{N-1} \left(\frac{1}{j} + \frac{1}{j^2} \right) \sim \log N$$

and

$$(3.4) \quad \sqrt[3]{\sum_{k=2}^N M[|\varepsilon_k - M(\varepsilon_k)|^3]} = O(\sqrt[3]{\log N})$$

Thus in view of Theorem 1. Liapounoff's form of the central limit law is applicable, and we get

THEOREM 2a. *For every real y we have*

$$(3.5) \quad \lim_{N \rightarrow +\infty} P\left(\frac{\mu_N - \log N}{\sqrt[3]{\log N}} < y\right) = \Phi(y)$$

where

$$(3.6) \quad \Phi(y) = \frac{1}{\sqrt[3]{2\pi}} \int_{-\infty}^y e^{-u^2/2} du.$$

As clearly

$$(3.7) \quad P(\mu_N < n) = P(q_n > N).$$

Theorem 2a can be written in the following equivalent form

THEOREM 2c. *For every real y*

$$(3.8) \quad \lim_{n \rightarrow +\infty} P\left(\frac{\log q_n - n}{\sqrt[3]{n}} < y\right) = \Phi(y).$$

Theorem 2c is identical with Theorem 2 of [12] and is originally due to P. LÉVY.

To prove the strong law of large numbers for the random variables ε_k we need the following general form of this law: *If $\xi_1, \xi_2, \dots, \xi_N, \dots$ are inde-*

pendent, nonnegative random variables with finite mean values $M_k = \mathbf{M}(\xi_k)$ and variances $D_k^2 = \mathbf{D}^2(\xi_k)$, and if putting $A_N = \sum_{k=1}^N M_k$ one has

$$(3.9) \quad \lim_{N \rightarrow +\infty} A_N = +\infty,$$

and further

$$(3.10) \quad \sum_{N=1}^{\infty} \frac{D_N^2}{A_N^2} < +\infty$$

then with probability 1 one has

$$(3.11) \quad \lim_{N \rightarrow +\infty} \frac{\sum_{k=1}^N \xi_k}{A_N} = 1.$$

This theorem follows easily from the three-series theorem of A. N. KOLMOGOROFF and KRONECKER's lemma.

(See [5], [6], [7]). The conditions of this theorem are clearly fulfilled for $\xi_k = \varepsilon_k$, in view of the fact that the series $\sum_{N=3}^{\infty} \frac{1}{N \log^2 N}$ is convergent. Thus we obtain

THEOREM 3a. *We have with probability 1 (i. e. for almost all x)*

$$(3.12) \quad \lim_{N \rightarrow +\infty} \frac{\mu_N}{\log N} = 1.$$

In view of $\mu_{q_n} = n$ Theorem 3a is equivalent with

THEOREM 3b. *We have with probability 1*

$$(3.13) \quad \lim_{n \rightarrow +\infty} \sqrt[n]{q_n} = e.$$

Theorem 3b is identical with Theorem 3 of [1] and is originally due to E. BOREL.

Similarly, as the conditions given by A. N. KOLMOGOROFF [8] for the law of the iterated logarithm are evidently fulfilled for the variables ε_k , we obtain

THEOREM 4a. *We have with probability 1 (i. e. for almost all x)*

$$(3.14) \quad \limsup_{N \rightarrow +\infty} \frac{\mu_N - \log N}{\sqrt{2 \log N \cdot \log \log \log N}} = +1 \quad \text{and} \quad \liminf_{N \rightarrow +\infty} \frac{\mu_N - \log N}{\sqrt{2 \log N \cdot \log \log \log N}} = -1$$

or equivalently

THEOREM 4b. *We have with probability 1 (i. e. for almost all x)*

$$(3.15) \quad \limsup_{n \rightarrow +\infty} \frac{\log q_n - n}{\sqrt{2n \cdot \log \log n}} = +1 \quad \text{and} \quad \liminf_{n \rightarrow +\infty} \frac{\log q_n - n}{\sqrt{2n \cdot \log \log n}} = -1.$$

Theorem 4b is identical with Theorem 4 of [1], due also to P. LÉVY, which was proved in [1] in a rather cumbersome way; here we obtain this result without any effort as a special case of a well-known general theorem.

§ 4. Some further results

We first prove the following theorem, which is a simple consequence of the Borel-Cantelli lemma.

THEOREM 5. *Let $2 \leq k_1 < k_2 < \dots < k_j < \dots$ be an increasing sequence of positive integers. Then the sequence $q_n = q_n(x)$ contains for almost all x infinitely many or only a finite number of terms of the sequence $k_j (j=1, 2, \dots)$ according to whether the series $\sum_{j=1}^{\infty} \frac{1}{k_j}$ is divergent or convergent.*

PROOF OF THEOREM 5. Let A_k denote the event that the number k is contained (at least once) in the sequence q_n . Then by Theorem 1 the events A_k are independent and

$$(4.1) \quad P(A_k) = P(\varepsilon_k \geq 1) = \frac{1}{k}.$$

Thus Theorem 5 follows immediately by the Borel-Cantelli lemma.

Especially it follows that for almost all x there are infinitely many primes in the sequence $q_n(x)$.

Let us consider now the following problem: what is the probability that the sequence $q_n(x)$ is strictly increasing for $n \geq n_0(x)$.

This question is answered by

THEOREM 6. *For almost all x the sequence $q_n(x)$ is strictly increasing for $n \geq n_0(x)$ where $n_0(x)$ depends on x .*

PROOF OF THEOREM 6. Let B_k denote the event that the number k occurs more than once in the sequence $q_n(x)$. Clearly the events B_k are independent and

$$(4.2) \quad P(B_k) = P(\varepsilon_k \geq 2) = \frac{1}{k^2}.$$

Thus the series

$$(4.3) \quad \sum_{k=2}^{\infty} P(B_k)$$

is convergent, and Theorem 6 follows also from the Borel-Cantelli lemma.

The least number $\kappa(x)$ having the property that no number $k > \kappa(x)$ occurs more than once in the sequence $q_n(x)$ is a random variable, and it is not difficult to obtain its distribution. As a matter of fact we have

$$(4.4) \quad P[\kappa(x) = k] = \frac{1}{k^2} \prod_{j=k+1}^{\infty} \left(1 - \frac{1}{j^2}\right).$$

As by an easy calculation

$$(4.5) \quad \sum_{k=2}^{\infty} P[\kappa(x) = k] = \sum_{k=2}^{\infty} \frac{1}{k^2} \prod_{j=k+1}^{\infty} \left(1 - \frac{1}{j^2}\right) = \frac{1}{2}$$

it follows that the probability of $\kappa(x) = 1$ is $1/2$. By other words, $1/2$ is the probability that q_n is strictly increasing from the very beginning.

Now let us drop our assumption that x is uniformly distributed in the interval $(0, 1]$ and replace this assumption by the supposition that x has an arbitrary absolutely continuous distribution in $(0, 1]$. As the random variables ε_k are independent, we can apply the theorem (see [4]) that if for a sequence of independent random variables a limit distribution theorem holds, then the assertion of this theorem remains valid if we replace the probability measure on the underlying probability space by a new measure which is absolutely continuous with respect to the original measure.

Thus it follows that the assertions of Theorems 2b and 3b and thus also those of Theorems 2a and 3a remain valid if x is a random variable having an arbitrary absolutely continuous distribution in the interval $(0, 1]$. Especially x may be uniformly distributed in an arbitrary subinterval (α, β) of $(0, 1]$.

§ 5. Modified Engel's series

In this § we consider the representation of a real number $x(0 < x \leq 1)$ in the form

$$(5.1) \quad x = \frac{1}{m_1} + \frac{1}{(m_1 - 1)m_2} + \dots + \frac{1}{(m_1 - 1)(m_2 - 1) \dots (m_{n-1} - 1)m_n} + \dots$$

where m_n is a *strictly increasing* sequence of positive integers, ≥ 2 which is defined as follows: we choose for m_1 the least positive integer for which $\frac{1}{m_1} < x$; evidently $m_1 \geq 2$; if m_1 is already chosen, we choose for m_2 the least positive integer for which $\frac{1}{m_1} + \frac{1}{(m_1 - 1)m_2} < x$. Then clearly $m_2 > m_1$ as $\frac{1}{m_1} + \frac{1}{(m_1 - 1)m_1} = \frac{1}{m_1 - 1} \geq x$ because of the definition of m_1 . If $m_1, m_2, \dots, m_n$ are already

determined, we choose for m_{n+1} the least positive integer for which $\frac{1}{m_1} +$

$$+ \frac{1}{(m_1 - 1)m_2} + \dots + \frac{1}{(m_1 - 1) \dots (m_n - 1)m_{n+1}} < x$$

It is easy to see that $m_{n+1} > m_n$ and that

$$(5.2) \quad 0 < x - \frac{1}{m_1} - \sum_{k=1}^n \frac{1}{(m_1 - 1) \dots (m_{k-1} - 1)m_k} \leq \frac{1}{(m_1 - 1)(m_2 - 1) \dots (m_n - 1)m_n}$$

and thus as $m_n \geq n+1$, (5.1) holds. We shall call (5.1) the *modified Engel's series* of x .

The denominators m_n have the same probable asymptotic behaviour as the denominators q_n of the ordinary Engel's series.

In fact the variables m_n ($n=1, 2, \dots$) form also a homogeneous Markov chain, with the transition probabilities

$$(5.3) \quad P(m_n = k | m_{n-1} = l) = \frac{l}{k(k-1)} \quad (k \geq l+1).$$

The basic independent random variables are defined here analogously. In fact if δ_k is 1 or 0 according to whether the number k occurs in the sequence m_n or not, then it can be shown — analogously as in § 1 we proved the corresponding fact for ordinary Engel's series — that the random variables

$\delta_2, \delta_3, \dots, \delta_k, \dots$ are independent and $P(\delta_k = 1) = \frac{1}{k}$. Starting from this fact it follows that Theorems 2b, 3b and 4b remain valid for m_n instead of q_n .

These results are connected with the theory of order statistics (see [9]).

References

- [1] P. ERDŐS, A. RÉNYI and P. SZÜSZ, On Engel's and Sylvester's series, *Annales Univ. Sci. Budapest, Sectio Math.*, **1** (1958), 7–12.
- [2] É. BOREL, Sur les développements unitaires normaux, *Comptes Rendus*, **225** (1947), 51.
- [3] P. LÉVY, Remarques sur un théorème de M. Émile Borel, *Comptes Rendus*, **225** (1947), 918–919.
- [4] A. RÉNYI, On mixing sequences of events, *Acta Math. Acad. Sci. Hung.*, **9** (1958), 389–394.
- [5] M. LOÉVE, *Probability theory*, Van Nostrand, New York, 1955, p. 238.
- [6] A. RÉNYI, A new axiomatic theory of probability, *Acta Math. Acad. Sci. Hung.*, **6** (1955), 185–336.
- [7] A. RÉNYI, A számjegyek eloszlása valós számok Cantor-féle előállításában, *Mat. Lapok*, **7** (1956), 77–100.
- [8] A. KOLMOGOROF, Über das Gesetz des iterierten Logarithmus, *Mathematische Annalen*, **101** (1929), 126–135.
- [9] A. RÉNYI, Megfigyeléssorozatok kiemelkedő elemeiről, *MTA III. Oszt. Közl.*, **12** (1962), 105–121.

ON THE REPRESENTATION OF AN EVEN NUMBER AS THE SUM OF A PRIME AND OF AN ALMOST PRIME

A. RÉNYI

Summary: It is proved in this paper that every even number is equal to the sum of a prime and of an "almost prime" (that is: an integer the number of prime factors of which is bounded by a certain constant). Th. Estermann has proved this previously only conditionally, showing that it is a consequence of the Riemann hypothesis. The (unconditional) proof given in the present paper is based, besides the sieve of Viggo Brun, on a new theorem concerning L -series. The same method leads also to the proof of the following theorem: there exist an infinity of primes p such that $p + 2$ is "almost prime".

Introduction

In the correspondence of Euler and Goldbach of the year 1742 the following conjectures have been stated:

- I. Every odd integer ≥ 9 is the sum of three primes.
- II. Every even integer ≥ 6 is the sum of two primes.

The first conjecture has been proved by I. M. Vinogradov [1] in 1937. The second conjecture is still open, though recently many interesting approaches to the problem have been found.

It follows immediately from I that every integer is the sum of four primes.

N. G. Čudakov [2] has proved, using I. M. Vinogradov's method, that almost all even numbers can be represented as the sum of two primes. Let us mention that the first result of a similar kind has been obtained by L. Šnirel'man [3], who proved that the set of even numbers which can be represented as the sum of two primes has positive density.

Other results are connected with the representation of all even numbers, but in a form which is somewhat less restrictive than that required by Goldbach. These investigations were started by Viggo Brun [4] in 1920, who—using the elementary method of the sieve of Eratosthenes—proved that every even number can be represented as the sum of two "almost primes" that is integers which have not more prime factors than a certain constant k ; he proved this in fact with $k = 9$.

Viggo Brun's method has been sharpened by many authors, every sharpening leading to a smaller value of k . The best results * are those obtained by A. A. Buhštab and V. A. Tartakovskii, who proved that one can take $k = 4$.

* Author's remark: Since this paper has been written, this result has been improved. A. I. Vinogradov has shown that every sufficiently large even integer is the sum of two integers, each of which have not more than 3 prime factors.

Let us mention that the conjecture of Goldbach mentioned above under II could not be deduced even from the generalized Riemann hypothesis, which is sufficient for the solution of a large number of open questions of number theory.

A "conditional" result of this type was obtained by Th. Estermann [7] who proved that if the Riemann hypothesis is true for all of Dirichlet's L -functions* then every sufficiently large even number is equal to the sum of a prime and an almost prime, the latter having at most 6 prime factors.** In this direction the best unconditional result is that of Buhřtab [8] according to which every even integer $2N$ can be represented in the form $2N = p + \Pi$ where p is a prime and the number of prime factors of Π does not exceed $(\log N)^\alpha$, where $\alpha > 0$ is an arbitrary fixed positive constant.

Recently Yu. V. Linnik has proved certain theorems on the zeros of L -functions (see [9] and [10]); related but somewhat weaker results have been obtained by P. Turán [11] and C. L. Siegel [12]. In many cases (see especially [10]) these results were sufficient to replace the Riemann hypothesis. Thus it was natural to ask whether this could be done also in the case of Estermann's theorem.

In the present paper we show that this can really be done*** as we prove the following theorem:

Theorem 1. *Every even number $2N$ can be represented in the form*

$$2N = p + P,$$

where p is a prime, and P an almost prime, that is the number of prime factors of P does not exceed a certain absolute constant K .

As regards the value of K , for the sake of simplicity we do not endeavour to obtain for K the least value which our methods are able to furnish. Nevertheless we give for K a rough estimate.****

The proof of Theorem 1 is based on Viggo Brun's method.

We prove also another result, Theorem 2, which can be considered as a step towards the well-known conjecture that there exist an infinity of twin primes.

Theorem 2. *There exist an infinity of primes p such that $P = p + 2$ is almost prime, i.e., the number of prime factors of P does not exceed a certain absolute constant K .*

As mentioned above, the idea of the proof of Theorem 1 consists in replacing the Riemann hypothesis in Estermann's proof by some theorem on the distribution of zeros of L -functions. For this purpose a new theorem of this type (Theorem 3) is needed,

* Author's remark: As a matter of fact, Estermann uses only the (unproved) hypothesis that no L -function $L(s, \chi)$ has a zero in the half plane $s = \sigma + it$, $\sigma \geq 0$, 54.

** Author's remark: Recently Y. Wang has proved that if the Riemann hypothesis is true for all L -functions, then every sufficiently large even number is equal to the sum of the prime and a number having not more than 4 prime factors.

*** A short summary of the results of the present paper has been given previously in [18].

**** Author's remark: A smaller value for K could be obtained (as has been pointed out to the author by P. Turán) by using instead of Brun's sieve the sieve method of A. Selberg.

which will be proved by combining two methods of Yu. V. Linnik; the method of the "large sieve" [13] which is generalized in Lemma 1, and the method applied by Yu. V. Linnik in his paper [9].

We formulate here, in view of further applications, a special case of Theorem 3.

Theorem 3b. *Let $A \geq c_4$ be a sufficiently larger number. * Then for all primes p in the interval $A \leq p < 2A$, with the possible exception of at most $A^{3/4}$ such primes, and for all nonprincipal characters $\chi = \chi(n)$ belonging to the modulus p , one has $L(s, \chi) \neq 0$ in the domain $s = \sigma + it$, $\sigma \geq 1 - \delta$, $|t| < \log^3 p$ where $\delta > 0$ is an absolute constant.*

Besides Theorem 3 we shall use also certain results of E. C. Titchmarsh [14], A. Page [15] and C. L. Siegel [16].

As regards the number of representations of an even number $2N$ in the form $2N = p + P$ (where p is prime and P almost prime) we obtain a lower bound of the order $\frac{N}{\log^3 N}$ only, instead of $\frac{N}{\log^2 N}$. The reason why our result is rather weak in this respect is that we consider instead of the sum $\sum \log p$ the sum

$$\sum \log p \cdot e^{-p \frac{\log 2N}{2N}};$$

this means that we take essentially only such primes p into account which are less than $\frac{N}{\log N}$. This makes it however possible to use, instead of the classical formulae of the Riemann-Hadamard type, the integral formula of J. E. Littlewood [17]

$$\sum_{n=1}^{\infty} \chi(n) \Lambda(n) e^{-nt} = -\frac{1}{2\pi i} \int_{(2)} \frac{L'}{L}(s, \chi) \Gamma(s) t^{-s} ds, \quad (1)$$

which has the advantage that it is sufficient to show (as is done in Theorem 3) about a relatively "small" rectangle that it is free of zeros of almost all L -functions. However a sharpening of our result in this direction (i.e., concerning the lower estimate of the number of representations) would be possible without encountering any essential difficulty.

I want to make use of this occasion also to express my most sincere thanks to Yu. V. Linnik, who called my attention to the problem considered in this paper and helped my work by his valuable advice.

Chapter 1

Application of Viggo Brun's method

1. Let N be a positive integer, p a prime; $p < 2N$; put

$$a_p = \log p \cdot \exp \left[-p \frac{\log 2N}{2N} \right]. \quad (1.1)$$

Let us put further

* In what follows $c_1, c_2, \dots$ denote positive constants.

$$H_0(2N) = \sum_{\substack{3 \leq p < 2N \\ (2N-p, \Delta_0)=1}} a_p, \quad (1.2)$$

where

$$\Delta_0 = \prod_{2 \leq p \leq (2N)^{1/R}} p, \quad (1.3)$$

and put

$$H(2N) = \sum_{\substack{3 \leq p < 2N \\ (2N-p, D_0)=1 \\ p \equiv v_1 \pmod{Q_0}}} a_p, \quad (1.4)$$

where

$$D_0 = \prod_{\substack{p_T \leq p \leq (2N)^{1/R} \\ (p, 2N)=1}} p, \quad Q_0 = \prod_{\substack{2 < p \leq p_T \\ (p, 2N)=1}} p, \quad (1.5)$$

and v_1 is such an integer that $(v_1(2N - v_1), Q_0) = 1$, further T is a positive integer and R a positive constant, and p_T denotes the T th prime (i.e., the T th term in the sequence of all primes arranged in increasing order).

If (1.4) contains the term a_p then clearly $(2N - p, D_0 Q_0) = 1$. Thus (1.4) contains besides terms which occur in (1.2) only such terms for which $p|2N$.** But the number of prime factors of $2N$ can not exceed $\frac{\log 2N}{\log 2}$, and therefore, taking into account that $a_p < \log 2N$, we obtain

$$H_0(2N) > H(2N) - \frac{\log^2 2N}{\log 2}. \quad (1.6)$$

In what follows it will be shown that $H(2N) > c_1 \frac{N}{\log^2 N}$. From this and (1.6) it follows that $H_0(2N) > \frac{c_2 N}{\log^2 N}$ for $N \geq c_3$. But this means that there exists such a prime p (as a matter of fact, that there exist at least $O\left[\frac{N}{\log^3 N}\right]$ such primes) for which $P = 2N - p$ is divisible only by primes greater than $(2N)^{1/R}$; it follows that the number of prime factors of P is less than R , which proves Theorem 1.

2. Following V. Brun, we choose two constants h and h_0 such that $1 < h < h_0$ and put $r = \log h_0$. We denote by p_T the least prime such that for $w > p_T$ one has

$$\sum_{w \leq p \leq w^h} \frac{1}{p-1} \leq r \quad \text{and} \quad \prod_{w \leq p \leq w^h} \left[1 - \frac{1}{p-1}\right] > \frac{1}{h_0}.$$

Let us put further $Y = (2N)^{1/R}$. The value of the constant R will be chosen in the

* Author's remark: Here and in what follows (a, b) denotes the greatest common divisor of a and b .

** Author's remark: $a|b$ denotes that a is a divisor of b , while $a \nmid b$ denotes that a is not a divisor of b .

last chapter.

Let us define the set E of square-free natural numbers Q as follows: E contains the numbers $Q = p_1 p_2 \cdots p_r Q_0$ where $p_1 > p_2 > \cdots > p_r$ are primes, where $(p_i, 2N) = 1$, $i = 1, 2, \dots, r$, further Q_0 is defined by (1.5) and the inequalities

$$p_T < p_i \leq Y^{\frac{1}{\left[\frac{i}{2}\right]}} \quad (i = 1, 2, \dots, r) \quad (1.7)$$

are satisfied; * here $r \leq 2m + 1$ while m is the least integer such that

$$\frac{1}{Y^{h^{m+1}}} \leq p_T.$$

By definition Q_0 itself belongs to the set E too.

Let us put

$$P(x, Q) = \sum_{\substack{p \leq x \\ p \equiv l \pmod{Q}}} a_p = \frac{x}{\phi(Q) \log x} + R_Q(x) \quad (1.8)$$

where ** $(l, Q) = 1$.

Following Brun, we obtain

$$H(2N) \geq \sum_{Q \in E} \mu \left[\frac{Q}{Q_0} \right] P(2N, Q), \quad (1.9)$$

where $\mu(n)$ is the function of Möbius. It follows that

$$H(2N) \geq \frac{\omega N}{\phi(Q_0) \log N} \cdot \prod_{p_T < p \leq Y} \left[1 - \frac{1}{p-1} \right] - \sum_{Q \in E} |R_Q(2N)|, \quad (1.10)$$

where

$$\omega = 1 - \sum_{k=1}^{\infty} \frac{(h_0 r^2 k^2)^k}{(2k)!}.$$

Let us choose $h_0 = e^{\frac{1}{4}} = 1,28 \dots$ and $h = 1,25$. Then we have $\omega \geq 0,75$. Therefore,

$$H(2N) > \frac{c_5 N}{\log^2 N} - \sum_{Q \in E} |R_Q(2N)|. \quad (1.11)$$

It remains only to estimate the remainder term in (1.11). This will be done in the following chapters, where it will be proved that

$$\sum_{Q \in E} |R_Q(2N)| < \frac{5N}{\log^3 N}$$

and thus that

$$H(2N) > \frac{c_1 N}{\log^2 N} \quad \text{for } N \geq c_{43}.$$

As mentioned above, this proves Theorem 1.

* Author's remark: $[x]$ denotes the integral part of the non-negative number x .

** Author's remark: l is defined mod Q by the congruences $l \equiv v_1 \pmod{Q_0}$ and $l \equiv 2N \pmod{Q/Q_0}$. Here and in what follows $\phi(n)$ denotes Euler's function.

Chapter 2

Generalization of the "large sieve"

1. **Lemma 1.** *Let there be given an arbitrary sequence of integers $1 \leq n_1 < n_2 < \dots < n_Z \leq X$, further a non-negative function $g(n)$, a square-free positive integer $q < \sqrt{X}$ and a number A such that $2 \leq A \leq (1/2) \sqrt{X/q}$. Let us put*

$$k = \frac{\log q}{\log A} + 1, \quad (2.1)$$

$$m = \max_{1 \leq j \leq Z} g(n_j), \quad (2.2)$$

$$S = \sum_{j=1}^Z g(n_j), \quad \lambda = \frac{S}{X}, \quad (2.3)$$

$$S_u = \sum_{n_j \equiv u \pmod{q}} g(n_j), \quad 0 \leq u \leq q-1. \quad (2.4)$$

For any prime p for which $(p, q) = 1$ and $A \leq p < 2A$ let us put

$$s_r = \sum_{n_j \equiv r \pmod{pq}} g(n_j), \quad 0 \leq r \leq pq-1, \quad (2.5)$$

in which case we have evidently

$$S_u = s_u + s_{u+q} + s_{u+2q} + \dots + s_{u+(p-1)q}. \quad (2.6)$$

Then for all primes p such that $(p, q) = 1$ and $A \leq p < 2A$, with the possible exception of not more than $12\pi/5 (m/\lambda)^3 A^{1/2}$ "exceptional" primes, and for all residue classes $r \pmod{pq}$, with the exception of at most $(pq)^{1-1/9k}$ "irregular" residue classes the following inequality holds

$$\left| s_r - \frac{S_u}{p} \right| \leq \frac{S}{(pq)^{1+1/9k}} \text{ for } 0 \leq u \leq q-1,$$

if $u \equiv r \pmod{q}$.

Proof of Lemma 1. Let us put

$$S(t) = \sum_{j=1}^Z g(n_j) e^{2\pi i n_j t} \quad (2.7)$$

and let us consider

$$I_{pq}(\delta_p) = \int_{-\delta_p}^{+\delta_p} \sum_{\gamma=0}^{p-1} \sum_{\nu=0}^{q-1} \left| S \left[\frac{\gamma}{p} + \frac{\nu}{q} + t \right] \right|^2 dt, \quad (2.8)$$

where

$$\delta_p = \frac{1}{2\pi X} \cdot \frac{\lambda}{m} \cdot \frac{1}{(pq)^{1/6k}}. \quad (2.9)$$

Evidently we have $\delta_p \leq \frac{1}{2\pi X}$. Carrying out the squaring of the terms in (2.8) and by interchanging the order of summation we obtain

$$I_{pq}(\delta_p) = \sum_{j=1}^Z \sum_{j'=1}^Z g(n_j) g(n_{j'}) \left[\sum_{\gamma=0}^{p-1} e^{2\pi i (n_j - n_{j'}) \frac{\gamma}{p}} \right] \left[\sum_{\nu=0}^{q-1} e^{2\pi i (n_j - n_{j'}) \frac{\nu}{q}} \right] \int_{-\delta_p}^{+\delta_p} e^{2\pi i (n_j - n_{j'}) t} dt. \quad (2.10)$$

It follows that

$$I_{pq}(\delta_p) = 2pq \sum_{\substack{n_j - n_{j'} \equiv 0 \pmod{pq} \\ n_j \neq n_{j'}}} g(n_j) g(n_{j'}) \frac{\sin 2\pi |(n_j - n_{j'})| \delta_p}{2\pi |(n_j - n_{j'})|} + \\ + 2pq \delta_p \sum_{j=1}^Z g^2(n_j). \quad (2.11)$$

Using the inequality $\sin \alpha > \alpha - \frac{\alpha^3}{6}$ which is valid for $0 < \alpha \leq 1$ (we may use this inequality in view of $\delta_p \leq \frac{1}{2\pi X}$) we get

$$I_{pq}(\delta_p) \geq 2\delta_p pq \left[1 - \frac{4\pi^2 \delta_p^2 X^2}{6} \right] \left[\sum_{r=0}^{pq-1} s_r^2 \right]. \quad (2.12)$$

From this, by using the obvious inequality $s_r \leq \frac{mX}{pq}$ it follows that

$$I_{pq}(\delta_p) \geq 2\delta_p \cdot pq \cdot \sum_{r=0}^{pq-1} s_r^2 - \frac{4\pi^2 \delta_p^3 X^4 m^2}{3}. \quad (2.13)$$

Analogously, putting

$$I_q(\delta_p) = \int_{-\delta_p}^{+\delta_p} \sum_{\nu=0}^{q-1} \left| S\left(\frac{\nu}{q} + t\right) \right|^2 dt, \quad (2.14)$$

we obtain

$$I_q(\delta_p) \leq 2pq \cdot \delta_p \cdot \sum_{n_j - n_{j'} \equiv 0 \pmod{q}} g(n_j) g(n_{j'}) \quad (2.15)$$

and similarly that

$$I_q(\delta_p) \leq 2\delta_p \cdot q \cdot \sum_{u=0}^{q-1} S_u^2. \quad (2.16)$$

Let us consider now on the unit circle described by $\exp(2\pi it)$ the system of intervals

$$\frac{\gamma}{p} + \frac{\nu}{q} - \delta_p \leq t \leq \frac{\gamma}{p} + \frac{\nu}{q} + \delta_p,$$

where $0 \leq \gamma \leq p-1$, $1 \leq \nu \leq q-1$ and p runs over all primes for which $(p, q) = 1$ and $A \leq p < 2A$. It is easy to see that these intervals do not overlap, because if $(p-p')^2 + (\nu-\nu')^2 + (\gamma-\gamma')^2 \neq 0$, then

$$\left| \left[\frac{\gamma}{p} + \frac{\nu}{q} \right] - \left[\frac{\gamma'}{p'} + \frac{\nu'}{q} \right] \right| \geq \frac{1}{pp'q} \geq \frac{1}{4A^2q} \geq \frac{1}{X} > \delta_p + \delta_{p'}.$$

Thus it follows that

$$\sum_{\substack{A \leq p < 2A \\ (p, q)=1}} [I_{pq}(\delta_p) - I_q(\delta_p)] \leq \int_0^1 |S(t)|^2 dt = \sum_{j=1}^Z g^2(n_j) \leq m^2 X. \quad (2.17)$$

On the other hand it follows from (2.6) that

$$\sum_{j=0}^{p-1} s_{u+jq}^2 - \frac{S_u^2}{p} = \sum_{j=0}^{p-1} \left[s_{u+jq} - \frac{S_u}{p} \right]^2. \quad (2.18)$$

Therefore we get from (2.13), (2.16) and (2.18) that

$$I_{pq}(\delta_p) - I_q(\delta_p) \geq 2\delta_p pq \sum_{\substack{r=0 \\ u \equiv r \pmod q}}^{pq-1} \left(s_r - \frac{S_u}{p}\right)^2 - \frac{4\pi^2 \delta_p^3 X^4 m^2}{3}. \quad (2.19)$$

Let us consider now an exceptional prime p for which there exist more than $(pq)^{1-1/9k}$ "irregular" residue classes $\pmod{pq}$ such that

$$\left|s_r - \frac{S_u}{p}\right| > \frac{S}{(pq)^{1+1/9k}},$$

where $u \equiv r \pmod q$. For such an exceptional prime p we clearly have

$$\sum_{\substack{r=0 \\ u \equiv r \pmod q}}^{pq-1} \left(s_r - \frac{S_u}{p}\right)^2 \geq \frac{S^2}{(pq)^{1+1/3k}}. \quad (2.20)$$

Substituting the value of δ_p from (2.9), we obtain from (2.19) and (2.20) that for such an exceptional prime p the inequality

$$I_{pq}(\delta_p) - I_q(\delta_p) > \frac{5}{6\pi} \frac{X\lambda^3}{m(pq)^{1/2k}} \geq \frac{5}{12\pi} \frac{X\lambda^3}{mA^{1/2}} \quad (2.21)$$

holds. Evidently for any prime p we have $I_{pq}(\delta_p) - I_q(\delta_p) > 0$; therefore, according to (2.17), the sum $\sum [I_{pq}(\delta_p) - I_q(\delta_p)]$ extended over all exceptional primes p , will be less than $m^2 X$.

Thus if $v(A)$ is the number of exceptional primes p , it follows from (2.21) and (2.17) that

$$\frac{5}{12\pi} \cdot \frac{X\lambda^3}{mA^{1/2}} \cdot v(A) \leq m^2 X,$$

that is

$$v(A) \leq \frac{12\pi}{5} \left(\frac{m}{\lambda}\right)^3 A^{1/2}. \quad (2.22)$$

This proves Lemma 1.

2. As an application of Lemma 1 we shall now prove another lemma, namely, Lemma 2 formulated below; but before doing this we introduce certain definitions. It is known that every character belonging to the square-free modulus D can be represented uniquely as a product of characters belonging to moduli which are the prime factors of D . Thus for instance if $D = pq$ where p is a prime, q is square-free and $(p, q) = 1$ then every character $\chi_D(n)$ belonging to the modulus $D = pq$ is of the form

$$\chi_D(n) = \chi_p(n) \chi_q(n), \quad (2.23)$$

where $\chi_p(n)$ resp. $\chi_q(n)$ are characters belonging to the moduli p resp. q .

If in (2.23) $\chi_p(n)$ is not a principal character, then we shall call $\chi_D(n)$ *primitive with respect to p* . Clearly if $\chi_D(n)$ is primitive with respect to every prime factor of D , then it is primitive in the usual sense.

Lemma 2. Let $1 \leq n_1 < n_2 < \dots < n_Z \leq X$ be an arbitrary sequence of integers, $q \leq \sqrt{X}$ a square-free positive integer, A an arbitrary number such that $2 \leq A \leq \frac{1}{2} \sqrt{\frac{X}{q}}$, $g(n)$ an arbitrary non-negative function, and let us put

$$m = \max_{1 \leq j \leq Z} g(n_j). \quad (2.24)$$

Let further $\chi_D(n)$ be an arbitrary character belonging to the modulus $D = pq$ where p is a prime and $A \leq p < 2A$, and $(p, q) = 1$ and which is primitive with respect to p , and let p be not exceptional in the sense of Lemma 1. Let us put finally

$$k = \frac{\log q}{\log A} + 1.$$

Then we have

$$\left| \sum_{j=1}^Z \chi_D(n_j) g(n_j) \right| \leq \frac{3mX}{D^{1/9k}}. \quad (2.25)$$

Proof of Lemma 2. Putting $\chi_D(n) = \chi_p(n) \chi_q(n)$ we have, using the notations of Lemma 1,

$$\sum_{j=1}^Z \chi_D(n_j) g(n_j) = \sum_{u=0}^{q-1} \chi_q(u) \cdot \sum_{\substack{r \equiv u \pmod{q} \\ 0 \leq r \leq pq-1}} \chi_p(r) s_r. \quad (2.26)$$

Let us suppose that p is not exceptional in the sense of Lemma 1. Let us divide the terms on the right of (2.26) in two groups, according to r being irregular or regular.* For a regular r if u is defined by $u \equiv r \pmod{q}$ we have

$$s_r = \frac{S_u}{p} + \frac{\mathfrak{S}_r S}{(pq)^{1+1/9k}} \quad (0 \leq |\mathfrak{S}_r| < 1). \quad (2.27)$$

For an irregular r we shall use the trivial estimate

$$s_r \leq \frac{mX}{D}. \quad (2.28)$$

It follows that

$$\sum_{j=1}^Z \chi_D(n_j) g(n_j) = \sum_{u=0}^{q-1} \chi_q(u) \cdot \sum_{r \equiv u \pmod{q}}^{(1)} \chi_p(r) \left[\frac{S_u}{p} + \frac{\mathfrak{S}_r S}{D^{1+1/9k}} \right] + \frac{\eta mX}{D^{1/9k}} \quad (2.29)$$

where $\sum^{(1)}$ denotes that the summation is to be extended over all regular residues r , and η is a number such that $|\eta| < 1$. Adding and subtracting to the right-hand side of (2.29) the sum

$$\sum_{u=0}^{q-1} \chi_q(u) \cdot \sum_{r \equiv u \pmod{q}}^{(2)} \chi_p(r) \frac{S_u}{p}, \quad (2.30)$$

where $\sum^{(2)}$ denotes that the summation is to be extended over all irregular residues r , in view of the trivial inequalities

$$S_u \leq \frac{mX}{q}, \quad S \leq mX, \quad (2.31)$$

* Author's remark: Residues which are not irregular will be called regular.

we obtain

$$\left| \sum_{j=1}^Z \chi_D(n_j) g(n_j) - \frac{1}{p} \sum_{u=0}^{q-1} \chi_q(u) S_u \cdot \sum_{\substack{r \equiv u \pmod{q} \\ 0 \leq r \leq pq-1}} \chi_p(r) \right| \leq \frac{3mX}{D^{1/9k}}. \quad (2.32)$$

As

$$\sum_{\substack{r \equiv u \pmod{q} \\ 0 \leq r \leq pq-1}} \chi_p(r) = 0 \quad (2.33)$$

because for a fixed value of u the numbers $r \equiv u \pmod{q}$, $0 \leq r \leq pq-1$ form a complete set of residues mod p , and by supposition $\chi_p(n)$ is not a principal character, the assertion of Lemma 2 follows immediately from (2.32).

Chapter 3

The method of Yu. V. Linnik

1. Lemma A. Let

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad (3.1)$$

be an L -series with χ being a non-principal character belonging to the modulus D . If $L(s, \chi)$ where $s = \sigma + it$ has a zero in the domain

$$\sigma \geq 1 - d, \quad |t| \leq \log^3 D,$$

where $\frac{1}{3} > d > \frac{1}{(\log D)^{4/5}}$ and if we put

$$S_{\chi}(N) = \sum_{p \leq N} \chi(p) \log p, \quad (3.2)$$

then there exists a number N_1 lying in the interval

$$(\log D)^{1/20d} < N_1 < D^{2K_3}, \quad (3.3)$$

(where K_3 is an absolute constant), such that

$$|S_{\chi}(N_1)| > N_1^{1-280d} \quad (3.4)$$

holds.

This lemma is identical with Lemma VI of Yu. V. Linnik's paper [9], (the correspondence between the above notations and that of [9] is:

$$d = \frac{\psi(D)}{\log D} \quad \text{and} \quad \lambda = \frac{1}{5}).$$

Combining Lemma A with Lemma 2 of the preceding chapter, we obtain the following:

Theorem 3. Let q be a square-free integer, $A \geq c_4$ an arbitrary number, and put

$$k = \frac{\log q}{\log A} + 1.$$

Suppose that $k \leq \log^3 A$. Then for all primes p such that $(p, q) = 1$ and $A \leq p < 2A$, with the possible exception of at most $A^{3/4}$ exceptional primes, no L -series

$L(s, \chi)$ formed with a character which belongs to the modulus $D = pq$ and is primitive with respect to p , has a zero in the domain

$$s = \sigma + it, \quad \sigma \geq 1 - \frac{d_1}{k+1}, \quad |t| < \log^3 D,$$

where

$$d_1 = \frac{1}{7500K_3}$$

and K_3 is the constant figuring in Lemma A.

Remark. Theorem 3 does not give any information on the zeros of L -series formed with principal characters, (and thus it gives no information about the zeros of the ζ -function) because a principal character can not be primitive with respect to any of the prime factors of its modulus.

Proof of Theorem 3. Let $U(A)$ denote the number of "bad" primes that is of such primes p with $(p, q) = 1$ and $A \leq p < 2A$ for which there is at least one L -series formed with a character belonging to the modulus $D = pq$ and primitive with respect to p , which has a zero in the domain

$$\sigma \geq 1 - \frac{d_1}{k+1} = 1 - d, \quad |t| < \log^3 D.$$

If p is such, then according to Lemma A one can find a number N_1 in the interval $(\log D)^{1/20d} < N_1 < D^{2K_3}$ such that

$$|S_{\chi}(N_1)| \geq N_1^{1-280d}. \quad (3.5)$$

Evidently the conditions of Lemma A are satisfied, as with respect to $k \leq \log^3 A$ we have

$$\frac{1}{(\log D)^{4/5}} < d < \frac{1}{3} \quad \text{if } A \geq c_6. \quad (3.6)$$

All these numbers N_1 (belonging to different "bad" primes) are lying in the interval

$$(k \log A)^{1/20d} < N_1 < 2^{2K_3} A^{2K_3k}. \quad (3.7)$$

Let us divide the interval (3.7) into the subintervals

$$(A^{2K_3k} \cdot 2^{2K_3l}, A^{2K_3k} \cdot 2^{2K_3l+1}), \quad l = 0, 1, \dots, [\log^5 A].$$

It is clear that at least one of these subintervals – say $(B, 2B)$ – contains more than $\frac{U(A)}{\log^5 A}$ of the numbers N_1 . If $A \geq 2$, we have

$$B \leq A^{2K_3(k+1)}. \quad (3.8)$$

Let us divide the interval $(B, 2B)$ again into subintervals of the length B^{1-300d} . The number of such subintervals does not exceed $B^{300d} < A^{2/25}$. There will be thus at least one such subinterval, which contains at least

$$\frac{U(A)}{A^{2/25} \log^5 A} > \frac{U(A)}{A^{1/12}} \quad (3.9)$$

of the numbers N_1 , provided that $A \geq c_7$. Taking into account that for

$0 < N_1 - N_2 < N_1^{1-300d}$ and if $|S_\chi(N_1)| > N_1^{1-280d}$ it follows from the trivial inequality

$$|S_\chi(N_1) - S_\chi(N_2)| < (N_1 - N_2) \log N_1, \quad (3.10)$$

that

$$|S_\chi(N_2)| > N_2^{1-300d} \quad (3.11)$$

holds, provided that $A \geq c_8$.

Thus for more than $U(A) \cdot A^{-1/12}$ "bad" primes p one can choose instead of a separate N_1 for each p the same value N_2 , namely, the left end of the selected subinterval; for this N_2 (3.11) will hold for at least $U(A) \cdot A^{-1/12}$ "bad" primes.

Let us choose now an integer $\nu \geq 1$ such that the inequalities

$$A^{(k+1)K_3} < N_2^\nu < A^{2(k+1)K_3} \quad (3.12)$$

shall be valid. Then we have

$$\nu \leq \frac{2(k+1) K_3 \log A}{\log N_2}, \quad (3.13)$$

and thus also

$$\nu \leq \frac{1}{180} \frac{\log A}{\log \log A}. \quad (3.14)$$

Let us define the sequence of integers n_j ($j = 1, 2, \dots, Z$) and the non-negative function $g(n)$ as follows: Let the sequence n_j consist of all numbers which are equal to the product of exactly ν (not necessarily distinct) primes $p \leq N_2$. If

$$n_j = p_1 p_2 \cdots p_\nu \quad (3.15)$$

then the value of the function $g(n)$ for $n = n_j$ shall be defined by

$$g(n_j) = G(n_j) \prod_{i=1}^{\nu} \log p_i, \quad (3.16)$$

where $G(n_j)$ is the number of representations of n_j in the form (3.15) where $p_1, p_2, \dots, p_\nu$ run independently over all primes $\leq N_2$. Thus for any character χ we have

$$\left(\sum_{p \leq N_2} \chi(p) \log p \right)^\nu = \sum_{j=1}^Z \chi(n_j) g(n_j) \quad (3.17)$$

and especially

$$\left(\sum_{p \leq N_2} \log p \right)^\nu = \sum_{j=1}^Z g(n_j) = S. \quad (3.18)$$

Now we shall make use of Lemma 2. We shall show that all the "bad" primes p for which the same N_2 could be chosen are exceptional in the sense of Lemma 1.

First let us estimate

$$m = \max_{1 \leq j \leq Z} g(n_j) \text{ and } \lambda = \frac{S}{X} \text{ where } X = N_2^\nu.$$

By (3.13) and (3.14) and by some calculations we obtain

$$m \leq A^{1/36}. \quad (3.19)$$

On the other hand,

$$\frac{S}{X} = \frac{(\sum_{p \leq N_2} \log p)^\nu}{N_2^\nu} > A^{-1/180} \text{ if } A \geq c_{11}. \quad (3.20)$$

It follows that $\frac{1}{\lambda} < A^{1/180}$, and thus the number of exceptional primes (in the sense of Lemma 1) does not exceed

$$\frac{12\pi}{5} A^{\frac{1}{2} + \frac{1}{10}}. \quad (3.21)$$

Let us suppose now that one of the "bad" primes p for which

$$|S_{\chi}(N_2)|^\nu = \left| \sum_{j=1}^Z \chi(n_j) g(n_j) \right| \geq N_2^{\nu(1-300d)} = X^{1-300d} \quad (3.22)$$

holds, would not be exceptional. Then, according to Lemma 2, for the character figuring in (3.22) we would have

$$\left| \sum_{j=1}^Z \chi(n_j) g(n_j) \right| < \frac{3X}{A^{1/12}}. \quad (3.23)$$

Comparing (3.22) and (3.23) we obtain

$$X^{1-300d} < \frac{3X}{A^{1/12}}, \quad (3.24)$$

and thus, in view of (3.12) that

$$A^{75} < 3A^{72}, \quad (3.25)$$

which is clearly impossible if $A \geq c_{12}$. Thus we arrived to a contradiction, which proves that all the "bad" primes in question (whose number exceeds $U(A) \cdot A^{-1/12}$), are exceptional primes in the sense of Lemma 1. As however the number of these exceptional primes cannot exceed $\frac{12\pi}{5} A^{1/2 + 1/10}$, it follows that for $A \geq c_{14}$ we have

$$U(A) < A^{1/4}.$$

Thus Theorem 3 is proved with $c_4 = \max(c_6, c_7, \dots, c_{14})$.

Chapter 4

Some results from the theory of L -series

1. Let us put, as in Chapter 1,

$$P(x, Q) = \sum_{\substack{p \leq x \\ p \equiv l \pmod{Q}}} \log p \cdot e^{-\frac{p \log x}{x}} \quad (4.1)$$

where

$$(l, Q) = 1.$$

In terms of $P(x, Q)$ the results of E. C. Titchmarsh [14], A. Page [15] and C. L. Siegel [16] can be formulated as follows:

Lemma B. For all positive integers $Q \leq \exp(c_{15} \sqrt{\log x})$ with the possible exception of those values of Q which are multiples of a certain integer Q_1 which

eventually may exist, and for $(l, Q) = 1$ we have

$$P(x, Q) = \frac{x}{\log x \cdot \phi(Q)} + O(xe^{-c_{16}\sqrt{\log x}}), \quad (4.2)$$

while if $Q_1|Q$ one has to add to the right-hand side of (4.2) the term

$$O\left[\frac{x}{\phi(Q)} \left(1 - \frac{c(\epsilon)}{Q_1^{(\epsilon)}}\right)\right], \quad (4.3)$$

where $\epsilon > 0$ is arbitrary and $c(\epsilon)$ a positive constant depending only on ϵ .

The O -estimates in (4.2) and (4.3) are valid uniformly for $Q \leq \exp(c_{15}\sqrt{\log x})$. Q_1 is the primitive modulus which is unique if it exists, for which an L -series $L(s, \chi)$ formed with a real character mod Q_1 has a so-called "Siegel-zero", that is a zero $s = \sigma + it$ with $\sigma > 1 - \frac{c_{17}}{\sqrt{\log x}}$.

The proof of Theorem B does not need any new idea (besides those contained in the papers cited above) and may be left to the reader.

2. We shall need also the elementary estimate:

Lemma C.

$$P(x, Q) < \frac{c_{18}x}{\phi(Q)} \quad (4.4)$$

uniformly for $Q < \sqrt{x}$.

Lemma C follows easily from Theorem 2 of Titchmarsh l.c., which he proves by Brun's method.

3. Let us put

$$K_\chi(x) = \sum_{p \leq x} \chi(p) \log p \cdot e^{-\frac{p \log x}{x}} \quad (4.5)$$

It is easy to prove the following:

Lemma 3. If $\chi(n)$ is a nonprincipal character mod Q and $L(s, \chi)$ has no zeros in the domain $s = \sigma + it$, $\sigma \geq 1 - \delta$, (where $0 < \delta < \frac{1}{2}$) $|t| < \log^3 Q$, then

$$|K_\chi(x)| < \frac{c_{19}}{\delta} x^{1-\frac{\delta}{4}} \quad (4.6)$$

uniformly for $\exp((\log x)^{2/5}) < Q < \sqrt{x}$.

This lemma can be deduced in a well-known way from Lemmas 12 and 15 of the paper [14] by Titchmarsh, by means of the formula of Littlewood (see [17]):

$$\sum_{n=1}^{\infty} \chi(n) \Lambda(n) e^{-\frac{n}{Y}} = -\frac{1}{2\pi i} \int_{(2)} \frac{L'}{L}(s, \chi) \Gamma(s) Y^s ds, \quad (4.7)$$

with $Y = \frac{x}{\log x}$. Combining Theorem 3 and Lemma 3 leads to

Lemma 4. Let q_1 be a square-free integer, $A \geq c_{20}$, p_1 a prime for which

$(p_1, q_1) = 1$ and $A \leq p_1 < 2A$. Then if $\frac{1}{2}$

$$\exp((\log x)^{\frac{1}{5}}) \leq Aq \leq \frac{\sqrt{x}}{2} \quad (4.8)$$

and putting

$$k_1 = \frac{\log q_1}{\log \frac{p_1}{2}} + 1 \geq \frac{\log q_1}{\log A} + 1 = k, \quad (4.9)$$

we have $k_1 \leq \log^3 A$, it follows that for all such p_1 with the possible exception of not more than $A^{\frac{3}{4}}$ exceptional primes and for all characters $\chi(n)$ belonging to the modulus $p_1 q_1$ which are primitive with respect to p_1 , the inequality

$$|K_\chi(x)| < c_{21} x^{1 - \frac{\delta_2}{k_1 + 1}} \quad (4.10)$$

holds with $\delta_2 = (4.10^4 \cdot K_3)^{-1}$

Lemma 4 is obtained by the remark that Lemma 1 can be applied with

$$\delta = \frac{\delta_1}{k_1 + 1} = \frac{1}{7500 K_3 (k_1 + 1)} \quad \text{and that by (4.8) and (4.9) one has}$$

$$\frac{1}{\delta} = 7500 K_3 (k_1 + 1) < \log^3 x.$$

Chapter 5

Some elementary properties of the set E

1. The set E has been defined in Chapter 1.

Lemma 5. If Q belongs to E and $\nu(Q)$ denotes the number of prime factors of Q then for $N \geq c_{22}$

$$\nu(Q) < 10 \log \log 2N.$$

Lemma 5 follows immediately from the definition of the set E .

2. Let us introduce certain notations. If $Q = p_1 p_2 \cdots p_r Q_0$, (where the p_i are primes, $p_1 > p_2 > \cdots > p_r$), belongs to the set E , let us put

$$Q = p_1 q_1, \quad q_1 = p_2 q_2, \quad \dots, \quad q_{r-1} = p_r q_r, \quad q_r = Q_0.$$

We shall call the numbers $q_1, q_2, \dots, q_r$ the "diagonal divisors" of Q .

Lemma 6. If Q belongs to E then all the diagonal divisors of Q belong to E also.

The proof of Lemma 6 is obvious.

3. **Lemma 7.** If Q belongs to E and p_1 is the greatest prime factor of Q and if the inequality

$$p_1 < Y^{\frac{1}{h^m}} \quad (m \geq 0 \text{ integer})$$

holds, then we have

$$Q < Q_0 Y^{\frac{2m+9}{h^m}}$$

Proof of Lemma 7. We have

$$p_i < p_1 < Y^{\frac{1}{h^m}} \quad \text{for } i = 2, 3, \dots, 2m+1$$

and

$$p_{2m+i} < Y^{\frac{1}{h^{m+[i/2]}}} \quad \text{for } i = 2, 3, \dots.$$

Therefore

$$q_1 < Q_0 p_1^{2m} Y^{\frac{8}{h^m}} < Q_0 Y^{\frac{2m+8}{h^m}},$$

and thus

$$Q < Q_0 Y^{\frac{2m+9}{h^m}},$$

which proves Lemma 7.

Corollary: The subset of E which consists of the numbers $Q = p_1 q_1$ for which we have

$$p_1 < Y^{\frac{1}{h^m}}$$

contains not more than

$$Y^{\frac{2m+9}{h^m}}$$

elements.

Especially for $m = 0$ we get that E itself contains not more than Y^9 elements.

4. Lemma 8. The subset of the set E which consists of those numbers $Q = p_1 q_1$ for which

$$p_1 < q_1^{\frac{1}{k}},$$

(where k is a positive integer) contains not more than

$$\frac{c_{23} k}{Y^{\frac{k}{2}}}$$

elements, where c_{23} is a positive absolute constant.

Proof of Lemma 8. Let us suppose that

$$Y^{\frac{1}{h^{m+1}}} < p_1 \leq Y^{\frac{1}{h^m}} \quad (m \geq 0).$$

It follows, as in the proof of Lemma 7, that

$$q_1 < Q_0 p_1^{2m} \cdot Y^{\frac{8}{h^m}} < p_1^{2m+T+8}$$

because of $Q_0 < p_1^T$. Thus if $p_1 < q_1^{1/k}$ then we have

$$p_1^k < p_1^{2m+T+8}$$

and therefore $k < 2m + T + 8$; but as $p_1 < Y^{\frac{1}{h^m}}$ and $q_1 < p_1^{2m+T+8}$ we obtain

$$Q < Y^{\frac{2m+T+9}{h^m}} < Y^{\frac{c_{23}k}{h^{k/2}}},$$

provided that c_{23} is sufficiently large, the value of c_{23} depending only on the value of T which has been fixed in Chapter 1. This proves Lemma 8.

5. We need also the following elementary results:

Lemma 9. *Let (p^*) be a sequence of certain primes, with the property that no interval $(A, 2A)$ contains more than $A^{3/4}$ terms of the sequence (p^*) . Then we have for any $B > 0$*

$$\sum_{p^* > B} \frac{1}{p^* - 1} < \frac{c_{24}}{\sqrt[4]{B}}.$$

The proof is immediate.

Lemma 10.

$$\sum_{n \leq x} \frac{1}{\phi(n)} < c_{25} \log x.$$

The proof is very easy (see [14]).

In what follows we shall often make use of the following estimate:

Lemma 11.

$$\phi(n) > \frac{c_{26}n}{\log n}.$$

This estimate follows easily from the asymptotic formula of Mertens for $\prod_{p \leq n} (1 - \frac{1}{p})$.

Chapter 6

Proof of the main theorem

1. In this chapter we shall deal at the same time with characters belonging to different moduli. Let us agree therefore to indicate the modulus of a character by writing it as a lower index. We shall denote the principal character mod D by χ_D^0 , and by $\sum_{(D)}$ that the summation has to be extended for all characters belonging to the modulus D . Let us put $x = 2N$.

2. We have to estimate the remainder term in (1.11). Let us begin by the formula* valid for $(l, Q) = 1$,

$$P(x, Q) = \frac{1}{\phi(Q)} \sum_{(Q)} \bar{\chi}_Q(l) K_{\chi_Q}(x), \quad (6.1)$$

which follows easily from (4.1) and (4.5). Let us consider a number $Q = p_1 p_2 \cdots p_r Q_0$ belonging to the set E . It follows from Lemma 5 that if

$$Q > \exp((\log x)^{2/5})$$

we have

$$p_1 > Q^{\nu(Q)} > 2 \exp((\log x)^{\frac{1}{3}}) \text{ for } x \geq c_{27}. \quad (6.2)$$

On the other hand

* Author's remark: $\bar{Z}$ denotes the conjugate of the complex number Z .

$$q_1 < p_1^{\nu(Q)} < p_1^{10 \log \log x},$$

and therefore

$$k_1 = \frac{\log q_1}{\log p_1^{1/2}} + 1 < 11 \log \log x. \quad (6.3)$$

Let us apply now Lemma 4 to (6.2) with fixed q_1 ; it is sufficient to consider the intervals $(A, 2A)$ with $A = 2^k B$ ($k = 1, 2, \dots$) where

$$B = \exp((\log x)^{\frac{1}{2}}). \quad (6.4)$$

Let us consider first only those elements Q of the set E for which the condition

$$Q > \exp((\log x)^{\frac{2}{5}})$$

is satisfied; we shall call this condition "condition 1".

Further, we suppose that if $Q = p_1 q_1$, that is if p_1 denotes the greatest prime factor of Q , then p_1 is not exceptional in the sense of Lemma 4. This supposition we shall call "condition 2". If both these conditions are fulfilled then we apply to (6.1) the decomposition (2.23) and separate in (6.1) the terms corresponding to characters which are primitive with respect to p_1 . Taking into account that $(l, Q) = 1$, and that therefore $\chi_{p_1}^0(l) = 1$ further that $\chi_{p_1}^0(p) = 1$ except for $p = p_1$, we obtain, using Lemma 4 that

$$P(x, Q) = \frac{1}{\phi(p_1)} P(x, q_1) + O\left[x^{1 - \frac{\delta_2}{k_1 + 1}}\right]. \quad (6.5)$$

If $q_1 = p_2 q_2$ satisfies also conditions 1 and 2, then the process can be continued. We obtain

$$P(x, Q) = \frac{1}{\phi(p_1 p_2)} P(x, q_2) + O\left[x^{1 - \frac{\delta_2}{k_1 + 1}}\right] + O\left[\frac{x^{1 - \frac{\delta_2}{k_2 + 1}}}{\phi(p_1)}\right], \quad (6.6)$$

where $k_2 = \frac{\log q_2}{\log(p_2/2)} + 1$ and so on, until after a certain number — say s — steps at least one of the conditions 1 and 2 will not be fulfilled.

If condition 1 fails to be fulfilled, that is if $q_s < \exp((\log x)^{2/5})$, then we use Lemma B and under the condition $Q_1 + q_{s+1}$ we obtain

$$P(x, Q) = \frac{x}{\phi(Q) \log x} + O\left[\sum_{r=1}^s \frac{x^{1 - \frac{\delta_2}{k_r + 1}}}{\phi\left[\frac{Q}{q_{r-1}}\right]}\right] + O\left[\frac{x e^{-c 16 \sqrt{\log x}}}{\phi\left[\frac{Q}{q_s}\right]}\right], \quad (6.7)$$

while if $Q_1 | q_{s+1}$ then one has to add to (6.7) the term

$$O\left[\frac{x^{1 - \frac{c(\epsilon)}{Q_1^\epsilon}}}{\phi(Q)}\right]. \quad (6.8)$$

Here $q_1, q_2, \dots, q_s$ are diagonal divisors of Q and

$$k_r = \frac{\log q_r}{\log \frac{p_r}{2}} + 1. \quad (6.9)$$

If condition 2 is not satisfied, that is if the prime p_{s+1} is exceptional with respect to q_{s+1} , then Lemma C gives us

$$P(x, Q) = O\left(\frac{x}{\phi(Q)}\right) + O\left(\sum_{r=1}^s \frac{x}{\phi\left(\frac{Q}{q_{r-1}}\right)}\right). \quad (6.10)$$

Thus the estimation of the remainder term in (1.11) leads to terms of four different types, namely:

$$\text{I: } \frac{x}{\phi(Q)}, \quad \text{II: } \frac{x e^{-c_{16}\sqrt{\log x}}}{\phi\left(\frac{Q}{q_s}\right)}, \quad \text{III: } \frac{x^{1-\frac{c(\epsilon)}{Q_1^\epsilon}}}{\phi(Q)}, \quad \text{IV: } \frac{x^{1-\frac{\delta_2}{k_r+1}}}{\phi\left(\frac{Q}{q_{r-1}}\right)}.$$

We shall denote the sum of all terms of types I, II, III, resp. IV, by R_I, R_{II}, R_{III} resp. by R_{IV} .

3. Now we shall add separately the terms belonging to the above mentioned four types.

Let us start with type I. Fixing the values of Q/q_s and q_{s+1} and taking the sum of all terms corresponding to all possible values of p_{s+1} (that is, for all primes p_{s+1} which are exceptional with respect to q_{s+1}) we obtain the estimate

$$c_{28} \frac{x}{\phi\left(\frac{Q q_{s+1}}{q_s}\right)} \cdot \sum_{p_{s+1} \geq 2 \exp((\log x)^{1/3})} \frac{1}{p_{s+1}}. \quad (6.11)$$

Applying to the exceptional primes satisfying (6.2) Lemma 9 with $B = 2 \exp((\log x)^{1/3})$ we obtain that (6.11) does not exceed

$$\frac{c_{29} x (\log x)^{1/3}}{\phi\left(\frac{Q q_{s+1}}{q_s}\right) e^{(1/4)(\log x)^{1/3}}}. \quad (6.12)$$

Summing over values of $Q q_{s+1}/q_s$ and applying Lemma 10 we obtain for the sum of all terms of type I the estimate

$$R_I < \frac{c_{30} x (\log x)^{4/3}}{e^{(1/4)(\log x)^{1/3}}} < \frac{x}{(\log x)^3} \quad \text{for } x \geq c_{31}. \quad (6.13)$$

4. Let us consider now the terms of type II. Fixing the values of Q/q_s we obtain the estimate

$$\frac{c_{32} x \exp[(\log x)^{2/5} - c_{16}\sqrt{\log x}]}{\phi\left(\frac{Q}{q_s}\right)}, \quad (6.14)$$

because the summation has to be extended only over values of q_{s+1} less than $\exp((\log x)^{2/5})$. Summation over values of Q/q_s and an application of Lemma 10 gives

$$R_{II} < \frac{x}{(\log x)^3} \quad \text{for } x \geq c_{33}. \quad (6.15)$$

5. Fixing the value of Q/q_s the summation of terms of type III has to be extended over such values of q_{s+1} which are multiples of Q_1 , (if the latter exists). According to the Lemmas 10 and 11 we get the estimate

$$\frac{c_{34} \log^2 x}{\phi \left[\frac{Q}{q_s} \right]} \cdot \frac{x^{1 - \frac{c(\epsilon)}{Q_1^\epsilon}}}{Q_1}. \quad (6.16)$$

Summing over values of Q/q_{s+1} gives the estimate

$$R_{III} < c_{35} x \log^3 x \cdot \exp \left[- \frac{c(\epsilon)}{Q_1^\epsilon} \log x - \log Q_1 \right]. \quad (6.17)$$

As we do not know anything about the value of Q_1 we have to take the maximal value of the right-hand side of (6.17) for $1 \leq Q_1 < +\infty$; this means that we have to find the minimum of

$$\frac{c(\epsilon)}{Q_1^\epsilon} \log x + \log Q_1.$$

By taking the derivative and equating it to 0 it is easy to see that this minimum is equal to

$$\frac{1}{\epsilon} \log \log x + \frac{1}{\epsilon} \log (e c(\epsilon)), \quad (6.18)$$

and is attained for $Q_1 = (\epsilon \cdot c(\epsilon) \cdot \log x)^{1/\epsilon}$. According to Siegel's theorem we may choose for ϵ an arbitrary positive number. By choosing $\epsilon = 1/8$, we obtain for the sum of all terms of type III the estimate

$$R_{III} < \frac{x}{\log^3 x} \quad \text{for } x \geq c_{36}. \quad (6.19)$$

6. Now we have to estimate the sum of the terms of type IV. By fixing $\frac{Q}{q_{r-1}}$ let us consider first those terms of type IV for which $k_r < 2$. For the number of such terms we use the trivial estimate that this number cannot exceed the total number of elements of the set E , and thus, by Lemma 7, is less than $x^{9/R}$. Thus the sum of such terms cannot exceed

$$\frac{c_{37}}{\phi \left[\frac{Q}{q_{r-1}} \right]} x^{1 - \left\{ \frac{\delta_2}{2} - \frac{9}{R} \right\}}.$$

Summing over values of Q/q_{r-1} we obtain for the sum of these terms, which we shall denote by $R_{IV}^{(1)}$, the estimate

$$R_{IV}^{(1)} < c_{38} x^{1 - \left[\frac{\delta_2}{2} - \frac{2}{R} \right] \log x} \text{ for } x \geq c_{39}.$$

By choosing R so that $R > 27/\delta_2$ should hold, we obtain

$$R_{IV}^{(1)} < \frac{x}{\log^3 x} \text{ for } x \geq c_{40}. \quad (6.20)$$

7. Let us consider now the terms of type IV for which

$$2\nu \leq k_r < 2\nu + 2, \quad (\nu = 1, 2, \dots, \left[\frac{11}{2} \log \log x \right]).$$

As $k_r \geq 2\nu$, further $q_r > \exp((\log x)^{2/5})$ and $\nu \leq \frac{11}{2} \log \log x$ we obtain

$$p_r < 2q_r^{\frac{1}{2\nu-1}} < q_r^{\frac{1}{\nu}}.$$

Let us fix the value of Q/q_{r-1} . Summing over all possible values of ν and applying Lemma 8, we obtain that the sum of these terms does not exceed

$$\frac{\frac{c_{23}^\nu}{x R h^{\nu/2}} \cdot x^{1 - \frac{\delta_2}{2\nu+4}}}{\phi \left[\frac{Q}{q_{r-1}} \right]}. \quad (6.21)$$

Let us now fix definitely the value of R by putting

$$R = \frac{450 c_{23}}{\delta_2} = 18 \cdot 10^6 \cdot K_3 \cdot c_{23}.$$

(By this choice of the value of R the condition $R > 27/\delta_2$ which has been postulated previously is clearly satisfied too.) In this case we have for all $\nu \geq 1$

$$\frac{c_{23}^\nu}{R h^{\nu/2}} < \frac{\delta_2}{2(2\nu+4)}.$$

Thus, we obtain from (6.21) the estimate

$$\frac{x^{1 - \frac{\delta_2}{4(\nu+2)}}}{\phi \left[\frac{Q}{q_{r-1}} \right]}. \quad (6.22)$$

Summing over all values of ν and Q/q_{r-1} we obtain for the sum of the terms considered, which we denote by $R_{IV}^{(2)}$, the estimate

$$R_{IV}^{(2)} < c_{41} \log x \cdot \sum_{\nu=1}^{\left[\frac{11}{2} \log x \right]} x^{1 - \frac{\delta_2}{4(\nu+2)}}. \quad (6.23)$$

Replacing all terms of the sum on the right of (6.23) by the largest among them (that is, by the last term) we get

$$R_{IV}^{(2)} < \frac{x}{\log^3 x} \text{ for } x \geq c_{42}. \quad (6.24)$$

Thus, collecting the results (6.13)–(6.24) by choosing for R the value $R = 18 \cdot 10^6 \cdot K_3 \cdot c_{23}$ we obtain finally that for $x \geq c_{43}$

$$\sum_{Q \in E} |R_Q(x)| < R_I + R_{II} + R_{III} + R_{IV}^{(1)} + R_{IV}^{(2)} < \frac{5x}{\log^3 x} \quad (6.25)$$

and therefore it follows that

$$H(2N) > \frac{c_1 N}{\log^2 N}$$

for $N \geq c_{43}$. As pointed out in Chapter 1, this proves Theorem 1.

8. To prove Theorem 2 we consider (instead of (1.2))

$$H_0(N) = \sum_{\substack{3 \leq p \leq N \\ (p+2, \Delta_0)=1}} a_p. \quad (6.26)$$

Everything else remains essentially unchanged and similarly as we proved Theorem 2, we prove that

$$H_0(N) > \frac{c_1 N}{\log^2 N}$$

for $N \geq c_{43}$. Thus the number of primes $p \leq N$ for which $p+2$ is almost prime, is greater than $\frac{c_1 N}{\log^3 N}$. This proves Theorem 2.

9. Evidently odd numbers can be also represented as the sum of a prime and an almost prime. Without any essential change in the proof we obtain

Theorem 1a. *Every odd integer $2N+1$ can be represented in the form $2N+1 = p+2P$, where p is a prime and P is an odd integer, the number of prime factors of which is bounded by a constant.*

We can generalize Theorem 2 also, without any further difficulty, as follows:

Theorem 2a. *For every fixed (positive or negative) integral value of m there exist an infinity of primes p such that $p+m$ is "almost prime", i.e., the number of prime factors of $p+m$ is bounded by a constant.**

These theorems are capable of further generalization, but we restricted ourselves here to the formulation of the simplest results which are closely related to famous unsolved problems of number theory.

BIBLIOGRAPHY

- [1] I. M. Vinogradov, *A new method in the analytic theory of numbers*, Trudy Mat. Inst. Steklov. 10 (1937). (Russian)
- [2] N. G. Čudakov, *The density of even numbers which cannot be represented as the sum of two primes*, Izv. Akad. Nauk SSSR. Ser. Mat. No. 1 (1938), 25–40. (Russian. English summary)
- [3] L. G. Šnirelman, *On additive properties of numbers*, Uspehi Mat. Nauk 7 (1940), 7–46. (Russian)
- [4] Viggo Brun, *Le crible d'Ératosthène et le théorème de Goldbach*, Norske Videnskapselskapets Skrifter I. Kristiania, 1920, no. 3.

* Author's remark: The constant in question may depend on m .

- [5] A. A. Buhštab, *On the representation of even numbers as the sum of two numbers with a bounded number of prime factors*, Dokl. Akad. Nauk SSSR 29 (1940), 544–548. (Russian)
- [6] V. A. Tartakovskiĭ, *The method of the selective "approximative sieve"*, Dokl. Akad. Nauk SSSR 23 (1939), 127–130. (Russian)
- [7] Th. Estermann, *Eine neue Darstellung und neue Anwendungen der Viggo Brunschen Methode*, J. Reine Angew. Math. 168 (1932), 106–116.
- [8] A. A. Buhštab, *On an additive representation of integers*, Mat. Sb. (N.S.) 10 (52) (1942), 87–91. (Russian)
- [9] Yu. V. Linnik, *On Dirichlet's L -series and prime-number sums*, Mat. Sb. (N.S.) 15(57) (1944), 3–12. (Russian summary)
- [10] Yu. V. Linnik, *On the possibility of avoiding the generalized Riemann hypothesis in studying the primes in an arithmetic progression*, Dokl. Akad. Nauk SSSR 44(1944), 147–150. (Russian)
- [11] P. Turán, *Über die Wurzeln der Dirichletschen L -Funktionen*, Acta Univ. Szeged Sect. Sci. Math. 10(1943), 188–201.
- [12] C. L. Siegel, *On the zeros of the Dirichlet L -functions*, Ann. of Math. (2) 46 (1945), 409–422.
- [13] Yu. V. Linnik, *The large sieve*, Dokl. Akad. Nauk SSSR 30 (1941), 290–292. (Russian)
- [14] E. C. Titchmarsh, *A divisor problem*, Rend. Circ. Mat. Palermo 54 (1930), 414–429.
- [15] A. Page, *On the number of primes in an arithmetic progression*, Proc. London Math. Soc. (2) 39 (1935), 116–141.
- [16] C. L. Siegel, *Über die Klassenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), 83–86.
- [17] J. E. Littlewood, *On the class number of the corpus $P(\sqrt{-k})$* , Proc. London Math. Soc. (2) 27 (1927/28), 358–372.
- [18] A. Rényi, *On the representation of even numbers as the sum of a prime and an almost prime number*, Dokl. Akad. Nauk SSSR 56 (1947), 455–458. (Russian)

Translated by:

A. Rényi

NOTE

This is an English version of the paper [9] which can be considered as one of Rényi's most significant papers. Its significance is twofold. First it opened a new possibility to approach the binary Goldbach conjecture, giving the first theorem of the sort that all sufficiently large numbers can be represented in the form $p + P_k$ where p prime and P_k is an integer having at most k prime factors (k absolute constant). This was gradually improved as to the value of k ; the last step was made by Chen [1] who proved it with $k = 2$ (which seems to be the limit of the strength of the method). Secondly Rényi was the first who succeeded in averaging the number of zeros of $L(s, k, \chi)$ -functions of Dirichlet not only with respect to variable χ and fixed k but also nontrivially at variable k which was in all development a very important step and apparently completely forgotten that it is due to him. He achieved it by strengthening a theorem of Linnik (see 1 and 1b in Rényi's paper No. 29) to a general "almost equidistribution" theorem called now the large sieve of Linnik—Rényi. We shall discuss first its development and then we shall turn to its applications to L -functions and in turn to arithmetics.

Rényi's most elegant sieve estimation can be found in his paper No. 29; this asserts that if

$$1 \leq n_1 < n_2 < \dots < n_Z \leq N$$

are integers, $Q \leq N^{1/2}$ and for a prime p $Z(p, a)$ denotes the number of n_j 's $\equiv a \pmod p$ then the inequality

$$(1) \quad \sum_{p \leq Q} p \sum_{a=0}^{p-1} \left(Z(a, p) - \frac{Z}{p} \right)^2 = O(Z) (Q^3 + N)$$

holds. The next, perhaps the most important, step ahead was made after a silence of 15 years by K. F. Roth [2], leaving the probabilistic approach; he replaced the right side by $O(ZQ^2 \log Q)$ for $Q = O \left(\sqrt{\frac{N}{\log N}} \right)$. Then the events followed quickly. Bombieri [3] found the very useful generalization, that if a_n are arbitrary complex numbers, further

$$(2) \quad S(\alpha) = \sum_{n=M+1}^{M+N} a_n e^{2\pi i n \alpha}, \quad Z^* = \sum_{n=M+1}^{M+N} |a_n|^2$$

then the inequality

$$(3) \quad \sum_{q \leq Q} \sum_{a=1}^q \left| S \left(\frac{a}{q} \right) \right|^2 = O(Z^*) (Q^2 + N)$$

holds. Here the summation for q runs for all $q \leq Q$; keeping only the primes $\leq Q$ the left side of (3) coincides with that of Rényi's (1). Significant further generalisation of (3) was attained by Davenport and Halberstam [4], replacing

the $\frac{a}{q}$ numbers in (3) by real α_r 's satisfying

$$(4) \quad ||\alpha_\mu - \alpha_\nu|| \geq \delta, \quad 1 \leq \mu \neq \nu \leq R \quad (R \text{ arbitrary})$$

where $||x||$ stands for the distance of x from the next integer. Very elegant short proofs were afterwards given, returning essentially to Linnik's approach by Gallagher [5]. The ultimate reason of the large sieve was found by A. Selberg by the inequality

$$(5) \quad \sum_{j=1}^R |(f, \varphi_j)|^2 \left\{ \sum_{k=1}^R |(\varphi_j, \varphi_k)| \right\}^{-1} \leq |f|^2$$

where $f, \varphi_1, \varphi_2, \dots, \varphi_R$ are arbitrary elements of a Hilbert space. Proper application of this led Bombieri to the inequality

$$(6) \quad \sum_{r=1}^R |S(\alpha_r)|^2 \leq \left(N + \frac{2}{\delta} \right) Z^*.$$

Montgomery's inequality (see [7]) is "generally" somewhat stronger; it replaces the first factor on the right of (6) by

$$(7) \quad N + \frac{2}{\delta\sqrt{3}} + 3.$$

The content of the large sieve in the form (1) can be described at the simplest so that "very many" $Z(p, a) = 0$ implies an upper bound for Z . In contrast to it the "small" sieve of Brun gives an upper bound for Z when sieving out a "few" residue classes $f(p)$ in number modulo the sieving primes p . In principle Brun's method has to work without this restriction; most probably, however, this works only when $f(p)$ increases "very slowly" with p . The more remarkable is then the fact — and this illuminates the connection of the small and large sieves — that rather strong "small sieve"-results could be *deduced*

from large sieve. The first result of this type was discovered by Bombieri and Davenport [6]; a more general form was found by Montgomery. This last one asserts that leaving out all integers from the interval $M + 1 \leq n \leq M + N$ which belong to $f(p)$ prescribed residue classes mod p where p runs over all primes $\leq Q$ the number of the remaining ones in $[M + 1, M + N]$ cannot exceed

$$(8) \quad \frac{N + 2Q^2}{\sum_{q \leq Q} \mu(q)^2 \prod_{r|q} \frac{f(p)}{p - f(p)}}.$$

Here $f(p)$ can be chosen from 1 to $p - 1$.

The large sieve was extended to algebraic number fields by Rieger [8],

Huxley [9] and Wilson [10]. For an extension to lattices in E_n see Hlawka [11].

Now we turn to applications of the large sieve to distribution of zeros of the $L(s, k, \chi)$ functions of Dirichlet. Let $N(T, \alpha, k, \chi)$ stand for the number of zeros of $L(s, k, \chi)$ for

$$(9) \quad \sigma \geq \alpha, |t| \leq T,$$

further $N(T, \alpha, k)$ for the total number of zeros of $L(s, k, \chi)$ functions in (9) for a fixed k (all according to their multiplicity). Known were before the large sieve method inequalities of type

$$(10) \quad N(T, \alpha, k) < c(kT)^{A(1-\alpha)} \log^B kT.$$

(Linnik, A. Selberg, Siegel, Turán); here c are immaterial A, B important positive constants, $\frac{1}{2} \leq \alpha \leq 1$, $T \geq 2$. Rényi's seminal result in this direction formulated explicitly in 9* could have been formulated as a nontrivial upper bound for

$$\sum_{p \leq Q} \sum_{\chi \neq \chi_0 \bmod p} N(T, \alpha, p, \chi).$$

Using the large sieve and additional device Bombieri [3] deduced the first properly formulated theorem in this direction by giving the inequality

$$(11) \quad \sum_{k \leq Q} \sum_{\chi \bmod k}^* N(T, \alpha, k, \chi) < cT(Q^2 + QT)^{\frac{4(1-\sigma)}{3-2\sigma}} \log^{10} QT$$

where the star means that the summation must be extended only to primitive characters. This was later much improved by Montgomery, Jutila and Huxley combining the large sieve with an ingenious idea of Halász which — as it turned out later — can be also deduced from (5).

As to the distribution of primes in various residue classes mod k the following theorem was known (see [12]). Suppose $\delta > 0$ is arbitrarily small, fixed, further $N = N(k)$ is chosen for each k so that

$$N > k \log^3 k$$

further that the Riemann—Piltz conjecture is true. Then for the number $h(k)$ of residue classes $\equiv l \bmod k$ for which the inequality

$$(12) \quad \left| \pi(N, k, l) - \frac{1}{\varphi(k)} L_l N \right| \leq \frac{\delta}{\varphi(k)} L_l N$$

holds, the relation

$$(13) \quad \lim_{k \rightarrow \infty} \frac{h(k)}{\varphi(k)} = 1$$

is true. Quite remarkably new was in 1949 Rényi's theorem (see his No. 29) on the possibility of an unconditional proof of such a theorem. Nobody dreamt at that time that it is a real possibility to prove that apart from $O(N^{1/4} \log N)$ p primes not exceeding $N^{1/3}$ at most, all remaining primes $\leq N^{1/3}$ have the property that the inequality

$$(14) \quad \pi(N, p, l) = \frac{\pi(N)}{p-1} + O\left(\frac{\pi(N)}{p^{5/4} \log N}\right)$$

holds for all $(l, p) = 1$, with exception $O(p^{3/4})$ such residue classes. Barban [13] made more than 10 years later the first (incomplete) attempt to deduce from density theorems a nontrivial upper bound for

$$\max_{k \leq x} \max_{(l, k)=1} \left| \psi(x, k, l) - \frac{x}{\varphi(k)} \right|$$

$\psi(x, k, l)$ standing for

$$\sum_{\substack{n \leq x \\ n \equiv l \pmod{k}}} \Lambda(n).$$

Such a theorem was rigorously proved first by Bombieri [3] using (11) and gave for any fixed $A > 0$ the inequality

$$(15) \quad \sum_{k \leq \sqrt{x} \log^{-A} x} \max_{y \leq x} \max_{(l, k)=1} \left| \psi(x, k, l) - \frac{y}{\varphi(k)} \right| < cx \log^{-A} x.$$

Gallagher [14] gave a much shorter proof of (15) with a slightly worse exponent than $(3A + 23)$, rediscovering also a very nice idea of Heilbronn's thesis (see [15]).

Denoting by $P(k, l)$ the smallest prime $\equiv l \pmod{k}$ Linnik proved (see [16]) the existence of an absolute constant B so that

$$(16) \quad P(k, l) < k^B.$$

Linnik's proof for his theorem did not use large sieve and is perhaps one of the most complicated proofs ever written down in the literature. The essential difficulty was to remove the log factor in (10); it turned out also that it is enough to take "small" parallelograms only. Linnik's proof was replaced by considerably simpler ones by Rodosskij [17], Turán [18], Knapowski [19], again without using the large sieve. Fogels [20] could prove (10) without the log-factor for "large" parallelograms, again without large sieve. It was Gallagher [21] who proved — using the large sieve and other devices — for all $T \geq 1$, $\frac{1}{2} \leq \alpha \leq 1$ the inequality

$$(17) \quad \sum_{k \leq T} \sum_{\chi \pmod{k}}^* N(T, \alpha, k, \chi) < cT^{A(1-\alpha)},$$

i.e. uniformly without a log factor. From this he deduced in the case of non-existence of Siegel-zero the following important inequality. For suitable positive absolute constants A_1 and B_1 the inequality

$$(18) \quad \sum_{2 \leq k \leq Q} \sum_{x \bmod k}^* \left| \sum_Y^{Y+h} \chi(p, k) \log p \right| < ch \exp \left(-A_1 \frac{\log Y}{\log Q} \right)$$

holds where

$$(19) \quad \frac{Y}{Q} \leq h \leq Y, \quad \exp(\sqrt{\log Y}) \leq Q \leq Y^{B_1};$$

if there is a Siegel zero (18) must be a little changed.

The list of arithmetical applications of the large sieve started with the following theorem of Linnik (for which he devised the large sieve). Let ε be arbitrarily small fixed positive quantity, $n(p)$ the smallest quadratic nonresidue mod p and $f_\varepsilon(x)$ stands for the number of p primes satisfying

$$(20) \quad x^\varepsilon \leq p \leq x \text{ and } n(p) \geq p^\varepsilon.$$

Then Linnik's theorem asserts that

$$(21) \quad f_\varepsilon(x) \leq c(\varepsilon) \log \log x$$

independently of x . I. M. Vinogradov conjectured since many years the inequality

$$n(p) < c(\varepsilon) p^\varepsilon;$$

(21) is a strong support to its truth. Then came Rényi's application to the quasigoldbach conjecture in 1947 which was followed by P. T. Bateman, S. Chowla and Erdős in 1950 (see [23]) who proved by it inequalities of type

$$(22) \quad \lim_{\substack{p \rightarrow \infty \\ p \equiv 1(4)}} \frac{\sum_{n=1}^{\infty} \left(\frac{n}{p} \right) \frac{1}{n}}{\log \log p} > \frac{1}{18} e^\gamma.$$

(γ the Euler-constant)

Then a longer silence followed which was broken only after the more transparent formulations of Roth and Bombieri. The main source of applications was Bombieri's formula (15) and for some purposes also Barban's formula in [13]

$$(23) \quad \sum_{k \leq x \log^{-B} x} \sum_{(l, k)=1}^* \left\{ \psi(x, k, l) - \frac{x}{\varphi(k)} \right\}^2 < cx^2 \log^{-A} x$$

where B can be taken — with an improvement of Gallagher (see [5]) — as $A + 1$. They refer first to two theorems proved unconditionally first by

Linnik (see [24]). The first asserts that all sufficiently large integers n can be represented in the form

$$(24) \quad p + x^2 + y^2 \quad (p \text{ prime, } x, y \text{ integers})$$

conjectured by Hardy-Littlewood and the second refers to the formula (a fixed, $x \rightarrow \infty$)

$$(25) \quad \sum_{a < p \leq x} d(p-a) = (1 + o(1))x \prod_{p|a} \left(1 - \frac{1}{p}\right) \prod_p \left\{1 + \frac{1}{p(p-1)}\right\},$$

proved first by Titchmarsh on the supposition of the Riemann—Piltz conjecture. (25) was deduced shortly from (15) by Rodriguez (see [25]) and (24) by Elliot and Halberstam (see [26]), combining it with ideas of Hooley. It is rather remarkable that Linnik's proofs for (24) and (25) do not use the large sieve at all and — as far as I know — he never used the method after proving (21) by it. The same holds essentially on Rényi. Another type of application of (15) was given by Gallagher (see [5]) who proved in connection with Artin's well known conjecture that the number of integers not exceeding N which are not primitive roots to some prime modulus $\leq \sqrt{N}$ cannot exceed the order $\sqrt{N} \log N$ (which is nearly best possible).

This list on results and applications of the large sieve is rather incomplete (and do not touch the applicability e.g. in combinatorics which is in statu nascendi). But confining ourselves to analytical number theory we can assert that at present the large sieve method has become one of the most effective methods of the analytical number theory and will be until the full Riemann—Piltz conjecture will be decided for the positive (which is not certain at all). (P. T.)

REFERENCES

- [1] According to a communication of Prof. H. Diamond it appeared in *Scientia Sinica* 1973 (after being announced in 1966).
- [2] Roth, K. F.: On the large sieve of Linnik and Rényi. *Matematika*, **12** (1965), 1–9.
- [3] Bombieri, E.: On the large sieve. *Ibid.*, 201–225.
- [4] Davenport, H. and Halberstam, H.: The values of a trigonometrical polynomial at well-spaced points. *Ibid.*, **13** (1966), 91–96.
- [5] Gallagher, P. X.: The large sieve. *Ibid.*, **14** (1967), 14–20.
- [6] Bombieri, E. and Davenport, H.: On the large sieve method. Abh. aus Zahlentheorie und Analysis. *Zur Erinnerung an Edmund Landau*. Deutsch. Verlag der Wiss. Berlin 1968, 11–22.
- [7] Montgomery, Hugh L.: Topics in multiplicative Number theory. *Lecture Notes in Mathematics* 227. Springer Verlag 1971.
- [8] Rieger, G. J.: Zum Sieb von Linnik. *Arch. der Math.* (1960), 14–22 and Das grosse Sieb von Linnik für algebraische Zahlen. *Ibid.*, (1961), 184–187.
- [9] Huxley, M. N.: The large sieve inequality for algebraic number fields. *Matematika*, **15** (1968), 178–187.
- [10] Wilson, R. J.: The large sieve in algebraic number fields. *Matematika*, **16** (1969), 189–204.
- [11] Hlawka, E.: Bemerkungen zum grossen Sieb von Linnik. *Österr. Akad. der Wiss. Math.-Naturw. Klasse*, (1970), 13–18.

- [12] Turán, P.: Über die Primzahlen der arithmetischen Progression. *Acta Litt. ac Scient. Szeged*, VIII (1937), 226–235.
- [13] Barban, M. B.: On the average error in the generalised prime number theorem. *Dokl. Akad. Nauk UZSSR*, (1964), 5–7.
- [14] Gallagher, P. X.: Bombieri's mean value theorem. *Mathematica*, (1968), 1–6.
- [15] Heilbronn, H.: Über den Primzahlsatz von Herrn Hoheisel. *Math. Zeitschr.*, (1933), 394–423.
- [16] Linnik, Yu. V.: On the least prime number in an arithmetic progression I. The basic theorem. *Mat. Sbornik*, (1947), 139–178, II. The Deuring-Heilbronn phenomenon. *Ibid.*, 347–368.
- [17] Rodossij, K. A.: On the smallest prime in an arithmetical progression. *Mat. Sbornik*, (1954), 331–356 (in Russian).
- [18] Turán, P.: On a density theorem of Yu. V. Linnik. *Publ. Math. Inst. of Hung. Acad. Sci.*, VI (1961), 165–179.
- [19] Knapowski, S.: On Linnik's theorem concerning exceptional L-zeros. *Publ. Math. Debrecen*, (1962), 168–178.
- [20] Fogels, E.: On the zeros of L-functions. *Acta Arith.*, XI (1965), 67–96.
- [21] Gallagher, P. X.: A large sieve density estimate near $\sigma = 1$. *Inventiones Math.*, (1971).
- [22] Linnik, Ju. V.: The large sieve. *Dokl. Akad. Nauk SSSR*, (1941), 292–294.
- [23] Bateman, P. T., Chowla, S. and Erdős, P.: Remarks on the size of $L(1, \chi)$. *Publ. Math. Debr.*, (1949–50), 165–182.
- [24] Linnik, Yu. V.: The dispersion method in binary additive problems. *American Math. Soc.*, 1963.
- [25] Rodriguez, G.: Sul problema dei divisori di Titchmarsh. *Bull. Unione Matem. Ital.*, (1965), 358–366.
- [26] Elliott, P. D. T. A. and Halberstam, H.: Some applications of Bombieri's theorem. *Matematika*, (1966), 196–203.

ON A PROBLEM IN THE THEORY OF GRAPHS

P. ERDŐS and A RÉNYI

INTRODUCTION

In this paper we study a graph-theoretical problem that is derived from the following question: one wants to establish two-way connections between a given number of airports such that one can reach any airport from any other directly without landing or with one change of planes, where the airports have bounded capacities, i.e. there is a prescribed limit as to how many airports may have direct connections with any given one; the question is how can one design the network of air connections that satisfies the above requirements such that the number of connections be as small as possible? The graph-theoretical formulation of this problem is arrived at as follows: to every airport assign a point as a vertex of the graph to be constructed. So, if we denote the number of airports by n , then our graph will have n vertices. Connect to vertices with an undirected edge if there is a direct air connection between the corresponding airports. Our conditions now require that the graph so obtained (which is undirected and has no loops or multiple edges) have “diameter” ≤ 2 and the maximum of the valencies of its vertices be equal to a given number, say k . Here the diameter of a connected graph is the least integer d such that any two vertices of the graph can be joined by a path consisting of at most d edges. A path is, by definition, a sequence of edges $P_i P_{i+1}$ ($i = 1, 2, \dots, s$), where $P_1, \dots, P_{s+1}$ are distinct points of the graph. For given n and k , we look for those graphs among the ones (if any) satisfying the above conditions that have the minimal number of edges. This latter number, which clearly depends only on n and k , will be denoted by $F_2(n, k)$. Denote by G_n an arbitrary graph with n vertices, by $P_1, P_2, \dots, P_n$ its vertices, by $v(P_j)$ the valency of the vertex P_j in G_n i.e. the number of those vertices of G_n which are joined with P_j by an edge, by $d(G_n)$ the diameter of G_n , and by $N(G_n)$ the number of its edges; then, denoting by $H_2(n, k)$ the set of all graphs G_n having $P_1, \dots, P_n$ as vertices for which $d(G_n) \leq 2$ and $\max_{1 \leq j \leq n} v(P_j) = k$, we have

$$(1) \quad F_2(n, k) = \min_{G_n \in H_2(n, k)} N(G_n),$$

provided the set $H_2(n, k)$ is not empty; otherwise set $F_2(n, k) = +\infty$. The subscript 2 in $F_2(n, k)$ and $H_2(n, k)$ indicates that only graphs having diameter ≤ 2 are considered. It is clear that the problem can be generalized by assuming only that any airport can be reached from any other by at most $r - 1$ change of planes instead of allowing just one change ($r \geq 2$). In other words, among the graphs with n vertices and with diameter $\leq r$ such that the maximum of the valencies of the vertices is k , find those having a minimum number of edges. This latter number is denoted by $F_r(n, k)$, and we have

$$(2) \quad F_r(n, k) = \min_{G_n \in H_r(n, k)} N(G_n),$$

where $H_r(n, k)$ denotes the set of those graphs G_n having $P_1, \dots, P_n$ as vertices for which $d(G_n) \leq r$ and $\max_{1 \leq j \leq n} v(P_j) = k$. If $H_r(n, k)$ is empty then $F_r(n, k) = +\infty$.

In §§ 1 and 2 of this paper we deal with the case $r = 2$. The case $r > 2$ will be touched upon in § 3; we intend to return to a detailed discussion of this case in a subsequent paper.

In § 1 we study the behaviour of the function $F_2(n, k)$ in case n and k are large numbers, and we give a formula for $F_2(n, k)$ that is asymptotically exact. In § 2 we give an algorithm that constructs certain graphs that are asymptotically the best.

We note that if we found a graph with a minimal number of edges that has diameter ≤ 2 and n vertices such that the maximum of the valencies of the vertices is k and we are given n other vertices, then these vertices can be put in a one-to-one correspondence with the vertices of the graph in $n!$ different ways. From among these correspondences one can select those which are optimal in some other respects as well. E.g. if the distances between the airports are given, then from among those air connection networks that have the minimal number of connections under the given conditions one can select that network for which the *total length* of the connections is minimal.

Our problem can also be considered as one in the field of nonlinear programming. Let $E = (\varepsilon_{ij})$ be a symmetrical matrix of type $n \times n$ having only 1 and 0 as elements such that all elements in the diagonal are equal to 1, and the maximum of the sums of elements in the rows is $k + 1$, and furthermore all elements of the matrix E^2 are ≥ 1 ; minimize the sum $\sum_{i=1}^n \sum_{j=1}^n \varepsilon_{ij}$ under these conditions.

We study the question in its graph-theoretical formulation.

In accordance with the nature of the problem, we only use elementary methods; for the algorithm, however, we also make use of the theory of finite fields and finite geometries. This is not the first case that the theory of finite fields proved to be a useful tool in solving graph-theoretical problems; the situation was similar in an earlier work [1] of ours investigating asymmetries of graphs. (See also [2].)

In § 3 we mention a few further results and unsolved problems concerning graphs of diameter 2.

We avail ourselves of the opportunity to express our gratitude to Tibor Gallai for his valuable remarks which we made free use of in the final draft of this paper.

§ 1. SOME INEQUALITIES

First we study the following question: for which integers n and k can there exist a graph of diameter 2 with n vertices such that the maximum of the valencies of the vertices is k . Let G_n be such a graph and let $P_1, \dots, P_n$ be its vertices. There are at most k edges incident to an arbitrary vertex, say P_1 , i.e. one can reach at most k vertices starting from P_1 via a path of length 1 (i.e. a path consisting of a single edge). The number of vertices that can be reached from P_1 via a path of length 2 (i.e. one consisting of two edges) is clearly at most the number of vertices other than P_1 that can be reached via an edge from vertices that can be reached from P_1 via a single edge; so the number of

vertices that can be reached from P_1 via one or two edges is at most $k + k(k - 1) = k^2$. According to our assumptions, however, every vertex other than P_1 can be reached from P_1 via a path of length 1 or 2, and so we must have the inequality

$$(1.1) \quad n \leq k^2 + 1.$$

It is also clear from the proof just given that equality can hold only in case the valency of every vertex is k , i.e. only in case of the regular graph of valency k .

We can have equality in (1.1) in case $k = 2$ or $k = 3$; this is shown in case $k = 2$ by the circuit having five vertices, and in case $k = 3$ by Petersen's

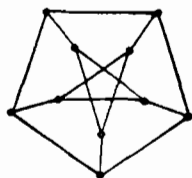


Fig. 1

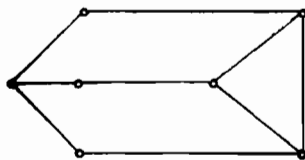


Fig. 2

graph (see Fig. 1). A. J. Hoffman and R. R. Singleton [4] also showed that one can have equality in case $k = 7$; furthermore, they showed that, unless $k = 2, 3$, or 7 , the only case in which it is possible that there exists a regular graph of diameter 2 and valency k having $k^2 + 1$ vertices is $k = 57$; whether or not such a graph exists for $k = 57$ is still an open question.

Since it is well known that the number of vertices with odd valencies is even in any graph, it is clear that no equality can hold in (1.1) if n and k are odd numbers; indeed, in this case we must have at least one vertex of the graph that has valency $k - 1$, and so we have the inequality

$$(1.1') \quad n \leq k(k - 1) + 1,$$

provided n and k are odd. We cannot improve inequality (1.1') in general either, since equality holds in (1.1') in case $k = 3$ and $n = 7$ (see Fig. 2). In all three examples mentioned so far, each graph has the minimal number of edges, and so we have $F_2(5, 2) = 5$, $F_2(10, 3) = 15$, and $F_2(7, 3) = 9$. In the first two cases this follows from Theorem 1 below; the relation $F_2(7, 3) = 9$ will be proved later.

What has been said so far also shows that if $k(n)$ denotes the least integer k for which there exists a graph of diameter 2 having n vertices such that the maximum of the valencies of the vertices equals k , then $k(n)$ is not a monotonic function of n ; indeed, we have $k(9) = 4$ and $k(10) = 3$. It follows from (1.1) nevertheless that we must have the inequality $k(n) \geq \sqrt{n - 1}$.

Now we are going to prove the following

Theorem 1. *The inequality*

$$(1.2) \quad F_2(n, k) \geq \frac{\binom{n}{2}}{k} = \frac{n(n - 1)}{2k}$$

holds.

Proof. Let G_n be a graph of diameter 2 that has n vertices and is such that the maximum of the valencies of the vertices is k . Let N be the number of edges in G_n .

To start with, estimate the number of paths of length ≤ 2 in G_n . Clearly, there are at most N paths of length 1; the number of those paths of length 2 that contain a given edge is obviously at most $2(k-1)$; now, taking into account that each path of length 2 contains two edges, and hence was counted twice just before, we can see that the number of paths of length 2 is at most $(k-1)N$, i.e. the number of paths of length ≤ 2 is at most kN . Now, any two points must be connected with a path of length ≤ 2 , and so the inequality $kN \geq \binom{n}{2}$ must hold. The proof of Theorem 1 is complete.

Inequality (1.2) cannot be strengthened in general; indeed, in case $n = 5$ and $k = 2$ we have $\frac{n(n-1)}{2k} = 5$, and the circuit with five vertices does in

fact have 5 edges, or e.g. in case $n = 10$ and $k = 3$ we have $\frac{n(n-1)}{2k} = 15$, and Petersen's graph shown in Fig. 1 does in fact have 15 edges.

Inequality (1.2) gives 7 as a lower bound for $F_2(7, 3)$. This value cannot, however, be assumed. Indeed, as the number of vertices with odd valencies is even in any graph, in a graph with 7 vertices every vertex cannot have valency 3. So, in a graph of diameter 2 having 7 vertices and such that the maximum of the valencies of the vertices is 3, there must be at least one vertex of valency 2. It is clear that no vertex can have valency 1, since in a graph where the valencies of the vertices is at most 3, at most 5 vertices can be reached from a vertex of valency 1 via a path of length ≤ 2 . If there were only one vertex of valency 2, then the graph would have $\frac{6 \cdot 3 + 2}{2} = 10$ edges.

If there is more than one vertex of valency 2, then the number vertices with valency 2 is 3 or 5. In the former case the graph has $\frac{4 \cdot 3 + 3 \cdot 2}{2} = 9$ edges.

This is indeed possible; such a graph of diameter 2 is shown by Fig. 2. If there were 5 vertices of valency 2, then the number of edges would be $\frac{2 \cdot 3 + 5 \cdot 2}{2} = 8$. Such a graph cannot, however, have diameter 2; indeed,

from a vertex of valency 2 that is connected with two vertices having valencies k_1 and k_2 , respectively, one can reach at most $k_1 + k_2$ vertices via a path of length ≤ 2 , and so each vertex of valency 2 ought to be connected with the two vertices of valency 3; this is, however, impossible, since in this case the valency of these latter points would be 5 and not 3.

So we have shown that $F_2(7, 3) \geq 9$; and since the graph in Fig. 2 has 9 edges, we have $F_2(7, 3) = 9$.

We note that inequality (1.1) can also be derived from Theorem 1. Indeed, a graph with n vertices in which the valencies of the vertices is at most k has at most $nk/2$ edges; so, in view of Theorem 1, a graph of diameter 2 in which the maximum of the valencies of the vertices is k can exist only if we have $\frac{nk}{2} \geq$

$\geq \frac{n(n-1)}{2k}$, i.e. only if $k^2 \geq n-1$, i.e. only if (1.1) holds. One can also see from the proof of (1.2) that equality there can hold only if there exists a regular graph of diameter 2 and of valency k with n vertices, i.e. only if $\frac{nk}{2} = \frac{n(n-1)}{2k}$, i.e. only if $k^2 = n-1$, that is only in case we have equality in (1.1). Furthermore, one can also see from the proof, that if this latter condition holds and there exists a regular graph of diameter 2 and of valency k that has n vertices, then in this graph any two points are connected with exactly one path of length ≤ 2 ; hence such a graph does not contain any triangle or quadrilateral.

According to Theorem 1 we have

$$(1.3) \quad \frac{F_2(n, k) \cdot k}{n(n-1)} \geq \frac{1}{2}.$$

In § 2 we are going to show that Theorem 1 is asymptotically exact in the sense that there exists an infinite sequence of pairs of integers k_j and n_j ($j = 1, 2, \dots$) such that $n_j \rightarrow +\infty$ (and so clearly $k_j \rightarrow +\infty$) and

$$(1.4) \quad \lim_{j \rightarrow +\infty} \frac{F_2(n_j, k_j) \cdot k_j}{n_j(n_j - 1)} = \frac{1}{2}.$$

As we pointed out above, we can have equality in (1.2) only if $k = \sqrt{n-1}$. So if $k > \sqrt{n-1}$ then $F_2(n, k) > \frac{n(n-1)}{2k}$ holds necessarily. Now we are going to show that if k is much larger than $\sqrt{n-1}$, then $F_2(n, k)$ is not only larger than $\frac{n(n-1)}{2k}$, but it is at least nearly twice as large as this latter number. This statement is expressed by

Theorem 2. *If $k^2 > 8n$ then*

$$(1.5) \quad F_2(n, k) \geq \frac{n(n-1)}{k + \frac{8n}{k}}.$$

Remark. In § 2 we shall show that Theorem 2 is asymptotically exact.

Proof of Theorem 2. Let G_n be a graph of diameter 2 that has n vertices and is such that the maximum of the valencies of the vertices is k . Let r denote the number of vertices having valencies $> k/2$; let these vertices themselves be denoted by $P_1, P_2, \dots, P_r$. Let $Q_1, Q_2, \dots, Q_{n-r}$ be the remaining vertices of G_n . Denote by N the number of edges in G_n . Denote by x_j the number of those vertices in G_n whose one end-point is P_j and the other one is among the vertices $Q_1, \dots, Q_{n-r}$; and, furthermore, denote by y_h the number of those vertices in

G_n whose one end-point is Q_h and the other is among the vertices $Q_1, \dots, Q_{h-1}, Q_{h+1}, \dots, Q_{n-r}$. Then we have

$$(1.6) \quad \frac{1}{2} \sum_{h=1}^{n-r} y_h + \sum_{j=1}^r \binom{x'_j}{2} + \sum_{h=1}^{n-r} \binom{y_h}{2} \geq \binom{n-r}{2};$$

indeed, any two vertices Q_i and Q_j ($i \neq j$) are connected either via an edge or via a path $Q_i P_h Q_j$ of length 2 or via a path $Q_i Q_h Q_j$ ($h \neq i, h \neq j$) of length 2.

So taking into account that $x'_j \leq k$ ($j = 1, \dots, r$) and $y_h \leq \frac{k}{2}$ ($h = 1, \dots, n-r$), we obtain

$$(1.7) \quad \frac{k}{2} \sum_{h=1}^{n-r} y_h + k \sum_{j=1}^r x'_j > (n-r)(n-r-1).$$

Since

$$\sum_{j=1}^r x'_j + \frac{1}{2} \sum_{h=1}^{n-r} y_h \leq N,$$

we have that

$$(1.8) \quad kN \geq (n-r)(n-r-1) > n(n-1) - 2rn.$$

Now clearly

$$(1.9) \quad \frac{rk}{2} \leq 2N,$$

and hence

$$N > \frac{n(n-1)}{k + 8n/k}.$$

This completes the proof of Theorem 2.

We note that inequality (1.5) is also valid in case $n-1 \leq k^2 \leq 8n$, this is however not new in respect of Theorem 1, as it gives a worse lower bound for $F_2(n, k)$ in this case than Theorem 1; this is why we announced Theorem 2 only for the case $k^2 > 8n$.

Theorem 2 can also be expressed in the following form: *If $k^2 \geq 8n\lambda$, where $\lambda > 1$, then*

$$(1.10) \quad F_2(n, k) \geq \frac{n(n-1)}{k(1 + 1/\lambda)}.$$

So it follows from Theorem 2 that if k_j and n_j tend to infinity in such a way that

$$(1.11) \quad \lim_{j \rightarrow +\infty} \frac{k_j^2}{n_j} = +\infty$$

then

$$\liminf_{j \rightarrow +\infty} \frac{F_2(n_j, k_j) k_j}{n_j(n_j-1)} \geq 1.$$

In § 2 we shall show that the sequences of integers k_j and n_j can be chosen in such a way that condition (1.11) holds and, moreover, we have

$$(1.12) \quad \lim_{j \rightarrow +\infty} \frac{F_2(n_j, k_j) k_j}{n_j(n_j - 1)} = 1.$$

So inequality (1.5) is asymptotically exact if $k^2/n \rightarrow +\infty$.

§ 2. CONSTRUCTION OF NEARLY EXTREMAL GRAPHS OF DIAMETER 2

To prove that Theorem 1 is asymptotically exact we shall need the following

Lemma 1. *If P is an arbitrary prime power, then there exists a graph of diameter 2 that has $n = P^2 + P + 1$ vertices and in which the maximum of the valencies of the vertices is $P + 1$.*

Remark. The number of edges of the graph the existence of which is asserted in Lemma 1 is clearly $\leq \frac{(P+1)(P^2+P+1)}{2}$; hence if P is a prime power, then in view of Lemma 1 we have

$$\frac{F_2(P^2 + P + 1, P + 1) (P + 1)}{(P^2 + P + 1) (P^2 + 1)} \leq \frac{1}{2} + \frac{1}{2P},$$

and so if k_j runs over numbers of form $P_j + 1$ and $n_j = P_j^2 + P_j + 1$, where P_j is a prime power, then (1.4) holds.

Proof of Lemma 1. Let $GF(P)$ be a finite field of P elements (i.e. a Galois field). We identify the "points" of the geometry $PG(P, 2)$ with the aid of projective coordinates, i.e. the points of this geometry will be represented by triples (a, b, c) , where a, b, c are elements of $GF(P)$ not all of which equal 0 (the null-element of the field $GF(P)$). As usual, if λ is an arbitrary element of $GF(P)$ that differs from 0, then the triples (a, b, c) and $(\lambda a, \lambda b, \lambda c)$ determine the same point. Hence the number of different points of $PG(P, 2)$ is $\frac{P^3 - 1}{P - 1} = P^2 + P + 1$. A straight "line" of the geometry $PG(P, 2)$ is by definition the set of points satisfying the equation $ax + by + cz = 0$, where a, b , and c are arbitrary elements of $GF(P)$ not all of which are equal to 0; the triple a, b, c are called the (line) coordinates of the line defined above, and we denote this line shortly by $[a, b, c]$. Clearly, the lines $[a, b, c]$ and $[\lambda a, \lambda b, \lambda c]$ are identical, where λ is an arbitrary element of $GF(P)$ that differs from 0. Hence $PG(P, 2)$ has $P^2 + P + 1$ lines. If $ax + by + cz = 0$ then we say that the point (x, y, z) lies on the line $[a, b, c]$ or that the line $[a, b, c]$ passes through the point (x, y, z) . It is clear that in this case it is also true that the point (a, b, c) lies on the line $[x, y, z]$ (i.e. the line $[x, y, z]$ passes through the point (a, b, c)). The following assertions can easily be verified:

1. On any line there lie $P + 1$ points.
2. Any two lines have exactly one point in common.
3. Exactly one line passes through any pair of points.

Now define a one-to-one correspondence between the points and lines of $PG(P, 2)$ by assigning to each point (a, b, c) the line $[a, b, c]$ and vice versa. Denote the points by Latin capitals, the lines by lower case Greek letters, and the above correspondence between points and lines by T ; i.e. if the line α is assigned to the point A , then we write either $\alpha = TA$ or $A = T\alpha$. It is easy to see that this correspondence has the following properties:

1'. If the point B belongs to the line $\alpha = TA$, then the point A belongs to the line $\beta = TB$.

2'. If C is the point in common of the lines TA and TB , then TC is the line passing through the points A and B . So, if we denote by $\alpha \cdot \beta$ the point in common of the lines α and β , and by $A \cdot B$ the line passing through the points A and B , then we have

$$TA \cdot TB = T(A \cdot B).$$

3'. Given an arbitrary line α , the lines corresponding to the points of α cover (contain) every point of the geometry; in fact, every point other than $A = T\alpha$ is covered exactly once, while the point $A = T\alpha$ itself is covered $P + 1$ times.

4'. The point $A = (a, b, c)$ lies on the line TA if and only if $a^2 + b^2 + c^2 = 0$.

Let the vertices of the graph $G[P]$ be the points of $PG(P, 2)$. Two distinct points, $A = (a, b, c)$ and $A' = (a', b', c')$, are connected via an edge in $G[P]$ exactly if A' lies on the line TA (i.e. if A lies on the line TA'), i.e. if $aa' + bb' + cc' = 0$. In view of what has been said above, this graph has the following properties:

I. The number of vertices of $G[P]$ is $P^2 + P + 1$.

II. The valency of an arbitrary vertex of $G[P]$ is $P + 1$ or P . (The valency of the vertex $A = (a, b, c)$ is P or $P + 1$ according as A does or does not lie on the line TA , i.e. according as $a^2 + b^2 + c^2 = 0$ or $\neq 0$.) Hence the number of edges in $G[P]$ cannot exceed $\frac{1}{2}(P + 1)(P^2 + P + 1)$.

III. The diameter of $G[P]$ equals 2.

IV. $G[P]$ contains no quadrilateral.

I and II are obvious. III can be established as follows: if A and B are arbitrary distinct vertices then A and B can be joined by the path ACB , where $C = TA \cdot TB$. Hence $G[P]$ has all the properties listed in Lemma 1, completing its proof.

Property IV can be verified as follows. If the quadrilateral $ABCD$ belonged to $G[P]$, then both B and D would be common points of the lines TA and TC , which is impossible in case the points A, B, C , and D are distinct.

Now we prove that Theorem 2 is also asymptotically exact in case $k^2/n \rightarrow +\infty$. Let P be a prime power again. Let n be an arbitrary integer of which $P^2 + P + 1$ is a proper divisor; e.g. let $n = s(P^2 + P + 1)$, where s is an integer ≥ 2 .

We construct a graph G_n^* as follows. Let the vertices of G_n^* be the points of the finite geometry $PG(P, 2)$ (these will be called vertices of the first kind of G_n^*), and the pairs (α, j) where α is an arbitrary line of the geometry $PG(P, 2)$ and j is one of the numbers $1, 2, \dots, s - 1$ (these will be called vertices of the second kind of G_n^*). So the number of vertices in G_n^* is $(P^2 + P + 1) + (s - 1)(P^2 + P + 1) = n$. Connect any two vertices of the first kind if they are

connected in the graph $G[P]$; i.e. if, in the notation used in the proof of Lemma 1, the two vertices of the first kind in question are (a, b, c) and (a', b', c') , then they are connected if and only if $aa' + bb' + cc' = 0$. Furthermore, if (a, b, c) is a vertex of the first kind and (α, j) is one of the second kind of G_n^* , where $\alpha = [x, y, z]$, then these are connected via an edge if and only if the point (a, b, c) lies on the line α in $PG(P, 2)$, i.e. if $ax + by + cz = 0$, irrespective of the value of j .

No vertices of the second kind will be connected with each other in G_n^* . We first prove that the graph G_n^* so defined has diameter 2. In fact, any two vertices of the first kind can be connected via a path of length ≤ 2 , as the subgraph of G_n^* consisting of all vertices of the first kind is isomorphic to the graph $G[P]$ constructed in the proof of Lemma 1, which was seen to have diameter 2. On the other hand, any two vertices of the second kind can be connected via a path of length 2; in fact, if (α, j) and (β, h) are two vertices of the second kind, then one alternative is that $\beta = \alpha$ and $j \neq h$, in which case both vertices are connected with every vertex (a, b, c) (of the first kind) of G_n^* for which the point (a, b, c) lies on the line α in $PG(P, 2)$. Or, if $\alpha \neq \beta$, then (α, j) and (β, h) are connected with that vertex (a, b, c) of the first kind of G_n^* for which the point (a, b, c) is the intersection of the lines α and β in $PG(P, 2)$.

It only remains to prove now that any vertex of the first kind is connected with any vertex of the second kind via a path of length ≤ 2 in G_n^* . Let (a, b, c) be an arbitrary vertex of the first kind, and (α, j) an arbitrary vertex of the second kind of G_n^* . We distinguish two cases. If, in $PG(P, 2)$, the point (a, b, c) lies on the line $\alpha = [a', b', c']$, then the two vertices in question are connected via an edge in G_n^* . If, on the other hand, the point (a, b, c) does not lie on the line $\alpha = [a', b', c']$, then let β denote the line $[a, b, c]$, and let (x, y, z) be the point in common of the lines α and β . Then (x, y, z) lies on the line $\beta = [a, b, c]$, i.e. $ax + by + cz = 0$, and so the vertex (x, y, z) is connected with (a, b, c) in G_n^* ; moreover, (x, y, z) lies also on the line $\alpha = [a', b', c']$, i.e. $a'x + b'y + c'z = 0$, and so the vertex (x, y, z) of the first kind is also connected with the vertex (α, j) of the second kind, and so there leads a path of length 2 from (α, j) to (a, b, c) through (x, y, z) . Thus we have proved that G_n^* has diameter 2. Now compute the maximum of the valencies of the vertices of G_n^* , which is denoted by k , and estimate the number of edges in G_n^* , which is denoted by N . It is clear that a vertex of the first kind can be connected with at most $P + 1$ vertices of the first kind and with $(s - 1)(P + 1)$ vertices of the second kind, and so its valency is at most $s(P + 1)$. A vertex of the second kind is connected exactly with $P + 1$ vertices of the first kind; hence $k = s(P + 1)$. The number of edges connecting vertices of the first kind is equal to the number of edges in $G[P]$, i.e. at most $\frac{1}{2}(P + 1)(P^2 + P + 1)$, while the number of edges connecting vertices of the first kind with vertices of the second kind is $(P^2 + P + 1)(P + 1)(s - 1)$, i.e.

$$N \leq (P^2 + P + 1)(P + 1)(s - 1/2).$$

As $P^2 + P + 1 \geq 7$, we obtain

$$\frac{Nk}{n(n-1)} \leq \frac{(P^2 + P + 1)(P + 1)^2 s(s - 1/2)}{s(P^2 + P + 1) \cdot [s(P^2 + P + 1) - 1]} \leq 1 + \frac{1}{P + 1}.$$

Hence, if $k_j = s_j(P_j + 1)$ and $n_j = s_j(P_j^2 + P_j + 1)$, where P_j is a prime power, then

$$(2.1) \quad \frac{F_2(n_j, k_j)k_j}{n_j(n_j - 1)} \leq 1 + \frac{1}{P_j + 1},$$

i.e. if $P_j \rightarrow +\infty$, then

$$(2.2) \quad \limsup_{j \rightarrow +\infty} \frac{F_2(n_j, k_j)k_j}{n_j(n_j - 1)} \leq 1.$$

Now, taking into account that

$$k_j^2/n_j > s_j,$$

we obtain by Theorem 2 that if $s_j \rightarrow +\infty$ then

$$(2.3) \quad \liminf_{j \rightarrow +\infty} \frac{F_2(n_j, k_j)k_j}{n_j(n_j - 1)} \geq 1;$$

now, from (2.2) and (2.3) we obtain that

$$(2.4) \quad \lim_{j \rightarrow +\infty} \frac{F_2(n_j, k_j)k_j}{n_j(n_j - 1)} = 1 \text{ if } P_j \rightarrow +\infty \text{ and } s_j \rightarrow +\infty.$$

So Theorem 2 is exact if $k^2/n \rightarrow +\infty$; the example constructed above does not, however, exclude the possibility that Theorem 2 can slightly be improved in case k^2/n is not large. The exact value of the function

$$\liminf_{k^2/n \leq c} \frac{F_2(n, k)k}{n(n - 1)} = g(c)$$

is not known ($c > 1$); Theorems 1 and 2 and the construction above only implies that

$$g(c) \geq \max \left(\frac{1}{2}, \frac{1}{1 + 8/c} \right) \text{ if } c > 1.$$

We wish to point out that if in case $s = 2$ we omit the edges connecting vertices of the first kind from G_n^* , then we obtain a graph which was given recently by Ferenc Kárteszi [2] as an example showing that there exists a regular graph of valency $P + 1$ that has $2(P^2 + P + 1)$ vertices and contains no circuit consisting of less than 6 edges (P is a prime power).

§ 3. SOME FURTHER PROBLEMS

So far we have studied $F_2(n, k)$ in the case in which k was relatively small in comparison with n (but, of course, larger than $\sqrt{n - 1}$ in view of (1.1)). Now we are going to study $F_2(n, k)$ under the assumption that k is only a little smaller than n ; more precisely, we are going to study the value of $F_2(n, n - d)$, where d is a fixed integer and $n = d + 2, d + 3, \dots$. It is clear that $F_2(n, k) \geq n - 1$ holds for any value of k , because a graph of diameter 2 is always connected, and a connected graph with n vertices contains at least $n - 1$ edges, and it contains exactly $n - 1$ edges if and only if it is a so-called "tree". Now it is easy to see that $F_2(n, n - 1) = n - 1$, since if there is a vertex of valency $n - 1$ in a graph with n vertices, then the graph already has diameter 2 (it is

“star-shaped”), and we do not need any more edges. It is also easy to see that $F_2(n, n-2) = 2n-4$; the simplest graph of diameter 2 that has n vertices and in which the maximum of the valencies of the vertices is $n-2$ can be obtained e.g. by connecting the vertices P_1 and P_2 with each of the vertices $P_3, P_4, \dots, P_n$.

The first non-trivial case is $d = 3$.

Theorem 3. *If $d \geq 3$ and $n \geq d + 2$ then*

$$(3.1) \quad F_2(n, n-d) \geq F_2(n, n-4) = F_2(n, n-3) = 2n-5.$$

Remark. The surprising fact about Theorem 3 is that

$$(3.2) \quad F_2(n, n-3) < F_2(n, n-2)$$

holds in view (3.1), which shows that $F_2(n, k)$ is not a monotonically decreasing function of k for fixed n , which would seem intuitively plausible.

Proof of Theorem 3. We prove the theorem by induction. The least value of n with which we are concerned is 5; the assertion of the theorem obviously holds for $n = 5$, as a graph of diameter 2 that has 5 vertices and in which the valency of each vertex is at most 2 must necessarily be a circuit with five vertices, and this has $5 = 2 \cdot 5 - 5$ edges. Assume that the theorem is valid for $n-1$ ($n \geq 6$), and let G_n be a graph of diameter 2 that has n vertices and in which the maximum of the valencies of the vertices is $\leq n-3$. We are going to prove that G_n has at least $2n-5$ edges. If the valency of every vertex is at least 4 in this graph, then it has at least $2n$ edges. If there is a vertex of valency 3 but there are no vertices of any smaller valency, then denote one such vertex by P_1 , and let P_2, P_3 , and P_4 be the vertices connected with it. In this case all the vertices $P_5, \dots, P_n$ must be reached from P_1 via a path of length 2, and so each of them is connected with one of the vertices P_2, P_3 and P_4 ; hence the sum of the valencies of these vertices is at least $n-1$; thus the sum of all valencies is $n-1 + 3(n-3) = 4n-10$, and so the number of edges is $\geq 2n-5$. If there is a vertex of valency 1, then the graph cannot have diameter 2 in case the valency of each of its vertices is $\leq n-3$. In fact, if e.g. P_1 is a vertex with valency 1 which is connected only with the vertex P_2 , then at most $n-3$ vertices can be reached from P_1 via a path of length ≤ 2 , as P_2 has valency $\leq n-3$. So we may assume that G_n has at least one vertex of valency 2. (The induction hypothesis will be used only in the discussion of this case.)

Let P_1 be such a vertex, and let P_2 and P_3 be the vertices connected with it. Then the remaining $n-3$ vertices of G_n must be connected either with P_2 or with P_3 . Assume that there is a vertex other than P_1 that is connected with both P_2 and P_3 . In this case, after omitting P_1 from G_n , we obtain a graph with $n-1$ vertices that has diameter 2. In fact, there is no pair of vertices other than P_2, P_3 that is connected with a path of length ≤ 2 leading through P_1 , and, as we have assumed, the vertices P_2 and P_3 are connected also with another path of length 2. We may assume that the maximum of the valencies of the vertices in the graph obtained by omitting P_1 is $\leq n-4 = (n-1)-3$. In fact, this is obvious if there is no vertex with valency $n-3$ in G_n . If there is a vertex with valency $n-3$ in G_n then two cases are possible: either there is a vertex other than P_2 or P_3 with valency $n-3$ or there is not. In the latter

case it is clear that the maximum of the valencies of the vertices in the graph obtained by omitting P_1 is $\leq n - 4$, as the valencies of P_2 and P_3 decrease by 1 in consequence of the omission of P_1 . If, however, there is a vertex other than P_2 and P_3 (and, of course, P_1) with valency $n - 3$, then let this be P_4 . Then the number of edges in the original graph G_n is at least $2 + 2(n - 3) - 1 = 2n - 5$, since each of the vertices $P_4, \dots, P_n$ is connected with either P_2 or P_3 . So there is nothing to prove in this case. Thus we may indeed assume that the maximum of the valencies of the vertices in G_{n-1} is at most $(n - 1) - 3$. Therefore, if Theorem 3 is valid for $n - 1$, then it follows that there are at least $2n - 7$ edges in the graph G_{n-1} obtained by omitting P_1 , and so there are at least $2n - 5$ edges in G_n itself. The only case that has not yet been settled is in which each of the vertices $P_4, \dots, P_n$ is connected either only with P_2 or only with P_3 .

It is, however, not possible that all the vertices $P_4, \dots, P_n$ are connected with the same one from among P_2 and P_3 , as in this case this latter vertex would have valency $n - 2$. So there must be such vertices among $P_4, \dots, P_n$ as are connected with P_2 as well as such as are connected with P_3 . But then we obtain a connected graph after omitting the vertices P_1, P_2 , and P_3 from G_n , since any two vertices of which one is connected with P_2 and the other with P_3 must be connected with a path of length ≤ 2 in G_n that does not pass through the vertices P_1, P_2 and P_3 . If we choose two vertices which are connected e.g. with P_2 then either of these can be joined by a path of length ≤ 2 that avoids the vertices P_1, P_2, P_3 to an arbitrary vertex connected with P_3 , so the two vertices chosen can be joined to each other by a path avoiding the vertices P_1, P_2, P_3 . As a connected graph with $n - 3$ vertices contains at least $n - 4$ edges, G_n itself must contain at least $2 + n - 3 + n - 4 = 2n - 5$ edges. So we have proved that $F_2(n, n - d) \geq 2n - 5$, provided $d \geq 3$ and $n \geq d + 2$. There exists however a graph of diameter 2 that has n vertices and is such that the maximum of the valencies of the vertices is $n - 3$ and the number of edges is $2n - 5$. Such a graph can be constructed as follows. Connect the vertices P_1 and P_2 with the vertices $P_5, \dots, P_n$ and connect P_1 with P_3 , P_2 with P_4 , and P_3 with P_5 , respectively. In case $n = 10$ this graph is shown by Fig. 3.

Thus we have proved that $F_2(n, n - 3) = 2n - 5$.

In order to complete the proof of Theorem 3 it remains to show that $F_2(n, n - 4) = 2n - 5$. This can be seen as follows. If we add further $n - 7$ vertices to the graph of diameter 2 with 7 vertices and 9 edges that is shown in Fig. 2, and we connect these $n - 7$ vertices with those two vertices of valency 3 of the original graph with which a given one of its vertices of valency 2 is connected, then we obtain a graph of diameter 2 that has n vertices and in which the maximum of the valencies of the vertices is $n - 4$ and the number of edges is $9 + 2(n - 7) = 2n - 5$. Such a graph is shown in Fig. 4 for $n = 12$.

We note that the graph shown in Fig. 3 is obtained in the same way from a circuit with n vertices as the graph shown in Fig. 4 is obtained from the one seen in Fig. 2. The general expression for $F_2(n, n - d)$ is not known to us in case $d > 5$. Apart from $F_2(n, n - d)$, it would be desirable to study also the asymptotic behaviour of $F_2(n, [nc])$ ($0 < c < 1$). It seems likely that the limit

$$\lim_{n \rightarrow +\infty} \frac{F_2(n, [nc])}{n} = h(c)$$

exists ($0 < c < 1$), and $h(c)$ is a decreasing function such that $h(1) = 2$ and $h(0) = +\infty$. From Theorem 2 it follows only that

$$\liminf_{n \rightarrow +\infty} \frac{F_2(n, [nc])}{n} \geq \frac{1}{c} \text{ if } 0 < c < 1.$$

As regards the function $F_r(n, k)$ for $r \geq 3$, we only note that similarly to the proof of (1.1) we can see that in order for $F_r(n, k)$ to be defined at all (i.e.

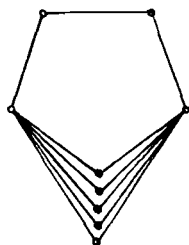


Fig. 3

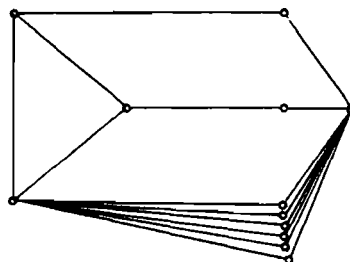


Fig. 4

in order for a graph of diameter r that has n vertices and is such that the maximum of the valencies of the vertices is k to exist) it is necessary that the inequality

$$n \leq 1 + k \frac{(k-1)^r - 1}{k-2}$$

hold; moreover, similarly to the proof of Theorem 1 we can see that

$$F_r(n, k) \geq \frac{\binom{n}{2} (k-2)}{(k-1)^r - 1}.$$

So far we have studied the question which is the least number $N = F_2(n, k)$ for which there is *at least one* that has diameter 2 among the graphs with n vertices and N edges in which the maximum of the valencies of the vertices is k . It is natural to ask the question which is the least integer $N = G_2(n, k)$ for which *every graph* with n vertices and N edges such that the maximum of the valencies of the vertices is k has diameter ≤ 2 . First we consider the case in which n is even. In this case the question is meaningful only if $k \geq n/2$. In fact, if $k \leq n/2 - 1$, then it is easy to construct a graph with n vertices in which the valency of each vertex is k (i.e. which contains the maximal number of edges allowed by the restriction on the valencies) and which has diameter ≥ 3 ; so, in this case $G_2(n, k)$ is indeed not defined.

Such a graph can be constructed as follows. Let $n = 2m$, and let $P_1, \dots, P_m$ and $Q_1, \dots, Q_m$ be the vertices of the graph. According to our assumption $k \leq m - 1$ holds. Connect the vertex P_j ($j = 1, \dots, m$) with the vertices $Q_{j+1}, \dots, Q_{j+k}$, where the indices that exceed m should be understood mod m , i.e. $Q_{m+h} = Q_h$. It is clear that the valency of any P_j ($j = 1, \dots, m$) is k ; and, similarly, the valency of every Q_h ($h = 1, \dots, m$) is also k , as Q_h is connected with the vertices $P_{h-1}, \dots, P_{h-k}$, where the indices are again to be under-

stood mod m , i.e. $P_{-j} = P_{m-j}$. It is clear, however, that the diameter of this graph is not 2, since a path connecting the vertices P_i and Q_j must consist of an odd number of edges, and so, P_1 and Q_1 not being connected via an edge, the graph has diameter ≥ 3 .

Now consider the case in which n is odd, say $n = 2m + 1$. We are going to show that $G_2(n, k)$ may be defined only in case $k \geq m + 1$, provided m is odd, or in case $k \geq m$, provided m is even. In fact, if $k \leq m - 1$, then consider the graph with vertices $P_1, \dots, P_m$ and $Q_1, \dots, Q_{m+1}$ in which the vertex P_j ($j = 1, \dots, m$) is connected with the vertices $Q_{j+1}, \dots, Q_{j+k}$ (the indices exceeding $m + 1$ are to be understood mod $(m + 1)$), and in which the vertices Q_{2l-1}, Q_{2l} are connected precisely if $2l \leq k$. Now, if k is even then the valency of every vertex is k , and if k is odd then the valency of every vertex except Q_k is k . In either case, the graph contains the maximal number of edges subject to the condition that the valency of every vertex is at most k . (In fact, if k and n are odd then there exists no regular graph of valency k with n vertices, as the number of vertices of odd valencies is even in every graph.) The length of the path joining the vertices P_{k+1} and Q_{k+1} , is, however, at least 3 in this graph.

If $n = 2m + 1$ and $k = m$ then we have to distinguish two cases. If m is odd then the above construction gives a graph in which the valency of every vertex except P_k is k and that of P_k is $k - 1$ and the diameter of which is > 2 , as the length of any path joining the vertices P_k and Q_k is at least 3. If, however, m is even and $k = m$ then the above construction gives a (regular) graph of diameter 2.

Summing up the case of even and odd n , we have obtained that $G_2(n, k)$ can be defined only if n is even and $k \geq n/2$, or if $n = 2m + 1$ where m is odd and $k \geq m + 1$, or if $n = 2m + 1$ where m is even and $k \geq m$.

Now we are going to show that $G_2(n, k)$ is indeed defined in the above cases and we shall determine its value.

Theorem 4. *If $n - 2 \geq k \geq m/2$, or if $n = 2m + 1$ where m is even and $k = m$, then*

$$(3.3) \quad G_2(n, k) = \left\{ \frac{(n-2)k + (n-1)}{2} \right\},$$

where $\{x\}$ denotes the least integer $\geq x$.

Proof. Let G_n be a graph with n vertices in which the valencies of the vertices is $\leq k$ and the number N of edges is $\geq \left\{ \frac{(n-2)k + (n-1)}{2} \right\}$. Let $P_1, \dots, P_n$ be the vertices of the graph G_n , and x_j , the valency of the vertex P_j . Then

$$x_1 + \dots + x_n = 2N,$$

and since $x_n \leq k$, for any i and j ($i \neq j$) we have

$$x_i + x_j \geq 2N - (n-2)k \geq 2 \left\{ \frac{(n-2)k + (n-1)}{2} \right\} - (n-2)k.$$

As for any positive integer a we have $2\{a/2\} \geq a$, we obtain

$$2 \left\{ \frac{(n-2)k + (n-1)}{2} \right\} - (n-2)k \geq n-1,$$

and so

$$(3.4) \quad x_i + x_j \geq n - 1.$$

If P_i and P_j are two fixed points of the graph G_n that are not connected with an edge, then (3.4) and the pigeon-hole principle implies that there is a P_h among the remaining $n - 2$ vertices that is connected with both of them, and so G_n has indeed diameter 2. We only have to show yet that if the number N of edges is $< \left\{ \frac{(n-2)k + (n-1)}{2} \right\}$ then the diameter of G_n is not necessarily

2. Assume first that $k < n - 2$.

Take an arbitrary graph G_{n-2} with $n - 2$ vertices in which the maximum of the valencies of the vertices is $k - 1$. If $n - 2$ or $k - 1$ is even, then we can ensure that all the vertices of G_{n-2} have valency $k - 1$; if $n - 2$ and $k - 1$ are odd then we can ensure that G_{n-2} has $n - 3$ vertices of valency $k - 1$ and one of valency $k - 2$. In the former case the number of edges of G_{n-2} is $(n - 2)(k - 1)/2$, and in the latter, $\frac{(n - 3)(k - 1) + (k - 2)}{2}$. The following simple lemma will show that such a graph can always be constructed.

Lemma 2. *Let m and l be arbitrary positive integers such that $1 \leq l \leq m - 1$. If at least one of the numbers m and l is even then there is a graph with m vertices in which the valency of every vertex is l ; and if m and l are both odd then there is a graph with m vertices in which the valency of $m - 1$ vertices is l and that of one vertex is $l - 1$.*

Remark. Lemma 2 is a special case of a general theorem given in [3], which in general gives the necessary and sufficient condition in order that, for an arbitrarily prescribed sequence of valencies, there exist a graph the vertices of which have these valencies in turn. As the proof of the special case needed for our purpose is rather simple, we shall present a direct proof of Lemma 2 after accomplishing the proof of Theorem 4.

Now the desired graph G_n can be constructed as follows: G_n includes the graph G_{n-2} as a subgraph and it contains two further vertices one of which is connected precisely with k vertices of G_{n-2} selected arbitrarily, and the other, with its remaining $n - 2 - k$ vertices. Then the diameter of G_n is clearly at least 3, the maximum of the valencies of its vertices is k , and the number of its edges in the first case is clearly

$$\frac{(n-2)(k-1)}{2} + n - 2 = \frac{(n-2)k + (n-2)}{2},$$

while in the second case

$$\frac{(n-3)(k-1) + (k-2)}{2} + n - 2 = \frac{(n-2)k + (n-3)}{2}$$

i.e. in both cases the number of edges is $\left\{ \frac{(n-2)k + (n-1)}{2} \right\} - 1$. The case $k = n - 2$ is easy to handle; in fact, we have $\left\{ \frac{(n-2)(n-2) + (n-1)}{2} \right\} =$

$= \binom{n-1}{2}$, and if G_n consists of a complete graph with $n-1$ vertices and of an isolated vertex, then it is clearly not connected, and so it has no diameter.

The case $n = 2m + 1$, $k = m$, where m is even can also be easily dealt with. Indeed, in this case we have

$$\left\lfloor \frac{(n-2)k + (n-1)}{2} \right\rfloor = \left\lfloor \frac{nk}{2} \right\rfloor = \frac{nk}{2},$$

and so we only have to show that if m is an even integer then a regular graph of valency m with $2m+1$ vertices has always diameter 2. This is, however, obvious, since if P and P' are two vertices of the graph that are not connected with an edge, then, as both vertices have valency m and the graph has $2m-1$ vertices apart from these two, there must be at least one vertex Q in the graph that is connected with both P and P' via an edge.

The proof of Theorem 4 is complete.

Proof of Lemma 2. If l is even, then let $P_1, \dots, P_m$ be the vertices of the graph to be constructed and connect the vertices P_i and P_j ($i \neq j$) with an edge if and only if there is an integer h such that $j - i \equiv h \pmod{m}$ and $|h| \leq l/2$. The valency of each vertex in this graph is l . If m is even and l is odd then connect the vertices P_i and P_j if there is an integer h such that $j - i \equiv h \pmod{m}$ and $|h| \leq \frac{l-1}{2}$, and, moreover, connect the vertices P_i and $P_{i+m/2}$ ($i = 1, \dots, m/2$). The valency of each vertex in this graph is also l . If m and l are odd then connect the vertices P_i and P_j again if $j - i \equiv h \pmod{m}$ with some h such that $|h| \leq \frac{l-1}{2}$, and connect the vertices P_i and $P_{i+\frac{m-1}{2}}$ for

Table 1

$n \backslash k$	1	2	3	4	5	6	7	8	9
2	1								
3		2							
4		4	3						
5		5	6	4					
6			7	8	5				
7			9	9	10	6			
8			12	11	11	12	7		
9				14	13	13	14	8	
10			15	16	15	15	15	16	9

$i = 1, \dots, \frac{m-1}{2}$. In this graph, the valency of the vertices $P_1, \dots, P_{m-1}$ is l , and that of P_m is $l-1$. So we have constructed a graph with the required properties in all the four cases.

The proof of Lemma 2 is complete.

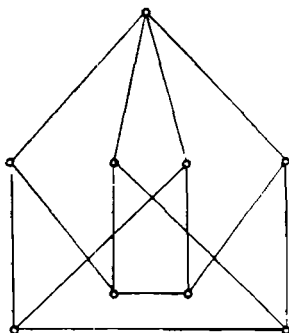


Fig. 5

Table 1 contains the values of $F_2(n, k)$ for all the pairs (n, k) for which it is defined and for which $k < 10$ and $n \leq 10$.

The equality $F_2(9, 4) = 14$ is confirmed by the graph shown in Fig. 5; the values at other places of $F_2(n, k)$ given in the Table can easily be computed with the aid of the theorems established above.

REFERENCES

- [1] Erdős, P. and Rényi, A.: Asymmetric graphs. *Acta Math. Acad. Sci. Hung.*, 14 (1963), 295—315.
- [2] Kárteszi, F.: Egy kombinatorikus minimum problémáról. *Mat. Lapok*, 11 (1960), 323—329.
- [3] Erdős, P. and Gallai, T.: Gráfok előírt fokú pontokkal. *Mat. Lapok*, 11 (1960), 264—274.
- [4] Hoffman, A. J. and Singleton, R. R.: On Moore graphs with diameters 2 and 3. *IBM Journal of Research and Development*, 4 (1960), 497—504.

Über die konvexe Hülle von n zufällig gewählten Punkten

Von

A. RÉNYI und R. SULANKE

Einleitung

Seien P_i ($i = 1, 2, \dots, n$) n nach einer gewissen Verteilung zufällig gewählte Punkte der Ebene, und bezeichne H_n die konvexe Hülle dieser Punkte, die ja bekanntlich ein konvexes Polygon ist. Die Anzahl X_n der Seiten von H_n ist dann eine Zufallsveränderliche, deren Verhalten für $n \rightarrow \infty$ bei verschiedenen Voraussetzungen über die Verteilung der Punkte P_i in dieser Arbeit untersucht werden soll. Dabei wird durchweg angenommen, daß die Punkte P_i unabhängig voneinander sind und dieselbe Verteilung haben. Durch $E_n = E(X_n)$ bezeichnen wir die mathematische Erwartung von X_n .

In § 1 betrachten wir den Fall, daß die P_i ($i = 1, \dots, n$) in einem konvexen Polygon K mit r Ecken gleichverteilt sind. Es wird gezeigt, daß $E_n = (2r/3)(\log n + C) + T + o(1)$ gilt; hierbei bezeichnet C die Eulersche Konstante. Die Größe $T = T(K)$ hängt dabei vom Bereich K ab. In § 2 beweisen wir den elementargeometrischen Satz, daß $T(K)$ für die dem regulären r -Eck affin äquivalenten Polygone und nur für diese maximal wird. In § 3 wird das asymptotische Verhalten von E_n untersucht, wenn die Punkte P_i in einem konvexen Bereich mit glattem Rand gleichverteilt sind. Es zeigt sich, daß E_n die Größenordnung $\sqrt[3]{n}$ hat. In § 4 schließlich beweisen wir, daß sich E_n wie $\sqrt{\log n}$ verhält, wenn die Punkte P_i normal verteilt sind.

§ 1. Zufällige Punkte in einem konvexen Polygon

Sei K ein konvexes Polygon mit den Eckpunkten $A_1, A_2, \dots, A_r$ und den entsprechenden Winkeln $\vartheta_1, \vartheta_2, \dots, \vartheta_r$. Bezeichne a_k die Länge der Seite $A_k A_{k+1}$ ($k = 1, \dots, r$; $A_{r+1} = A_1$). Ferner bezeichne F den Flächeninhalt von K .

Sei $\varepsilon_{ij} = 1$, wenn $i \neq j$ ist und die Strecke $P_i P_j$ zur Begrenzung von H_n gehört, und $\varepsilon_{ij} = 0$ sonst. Dann gilt offenbar

$$X_n = \sum_{1 \leq i < j \leq n} \varepsilon_{ij}. \quad (1)$$

Die Wahrscheinlichkeit

$$W_n = P(\varepsilon_{ij} = 1) \quad (2)$$

ist für alle Zahlenpaare (i, j) mit $1 \leq i < j \leq n$ dieselbe, und es gilt

$$E_n = E(X_n) = \binom{n}{2} W_n. \quad (3)$$

Um das asymptotische Verhalten von E_n zu bestimmen genügt es also, die Wahrscheinlichkeit W_n zu berechnen. Es ist nun W_n die Wahrscheinlichkeit dafür, daß

alle Punkte P_h ($h = 3, 4, \dots, n$) auf derselben Seite der Geraden durch P_1 und P_2 liegen. Bezeichnen wir durch $F_1 \leq F/2$ und $F - F_1$ die Flächeninhalte der Teile von K , in die K durch die Gerade $P_1 P_2$ zerlegt wird, so gilt

$$W_n = \frac{1}{F^2} \int_K \int_K \left[\left(1 - \frac{F_1}{F}\right)^{n-2} + \left(\frac{F_1}{F}\right)^{n-2} \right] dP_1 dP_2. \quad (4)$$

Offenbar ist wegen $F_1/F \leq 1/2$

$$\frac{1}{F^2} \int_K \int_K \left(\frac{F_1}{F}\right)^{n-2} dP_1 dP_2 \leq \frac{1}{2^{n-2}},$$

und somit*

$$E_n \sim \frac{\binom{n}{2}}{F^2} \int_K \int_K \left(1 - \frac{F_1}{F}\right)^{n-2} dP_1 dP_2. \quad (5)$$

Bezeichne nun f_i den Flächeninhalt des Dreiecks $A_{i-1} A_i A_{i+1}$ ($A_{r+j} = A_j$), und sei $f = \min_{1 \leq i \leq r} f_i$. Offenbar können wir uns bei der Untersuchung des asymptotischen Verhaltens von E_n auf solche Punktepaare P_1, P_2 beschränken, für die die Gerade $P_1 P_2$ entweder zwei benachbarte Seiten oder aber zwei durch eine andere Seite von K getrennte Seiten von K trifft. Für alle anderen Geraden gilt nämlich $1 - F_1/F \leq 1 - f/F$. Daher können wir den entsprechenden Anteil des Integrals auf der rechten Seite von (5) vernachlässigen, und es gilt

$$E_n \sim \frac{\binom{n}{2}}{F^2} \left(\sum_{i=1}^r (I_i + J_i) \right), \quad (6)$$

wobei

$$I_i = \int_{C_i} \left(1 - \frac{F_1}{F}\right)^{n-2} dP_1 dP_2 \quad (7)$$

und

$$J_i = \int_{D_i} \left(1 - \frac{F_1}{F}\right)^{n-2} dP_1 dP_2. \quad (8)$$

Hier bedeutet C_i die Menge der Punktepaare P_1, P_2 , für die die Gerade $P_1 P_2$ die Seiten $A_{i-1} A_i$ und $A_i A_{i+1}$ von K trifft, und D_i die Menge der Punktepaare, für die die Gerade $P_1 P_2$ die Seiten $A_{i-1} A_i$ und $A_{i+1} A_{i+2}$ von K trifft.

Wir untersuchen zuerst das Integral I_i . Bezeichne G_{ab} die Menge der Punktepaare P_1, P_2 , für die $|A_i Q_1| < a$ und $|A_i Q_2| < b$ gilt; hierbei bezeichnet Q_1 den Schnittpunkt der Geraden $P_1 P_2$ mit der Seite $A_{i-1} A_i$ und Q_2 ihren Schnittpunkt mit der Seite $A_i A_{i+1}$, ferner bedeutet $|AB|$ die Länge der Strecke AB . Durch eine elementare Rechnung ergibt sich

$$\int_{G_{ab}} dP_1 dP_2 = \frac{a^2 b^2 \sin^2 \vartheta_i}{12}. \quad (9)$$

Der Flächeninhalt des von der Geraden $P_1 P_2$ abgeschnittenen Dreiecks $Q_1 A_i Q_2$

* $\sim$ bezeichnet „asymptotisch gleich“, d. h. $A_n \sim B_n$ bedeutet, daß $\lim_{n \rightarrow +\infty} \frac{A_n}{B_n} = 1$ ist.

ist gleich $1/2 ab \sin \vartheta_i$. Somit erhalten wir

$$I_i = \int_0^{a_{i-1}} \int_0^{a_i} \left(1 - \frac{ab \sin \vartheta_i}{2F}\right)^{n-2} \sin^2 \vartheta_i \frac{ab}{3} da db, \quad (10)$$

wo a_i die Länge der Seite $A_i A_{i+1}$ bedeutet.

Durch die Transformation

$$X = a \sqrt{\frac{\sin \vartheta_i}{2F}}, \quad Y = b \sqrt{\frac{\sin \vartheta_i}{2F}} \quad (11)$$

ergibt sich

$$I_i = \frac{4F^2}{3} \int_0^{X_i} \int_0^{Y_i} (1 - XY)^{n-2} XY dX dY, \quad (12)$$

wobei

$$X_i = a_{i-1} \sqrt{\frac{\sin \vartheta_i}{2F}}, \quad Y_i = a_i \sqrt{\frac{\sin \vartheta_i}{2F}},$$

also

$$\varrho_i = X_i Y_i = \frac{a_{i-1} a_i \sin \vartheta_i}{2F} = \frac{f_i}{F} < 1 \quad (13)$$

gilt. Nun ist

$$\int_0^{X_i} \int_0^{Y_i} (1 - XY)^{n-2} XY dX dY = \int_0^{X_i} \int_0^{Y_i} (1 - XY)^{n-2} dX dY - \int_0^{X_i} \int_0^{Y_i} (1 - XY)^{n-1} dX dY.$$

Weiter gilt

$$\begin{aligned} \int_0^{X_i} \int_0^{Y_i} (1 - XY)^{n-1} dX dY &= \int_0^{X_i} \frac{1 - (1 - XY_i)^n}{nX} dX = \\ &= \frac{1 + \frac{1}{2} + \dots + \frac{1}{n} - \sum_{k=1}^n \frac{(1 - \varrho_i)^k}{k}}{n}. \end{aligned}$$

Somit erhalten wir

$$I_i = \frac{4F^2}{3} \left\{ \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \frac{\sum_{k=1}^{n-1} \frac{(1 - \varrho_i)^k}{k}}{n(n-1)} + \frac{(1 - \varrho_i)^n}{n^2} \right\}. \quad (14)$$

Setzen wir

$$S_i = \sum_{k=1}^{\infty} \frac{(1 - \varrho_i)^k}{k} = \log \frac{1}{\varrho_i}, \quad (15)$$

so ergibt sich schließlich

$$E_n = \frac{2}{3} (C - 1 + \log n) r - \frac{2}{3} \sum_{i=1}^r S_i + o(1) + \frac{\binom{n}{2}}{F^2} \sum_{i=1}^r J_i, \quad (16)$$

wobei C die Eulersche Konstante bedeutet.

Nun berechnen wir das Integral J_i . Wir verlängern die Seiten $A_{i-1}A_i$ und $A_{i+1}A_{i+2}$ bis zu ihrem Schnittpunkt A_i^* ; der Fall, daß diese Seiten parallel sind, läßt sich ähnlich behandeln. Sei wieder Q_1 der Schnittpunkt der Geraden P_1P_2 mit der Seite $A_{i-1}A_i$ und Q_2 der Schnittpunkt mit der Seite $A_{i+1}A_{i+2}$ und sei $a' = |A_i A_i^*|$, $b' = |A_{i+1} A_i^*|$, $a = |A_i Q_1|$, $b = |A_{i+1} Q_2|$; G_{ab} sei wie oben definiert. Wir erhalten aus (9)

$$\int_{G_{ab}} dP_1 dP_2 = \frac{\sin^2 \gamma_i}{12} (a^2 + 2aa')(b^2 + 2bb'), \quad (17)$$

wobei γ_i den Winkel bei A_i^* bedeutet. Somit ist

$$J_i = \int_{D_i} \left(1 - \frac{(ab + a'b + ab') \sin \gamma_i}{2F} \right)^{n-2} \frac{\sin^2 \gamma_i}{3} (a + a')(b + b') da db \quad (18)$$

und dieses Integral ist asymptotisch gleich

$$J_i \sim \int_{D_i} \left(1 - \frac{(a'b + ab') \sin \gamma_i}{2F} \right)^{n-2} \frac{\sin^2 \gamma_i}{3} a' b' da db. \quad (19)$$

Führen wir die Transformation

$$a = \frac{F}{b' \sin \gamma_i} X, \quad b = \frac{F}{a' \sin \gamma_i} Y$$

aus, so folgt

$$\begin{aligned} J_i &\sim \frac{F^2}{3} \int_0^{a'_{i-1}} \int_0^{a'_{i+1}} \left(1 - \frac{X+Y}{2} \right)^{n-2} dX dY = \\ &= \frac{4F^2}{3n(n-1)} \left\{ 1 - \left(1 - \frac{a'_{i-1}}{2} \right)^n - \left(1 - \frac{a'_{i+1}}{2} \right)^n + \left(1 - \frac{a'_{i-1} + a'_{i+1}}{2} \right)^n \right\}, \end{aligned}$$

wobei

$$a'_{i-1} = \frac{a_i b' \sin \gamma_i}{F}, \quad a'_{i+1} = \frac{a_{i+2} a' \sin \gamma_i}{F}$$

gesetzt ist. Somit ergibt sich

$$E_n = \frac{2r}{3} (\log n + C) - \frac{2}{3} \sum_{i=1}^r S_i + o(1).$$

Fassen wir das Bewiesene in dem folgenden Satz zusammen:

Satz 1. Sei K ein konvexes Polygon mit r Seiten. Die mathematische Erwartung E_n der Anzahl der Seiten der konvexen Hülle H_n von n in K zufällig gewählten Punkten ist gleich

$$E_n = \frac{2r}{3} (\log n + C) + \frac{2}{3} \log \frac{\prod_{i=1}^r f_i}{Fr} + o(1). \quad (20)$$

Hierbei bedeutet F den Flächeninhalt von K und f_i den Flächeninhalt des von den Ecken A_{i-1}, A_i, A_{i+1} von K gebildeten Dreiecks.

Ist z.B. K ein Dreieck, so gilt $f_1 = f_2 = f_3 = F$ und es folgt

$$E_n = 2(\log n + C) + o(1). \quad (21)$$

Die Formel für E_n hängt also nicht von der Form des Dreiecks ab. Das ist verständlich; denn E_n muß offenbar gegenüber affinen Transformationen invariant sein. In § 2 werden wir zeigen, daß die in (20) auftretende, von der Gestalt von K abhängende Konstante

$$Z(K) = \frac{\prod_{i=1}^r f_i}{Fr} \quad (22)$$

für ein reguläres r -Eck (und die zu ihm affin äquivalenten Polygone) maximal wird.

§ 2. Ein Extremalproblem für konvexe Polygone

Bevor wir zu weiteren asymptotischen Abschätzungen für E_n unter anderen Voraussetzungen über die Verteilung der Punkte P_i übergehen, beweisen wir den folgenden

Satz 2. *Sei K ein konvexes Polygon mit r Seiten. Dann gilt mit den Bezeichnungen des vorigen §: Die Funktion*

$$Z(K) = \frac{1}{F^r} \prod_{i=1}^r f_i \quad (23)$$

ist maximal genau dann, wenn K durch eine affine Transformation in das reguläre r -Eck übergeführt werden kann.

Sei $a_i = \overline{A_{i-1}A_i}$, wobei $A_{r+i} = A_i$ gesetzt werde. Dann gilt

$$f_i = \frac{1}{2} [a_i, a_{i+1}], \quad F = \frac{1}{2} \sum_{i=1}^{r-2} [a_1 + a_2 + \dots + a_i, a_{i+1}], \quad (24)$$

wobei $[a, b]$ die Determinante der Vektoren a, b bedeutet. Die Funktion $Z(K)$ ist nun eine Funktion der r Vektoren a_i ($i = 1, \dots, r$), die der Schließungsbedingung

$$\sum_{i=1}^r a_i = 0 \quad (25)$$

genügen. Wir denken uns jetzt die Eckpunkte A_i von K genügend kleinen Verschiebungen unterworfen, die stetig differenzierbar von einem Parameter t abhängen mögen. Da das Ausgangspolygon K , das dem Parameterwert $t = 0$ entsprechen möge, ein konvexes r -Eck ist, sind dann auch die durch genügend kleine Variation von t entstehenden Polygone konvexe r -Ecke. Die Funktion Z muß, betrachtet als Funktion von t , an der Stelle $t = 0$ ein Maximum haben, wenn K ein maximales Polygon ist. Als notwendige Bedingung dafür, daß K maximal ist, erhalten wir durch eine elementare Rechnung:

$$\begin{aligned} \sum_{i=1}^r \frac{F}{f_i} ([\dot{a}_i, a_{i+1}] + [a_i, \dot{a}_{i+1}]) - \\ - r \sum_{i=1}^{r-2} ([\dot{a}_1 + \dots + \dot{a}_i, a_{i+1}] + [a_1 + \dots + a_i, \dot{a}_{i+1}]) = 0. \end{aligned} \quad (26)$$

Hierbei wurde

$$\dot{a}_i = \left. \frac{d}{dt} a_i \right|_{t=0}$$

gesetzt. Die $\dot{a}_i$ sind beliebige Vektoren, die nur der aus (25) folgenden Schließungsbedingung

$$\sum_{i=1}^r \dot{a}_i = 0 \quad (27)$$

zu genügen haben. Setzen wir nun nacheinander

$$\dot{a}_j = b, \quad \dot{a}_{j+1} = -b, \quad \dot{a}_i = 0 \quad \text{für } i \neq j, j+1, \quad (28)$$

wobei b ein zunächst noch willkürlicher Vektor ist, so ist die Schließungsbedingung

offenbar erfüllt und wir erhalten für $j = 1, \dots, r$

$$\frac{F}{r} \left\{ \frac{[a_{j-1}, b]}{f_{j-1}} - \frac{[b, a_{j+2}]}{f_{j+1}} + \frac{1}{f_j} [b, a_j + a_{j+1}] \right\} = [b, a_j + a_{j+1}]. \quad (29)$$

Wählen wir nun speziell $b = a_j$, so folgt

$$\frac{F}{r} \left\{ 4 - \frac{[a_j, a_{j+2}]}{f_{j+1}} \right\} = 2f_j \quad (30)$$

und für $b = -a_{j+1}$ ergibt sich

$$\frac{F}{r} \left\{ 4 - \frac{[a_{j-1}, a_{j+1}]}{f_{j-1}} \right\} = 2f_j. \quad (31)$$

Der Vergleich dieser Formeln liefert

$$[a_j, a_{j+2}] = \frac{f_{j+1}}{f_{j-1}} [a_{j-1}, a_{j+1}]. \quad (32)$$

Wir schreiben jetzt (31) in der Gestalt

$$2 \left(2 - \frac{rf_j}{F} \right) = \frac{[a_{j-1}, a_{j+1}]}{f_{j-1}}$$

und erhalten durch wiederholte Anwendung von (32)

$$2 \left(2 - \frac{rf_j}{F} \right) = \frac{f_j}{f_1 \cdot f_2} [a_1, a_3]$$

oder

$$f_j = \frac{2}{\frac{r}{F} + \frac{[a_1, a_3]}{2f_1 \cdot f_2}}. \quad (33)$$

Für $r = 3$ ist unsere Extremalaufgabe trivial. Im Falle $r \geq 4$ ergibt sich zunächst $f_3 = f_4 = \dots = f_r$. Durch eine zyklische Vertauschung der Numerierung der Eckpunkte von K folgt unmittelbar

$$f_1 = f_2 = \dots = f_r \quad (34)$$

und nach (32) erhalten wir außerdem

$$[a_i, a_{i+2}] = [a_1, a_3] = b \quad (i = 1, 2, \dots, r), \quad (35)$$

wobei b eine gewisse Konstante ist.

Bemerkung. Im Fall $b = [a_i, a_{i+2}] = 0$ ist $f_j = 2F/r$. Also ist stets a_{i+2} parallel zu a_i . Das ist nur möglich, wenn $r = 4$ und K ein Parallelogramm ist.

Wir kehren nun zum allgemeinen Fall zurück. Durch eine affine Transformation können wir stets erreichen, daß $f_j = 1/2$, d. h.

$$[a_i, a_{i+1}] = 1 \quad (36)$$

gilt. Aus (33) folgt dann sofort

$$F = \frac{r}{2(2-b)} \quad \text{und daher} \quad b < 2. \quad (37)$$

Da die Vektoren a_{i-2} und a_{i-1} linear unabhängig sind, folgt aus dem Ansatz $a_i = \alpha a_{i-2} + \beta a_{i-1}$ unter Beachtung von (35) und (36) die Rekursion

$$a_i = -a_{i-2} + b a_{i-1}. \quad (38)$$

Wir haben also gezeigt, daß die Seitenvektoren a_i eines maximalen konvexen r -Ecks notwendig eine Rekursion der Gestalt (38) erfüllen müssen. Der Beweis wird jetzt zu Ende geführt, indem wir zeigen, daß sich in diesem Fall eine euklidische Metrik in der affinen Ebene definieren läßt, bezüglich der das Polygon K gerade als reguläres r -Eck erscheint.

Zunächst bemerken wir, daß stets

$$-1 \leq b < 2 \quad (39)$$

gelten muß. Wäre nämlich $b < -1$, so würde die Seite a_3 die Seite a_1 durchdringen, was der Konvexität von K widerspricht. Die obere Abschätzung $b < 2$ ist schon bewiesen ((37)).

Die euklidische Metrik ist eindeutig bestimmt, wenn wir die Skalarprodukte der Vektoren a_1, a_2 festlegen, die wir als Basisvektoren betrachten. Diese Skalarprodukte definieren wir durch

$$a_1^2 = a_2^2 = \frac{2}{\sqrt{4-b^2}}, \quad a_1 a_2 = \frac{b}{\sqrt{4-b^2}}. \quad (40)$$

Offenbar gilt

$$[a_1, a_2]^2 = \begin{vmatrix} a_1^2 & a_1 a_2 \\ a_1 a_2 & a_2^2 \end{vmatrix} = 1.$$

Daher ist die so definierte Metrik positiv definit, d. h. euklidisch. Durch vollständige Induktion beweist man nun leicht unter Benutzung der Rekursion (38), daß für alle j

$$a_j^2 = \frac{2}{\sqrt{4-b^2}}, \quad a_j a_{j+1} = \frac{b}{\sqrt{4-b^2}}, \quad [a_j, a_{j+1}] = 1$$

gelten muß. Hieraus folgt, daß alle Seiten unseres r -Ecks K dieselbe Länge haben und daß sich zwei aufeinander folgende Seiten unter demselben Winkel schneiden. Also muß das r -Eck bezüglich dieser Metrik regulär sein.

Hiermit ist die Eindeutigkeit des maximalen Polygons bewiesen. Die Existenz ergibt sich durch eine einfache Folgerung aus der Beschränktheit von $Z(K)$ sowie der Stetigkeit von F und Z . Also ist Satz 2 vollständig bewiesen.

§ 3. Zufällige Punkte in einem konvexen Bereich mit glattem Rand

Sei jetzt K ein konvexer Bereich, dessen Rand eine Krümmung besitzt, die als Funktion der Bogenlänge stetig ist. Mit den Bezeichnungen der vorigen Paragraphen haben wir wieder

$$E_n = \binom{n}{2} W_n.$$

Nach einem bekannten Satz der Integralgeometrie (vgl. BLASCKE [1], S. 17, (86)) kann die Dichte für Punktpaare folgendermaßen umgeformt werden:

$$dP_1 dP_2 = |t_1 - t_2| dt_1 dt_2 d\varphi dp, \quad (41)$$

wobei p den Abstand der Geraden $P_1 P_2$ vom Koordinatenursprung, φ den Winkel dieser Geraden mit einer Nullrichtung und t_1, t_2 die Parameterwerte der Bogen-

länge der Punkte P_1, P_2 auf der Geraden $P_1 P_2$ bedeutet. Bezeichne f den Flächeninhalt des durch die Gerade $P_1 P_2$ von K abgeschnittenen Teils. Dann gilt

$$E_n = \frac{\binom{n}{2}}{F^2} \int_0^{2\pi} \left\{ \int_0^{p(\varphi)} \left(1 - \frac{f}{F}\right)^{n-2} (\iint |t_1 - t_2| dt_1 dt_2) dp \right\} d\varphi. \quad (42)$$

Durch $l(p, \varphi)$ bezeichnen wir die Länge der Sehne, in der die Gerade mit den Koordinaten p, φ den Bereich K trifft. Es gilt

$$\iint |t_1 - t_2| dt_1 dt_2 = \frac{l^3(p, \varphi)}{3}. \quad (43)$$

Somit erhalten wir

$$E_n = \frac{\binom{n}{2}}{3F^2} \int_0^{2\pi} \left\{ \int_0^{p(\varphi)} \left(1 - \frac{f}{F}\right)^{n-2} l^3(p, \varphi) dp \right\} d\varphi. \quad (44)$$

Bei der Berechnung des asymptotischen Wertes von E_n kann man sich offenbar auf solche Wertepaare p, φ beschränken, für die $f/F < \varepsilon$ gilt; denn die anderen Wertepaare geben nur ein Restglied der Ordnung $n^2(1 - \varepsilon)^n = o(1)$. Wir betrachten nun einen festen Wert von φ . Es sei $P(\varphi)$ der Punkt, in dem die Tangente von K die Richtung φ hat. Bei der Berechnung von E_n kann man f und l durch die entsprechenden Größen $\bar{f}$ und $\bar{l}$ des Schmieglekreises im Punkte $P(\varphi)$ ersetzen, wie aus den folgenden Abschätzungen hervorgeht. Sei α der zur Sehne $\bar{l}$ gehörende Zentriwinkel und $r(\varphi)$ der Radius des Schmieglekreises im Punkte $P(\varphi)$. Dann gilt

$$\bar{l} = 2r(\varphi) \sin \alpha/2 \quad \text{und} \quad \bar{f} = \frac{1}{2}(\alpha - \sin \alpha)r^2(\varphi), \quad (45)$$

ferner

$$|dp| = \frac{1}{2}r(\varphi) \sin \alpha/2 |d\alpha|. \quad (46)$$

Schließlich ist

$$l - \bar{l} = o(\alpha^2) \quad \text{und} \quad f - \bar{f} = o(\alpha^4). \quad (47)$$

Somit ergibt sich

$$E_n = \frac{\binom{n}{2}}{12F^2} \int_0^{2\pi} r^4 \int_0^{\alpha(\varphi)} \left(1 - \frac{\alpha^3 r^2}{12F^2} + o(\alpha^3)\right)^{n-2} (\alpha^4 + o(\alpha^5)) d\alpha d\varphi. \quad (48)$$

Durch die Substitution

$$\frac{\alpha^3 r^2}{12F} = \frac{X}{n} \quad (49)$$

erhalten wir

$$S(\varphi) = \int_0^{\alpha(\varphi)} \left(1 - \frac{\alpha^3 r^2}{12F} + o(\alpha^3)\right)^{n-2} (\alpha^4 + o(\alpha^5)) d\alpha, \quad (50)$$

$$S(\varphi) = \frac{1}{3} \left(\frac{12F}{r^2 n}\right)^{5/3} \left(\int_0^\infty \left(1 - \frac{X}{n}\right)^{n-2} x^{2/3} dx + o(1)\right) = \frac{\Gamma\left(\frac{5}{3}\right)}{3} \left(\frac{12F}{r^2 n}\right)^{5/3} (1 + o(1)).$$

Somit gilt

$$E_n \sim \Gamma\left(\frac{5}{3}\right) \sqrt[3]{\frac{2n}{3F}} \int_0^{2\pi} r^{2/3} d\varphi. \quad (51)$$

Bezeichnet nun s die Bogenlänge auf dem Rand von K , so erhalten wir unter

Beachtung von $d\varphi/ds = 1/r$ den folgenden Satz:

Satz 3. *Ist K ein konvexer Bereich, dessen Randkurve L die stetige Krümmung $\kappa = \kappa(s)$ besitzt, so gilt*

$$E_n \sim \Gamma\left(\frac{5}{3}\right) \sqrt[3]{\frac{2}{3}} (F^{-1/3} \int_L \kappa^{1/3} ds) \sqrt[3]{n}. \quad (52)$$

Das in (52) auftretende Integral $\int_L \kappa^{1/3} ds$ ist gerade die äquiaffine Länge der Kurve L . Man erkennt leicht, daß der Faktor von $\sqrt[3]{n}$ sogar affin invariant ist. Aus der affinen isoperimetrischen Eigenschaft der Ellipsen (BLASCHKE-REIDE-MEISTER) folgt unmittelbar, daß dieser Faktor für die Ellipsen und nur für die Ellipsen maximal ist.

§ 4. Normal verteilte zufällige Punkte

In diesem Paragraphen beweisen wir den folgenden Satz:

Satz 4. *Die Punkte P_i ($i = 1, 2, \dots, n$) seien unabhängig voneinander und nach derselben Normalverteilung in der Ebene gewählt. Dann gilt*

$$E_n \sim 2 \sqrt{2\pi \log n}. \quad (53)$$

Beweis. Da E_n offenbar gegenüber affinen Transformationen der Ebene invariant ist, können wir annehmen, daß die Dichtefunktion unserer Normalverteilung die Gestalt $\frac{1}{2\pi} e^{-\frac{x^2+y^2}{2}}$ hat. Wie schon in den vorigen Paragraphen gilt

$$E_n = \binom{n}{2} W_n,$$

wobei W_n die Wahrscheinlichkeit dafür ist, daß alle Punkte $P_3, \dots, P_n$ auf derselben Seite der Geraden $P_1 P_2$ liegen. Wegen der integralgeometrischen Formel

$$dP_1 dP_2 = dp d\varphi |t_1 - t_2| dt_1 dt_2$$

und wegen der Kreissymmetrie der Normalverteilung erhalten wir

$$W_n = \frac{1}{2\pi} \iint (g(p)^{n-2} + (1 - g(p))^{n-2}) |t_1 - t_2| e^{-p^2 - \frac{t_1^2 + t_2^2}{2}} dt_1 dt_2 dp, \quad (54)$$

wobei

$$g(p) = \int_{-\infty}^{+\infty} \int_P^{+\infty} e^{-\frac{x^2+y^2}{2}} dx dy = 1 - \Phi(p) \quad (55)$$

gesetzt wurde und

$$\Phi(p) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^p e^{-\frac{u^2}{2}} du \quad (56)$$

gilt.

Durch die Transformation

$$u = \frac{t_1 - t_2}{\sqrt{2}}, \quad v = \frac{t_1 + t_2}{\sqrt{2}}, \quad \frac{\partial(t_1, t_2)}{\partial(u, v)} = 1 \quad (57)$$

erhalten wir

$$\frac{1}{2\pi} \iint |t_1 - t_2| e^{-\frac{t_1^2 + t_2^2}{2}} dt_1 dt_2 = \frac{2}{\sqrt{\pi}}. \quad (58)$$

Also gilt

$$W_n = \frac{2}{\sqrt{\pi}} \int_0^\infty [\Phi^{n-2}(p) + (1 - \Phi(p))^{n-2}] e^{-p^2} dp \quad (59)$$

und da offenbar $1 - \Phi(p) \leq 1/2$ für $p \geq 0$ ist, folgt

$$W_n \sim \frac{2}{\sqrt{\pi}} \int_0^\infty \Phi^{n-2}(p) e^{-p^2} dp. \quad (60)$$

Nun ist für $p > 1$

$$\Phi(p) = 1 - \frac{e^{-\frac{p^2}{2}}}{\sqrt{2\pi} p \left(1 + \frac{\theta p}{p^2}\right)} \quad (61)$$

wobei $0 < \theta_p < 1$ gilt (A. RÉNYI, [3], S. 136, Aufgabe 18). Durch die Substitution

$$p = \sqrt{2 \log n - \log(2 \log n)} + \frac{u - \log \sqrt{2\pi}}{\sqrt{2 \log n}} \quad (62)$$

erhält man schließlich nach einigem Rechnen

$$W_n \sim \frac{4 \sqrt{2\pi \log n}}{n^2}.$$

Also ist

$$E_n \sim 2 \sqrt{2\pi \log n},$$

was zu beweisen war.

Literatur

- [1] BLASCHKE, W.: Integralgeometrie. 3. Aufl. Berlin: VEB Deutscher Verlag der Wissenschaften 1955, 1–130.
- [2] —, und K. REIDEMEISTER: Differentialgeometrie II, Berlin: Springer 1923, 60.
- [3] RÉNYI, A.: Wahrscheinlichkeitsrechnung, mit einem Anhang über Informationstheorie. Berlin: VEB Deutscher Verlag der Wissenschaften 1962, 1–547.

ON STABLE SEQUENCES OF EVENTS

By ALFRED RÉNYI

Mathematical Institute, Hungarian Academy of Sciences

SUMMARY. A sequence $\{A_n\}$ of events is called a *stable sequence* if for every event B the limit $\lim_{n \rightarrow +\infty} P(A_n B) = Q(B)$ exists. It is shown that in this case Q is a bounded measure which is absolutely continuous with respect to the underlying probability measure P . The Radon-Nikodym derivative $\frac{dQ}{dP} = \alpha$ is called the *local density* of the stable sequence $\{A_n\}$. Criteria for a sequence of events being stable are given, further examples of stable sequences are discussed. The notion of a stable sequence of events generalizes the notion of a mixing sequence of events, introduced in a previous paper of the author. A stable sequence is mixing if its local density is constant almost everywhere.

1. INTRODUCTION

Let $[\Omega, \mathcal{A}, P]$ be a probability space in the sense of Kolmogoroff, i.e. let Ω be an arbitrary set whose elements shall be denoted by ω and called elementary events, $\mathcal{A}$ a σ -algebra of subsets of Ω whose elements will be denoted by capital letters A, B etc., and called random events or simply events and $P = P(A)$ a measure, i.e. a non-negative and σ -additive set function defined on $\mathcal{A}$ and normed by the condition $P(\Omega) = 1$; $P(A)$ will be called the probability of the event $A \in \mathcal{A}$.

We shall denote by ϕ the empty set which represents the impossible event, further by $A+B$ the union and by $A.B$ the intersection of the sets A and B . If $A_n (n = 1, 2, \dots)$ is a sequence of sets, we shall use also the notation $\sum_n A_n$ for the union of the sets A_n . We denote by $A-B$ the set of elements which belong to A but not to B and put $\Omega-A = \bar{A}$. If A and B are arbitrary events such that $P(B) > 0$, we shall denote by $P(A|B)$ the conditional probability of the event A with respect to the condition B , i.e. we put

$$P(A|B) = \frac{P(AB)}{P(B)}.$$

We shall denote by $a \in A$ that a is an element of the set A and by $A \subset B$ that the set A is a subset of the set B .

As usual a real function $\xi = \xi(\omega)$ defined on Ω is called a random variable if it is measurable with respect to $\mathcal{A}$, that is, if denoting by $\xi^{-1}(I)$ the set of those $\omega \in \Omega$ for which $\xi(\omega) \in I$, then $\xi^{-1}(I)$ belongs to $\mathcal{A}$ if I is an arbitrary interval of the real line.

We denote by $E(\xi)$ the mean value (expectation) of the random variable ξ , i.e. we put $E(\xi) = \int_{\Omega} \xi dP$.

The infinite sequence of events $A_1, A_2, \dots, A_n, \dots$, i.e. of subsets of Ω belonging to $\mathcal{A}$ will be called a *stable sequence*, if the limit

$$\lim_{n \rightarrow +\infty} P(A_n B) = Q(B) \quad (1.1)$$

exists for every $B \in \mathcal{A}$. We shall show that in this case $Q(B)$ is a bounded measure on $\mathcal{A}$, which is absolutely continuous with respect to the measure P , and thus

$$Q(B) = \int_B \alpha dP \quad (1.2)$$

for every $B \in \mathcal{A}$ where $\alpha = \alpha(\omega)$ is a measurable function on Ω such that $0 \leq \alpha(\omega) \leq 1$. We shall call $\alpha(\omega)$ the *local density* of the stable sequence of events $\{A_n\}$.

As well known $\alpha(\omega)$ is not uniquely determined, but if (1.2) holds both with $\alpha = \alpha_1(\omega)$ and $\alpha = \alpha_2(\omega)$ then $\alpha_1(\omega)$ and $\alpha_2(\omega)$ are almost everywhere equal to another.

In the special case when the local density is constant, i.e. $\alpha(\omega) \equiv \alpha$, then $Q(B) = \alpha P(B)$ for every $B \in \mathcal{A}$, i.e. in this case

$$\lim_{n \rightarrow +\infty} P(A_n B) = \alpha P(B). \quad (1.3)$$

Sequences $\{A_n\}$ for which (1.3) holds have been considered already in a previous paper (Rényi, 1958) and have been called strongly *mixing* sequences of events with density α . Thus the notion of a stable sequence of events is a generalization of the notion of a mixing sequence.

The definition of a stable sequence of events can be formulated also in the following equivalent form: The sequence of events $\{A_n\}$ ($n = 1, 2, \dots$) is called stable if for every event $B \in \mathcal{A}$ such that $P(B) > 0$ the conditional probability $P(A_n | B)$ tends to a limit, i.e.

$$\lim_{n \rightarrow +\infty} P(A_n | B) = q(B) \quad (1.4)$$

exists. Clearly, if $P(B) > 0$ then (1.1) and (1.4) with $q(B) = \frac{Q(B)}{P(B)}$ are equivalent, while if $P(B) = 0$ then (1.1) holds with $Q(B) = 0$ for any sequence $\{A_n\}$.

We shall show that stable sequences of events can be simply characterized in terms of Hilbert space theory. Let H denote the Hilbert space of all random variables ξ , defined on the probability space $[\Omega, \mathcal{A}, P]$, for which $E(\xi^2)$ is finite, the inner product (ξ, η) being defined by $(\xi, \eta) = E(\xi \cdot \eta)$. Let $\alpha_n = \alpha_n(\omega)$ denote the indicator of the set A_n , i.e. $\alpha_n(\omega) = 1$ for $\omega \in A_n$ and $\alpha_n(\omega) = 0$ for $\omega \in \bar{A}_n$. Then the sequence $\{A_n\}$ of events is stable if and only if the sequence α_n converges weakly; the weak limit of the sequence α_n being equal to the local density of the sequence $\{A_n\}$. It follows that the sequence $\{A_n\}$ is mixing if and only if α_n converges weakly to a constant.

We introduce further the notion of a stable sequence of random variables. The sequence of random variables $\xi_n = \xi_n(\omega)$ ($n = 1, 2, \dots$) will be called *stable* if for any event B with $P(B) > 0$ the conditional distribution of ξ_n with respect to B tends to a limiting distribution, i.e.

$$\lim_{n \rightarrow +\infty} P(\xi_n < x | B) = F_B(x) \quad (1.5)$$

for every x which is a continuity point of the distribution function $F_B(x)$.

Expressed in terms of Hilbert space theory this means that for every bounded and continuous function $g(x)$ the sequence $g(\xi_n)$ converges weakly.

ON STABLE SEQUENCES OF EVENTS

An other equivalent definition of a stable sequence of random variables is the following: the sequence of random variables $\xi_n (n = 1, 2, \dots)$ is called *stable*, if for every $x \in X$ where X is a set of real numbers which is everywhere dense on the real line, the sequence of events $\xi_n < x (n = 1, 2, \dots)$ is stable.

Clearly such a sequence $\{\xi_n\}$ of random variables is stable in the sense of (1.5), because if (1.5) holds for x belonging to an everywhere dense set X then it holds for every continuity point x of $F_\mu(x)$. On the other hand (1.5) implies the stability of the sequence of events $\xi_n < x$ for $x \in X$ where the set X is everywhere dense on the real line.

In the special case when the limiting distribution $F_\mu(x)$ does not depend on the choice of B we arrive at the notion of a strongly mixing sequence of random variables, introduced previously (Rényi and Révész, 1958).

The aim of the present paper is to study general properties of stable sequences of events and to give criteria for the stability of a sequence of events which are discussed in Section 2; some examples and applications of these notions in probability theory are discussed in Section 3.

2. SOME GENERAL THEOREMS ON STABLE SEQUENCES OF EVENTS

Let $\alpha_n = \alpha_n(\omega)$ ($n = 1, 2, \dots$) be the indicator of the set A_n , i.e. $\alpha_n(\omega) = 1$ if $\omega \in A_n$ and $\alpha_n(\omega) = 0$ if $\omega \notin A_n$.

Let H denote the Hilbert space of all random variables ξ for which $E(\xi^2)$ exists, the inner product (ξ, η) being defined by $(\xi, \eta) = E(\xi \cdot \eta)$. We put further $\|\xi\| = (\xi, \xi)^{1/2}$. All definitions and theorems from Hilbert space theory which will be needed in the sequel can be found, e.g., in Szőkefalvi-Nagy (1942).

We prove first the following theorem.

Theorem 1: $\{A_n\}$ is a stable sequence of events, i.e. the limit

$$\lim_{n \rightarrow +\infty} P(A_n B) = Q(B) \quad (2.1)$$

exists for every $B \in \mathcal{A}$, if and only if $\{\alpha_n\}$ is a weakly convergent sequence of elements of the Hilbert space H , i.e. if for any $\eta \in H$ the limit

$$\lim_{n \rightarrow +\infty} (\alpha_n, \eta) = A(\eta) \quad (2.2)$$

exists.

Proof of Theorem 1: Clearly, if β is the indicator of the set B then $(\alpha_n, \beta) = P(A_n B)$. Thus (2.2) reduces to (2.1) if we substitute β instead of η . Thus to prove Theorem 1 it suffices to show that if the limit (2.2) exists whenever η is the indicator of a set B then it exists for every $\eta \in H$. Clearly, if the limit (2.2) exists for every indicator η , it exists also if η is an arbitrary element of H which takes on only a finite number of values. As to every random variable η for which $E(|\eta|) < +\infty$ and to every $\varepsilon > 0$ one can find, by the definition of the Lebesgue integral (Halmos, 1950) a random variable η_1 which takes on only a finite number of values, such that $E(|\eta - \eta_1|) < \varepsilon$, it follows easily that (2.2) holds not only for every $\eta \in H$ but also for every η for which $E(\eta)$ is finite. Thus Theorem 1 is proved.

As a consequence of Theorem 1 we obtain the following theorem.

Theorem 2 : If $\{A_n\}$ is a stable sequence of events, i.e. if

$$\lim_{n \rightarrow +\infty} P(A_n B) = Q(B) \quad (2.3)$$

exists for every $B \in \mathcal{A}$, then $Q(B)$ is a measure on $\mathcal{A}$ which is absolutely continuous with respect to the measure P , and thus can be represented in the form

$$Q(B) = \int_B \alpha dP \quad (2.4)$$

where $\alpha = \alpha(\omega)$ is a random variable; we have further $0 \leq \alpha \leq 1$.

Proof of Theorem 2 : Clearly $A(\eta)$ defined by (2.2) is a bounded linear operation on H , and thus by a well-known theorem [Szökefalvi-Nagy (1942)] there exists an $\alpha \in H$ such that $A(\eta)$ can be represented in the form $A(\eta) = (\alpha, \eta)$. It is easy to see that $0 \leq \alpha \leq 1$. It follows that, denoting by β the indicator of the event B , we have

$$Q(B) = (\alpha, \beta) = \int_B \alpha dP. \quad (2.5)$$

Thus $Q(B)$ is a measure, which is absolutely continuous with respect to the measure $P(B)$. We shall call $\alpha = \alpha(\omega)$ the *local density* of the stable sequence $\{A_n\}$.

Now we shall prove a criterion of the stability of a sequence of events which is the generalization of a corresponding criterion for mixing sequences, proved by the author (Rényi, 1958).

Theorem 3 : Let $\{A_n\}$ ($n = 1, 2, \dots$) be a sequence of events such that the limit

$$\lim_{n \rightarrow +\infty} P(A_n A_k) = Q_k \quad (2.6)$$

exists for $k = 1, 2, \dots$. Then the sequence $\{A_n\}$ is stable, i.e. (2.1) holds for every $B \in \mathcal{A}$.

Proof of Theorem 3 : Let H_1 denote the subspace of H spanned by the sequence $\{\alpha_n\}$ where α_n is the indicator of the event A_n ($n = 1, 2, \dots$), i.e. the closure with respect to the distance $\|\xi - \eta\|$ of the set of all finite linear combinations $\sum_{k=1}^n c_k \alpha_k$ where $c_1, c_2, \dots, c_n$ are arbitrary real numbers. Let H_2 denote the set of those elements ξ_2 of H which are orthogonal to every $\xi_1 \in H_1$.

According to a well-known theorem (see Szökefalvi-Nagy, 1942, p. 8) each element ξ of H can be represented in the form $\xi = \xi_1 + \xi_2$ where $\xi_1 \in H_1$ and $\xi_2 \in H_2$. Now we shall prove that if the limit (2.6) exists for $k = 1, 2, \dots$ then the limit

$$\lim_{n \rightarrow +\infty} (\alpha_n, \xi) = A(\xi) \quad (2.7)$$

exists for every $\xi \in H$. To prove this it suffices to show that (2.7) exists if $\xi = \xi_1 \in H_1$, because of the above mentioned decomposition of every $\xi \in H$ into the sum of a $\xi_1 \in H_1$ and a $\xi_2 \in H_2$; as a matter of fact if $\xi = \xi_2 \in H_2$ then (2.7) holds with $A(\xi_2) = 0$ while if the limit (2.7) exists for $\xi = \xi_1$ and $\xi = \xi_2$ it clearly exists for $\xi = \xi_1 + \xi_2$ also.

Now if ξ_1 is a linear combination of a finite number of the α_k 's then clearly the limit (2.7) exists. Let now ξ_1 be an arbitrary element of H_1 . Then to every $\epsilon > 0$ one can find a finite linear combination $\sum_{k=1}^N c_k \alpha_k$ such that

$$\left\| \xi_1 - \sum_{k=1}^N c_k \alpha_k \right\| < \epsilon. \quad (2.8)$$

But (2.8) implies in view of $\|\alpha_n\| \leq 1$ and the inequality $|(\xi, \eta)| \leq \|\xi\| \cdot \|\eta\|$, that

$$|(\alpha_n, \xi_1) - \sum_{k=1}^N c_k(\alpha_n, \alpha_k)| \leq \varepsilon. \quad (2.9)$$

Thus it follows that

$$|\overline{\lim}_{n \rightarrow +\infty} (\alpha_n, \xi_1) - \lim_{n \rightarrow +\infty} (\alpha_n, \xi_1)| \leq 2\varepsilon. \quad (2.10)$$

As $\varepsilon > 0$ is arbitrary it follows from (2.10) that the limit (2.7) exists. Thus Theorem 3 is proved.

Let us put (supposing $P(A_k) > 0$ for $k = 1, 2, \dots$, which is no essential restriction)

$$q_k = \frac{Q_k}{P(A_k)} \quad (k = 1, 2, \dots) \quad (2.11)$$

where Q_k is defined by (2.6).

Note that even if all the numbers q_k ($k = 1, 2, \dots$) are equal, it is not sure that the sequence $\{A_n\}$ is mixing. See for instance examples 1 and 2 of Section 3. This is true, however, in case $A_1 = \Omega$ as it has been shown by the author (Rényi, 1958).

Another way to express this fact is contained in Theorem 4.

Theorem 4: *Let $\{A_n\}$ be a stable sequence of events such that $\lim_{n \rightarrow +\infty} P(A_n) = q_0$ and $\lim_{n \rightarrow +\infty} P(A_n A_k) = q_k P(A_k)$ ($k = 1, 2, \dots$). Then the sequence $\{A_n\}$ is mixing if and only if the numbers q_k ($k = 0, 1, \dots$) are all equal to another.*

Proof of Theorem 4: The necessity of the condition follows immediately from the definition of mixing sequences.

The sufficiency can be proved as follows: Let α denote the local density of the sequence $\{A_n\}$. If $q_k = q \neq 0$ ($k = 0, 1, \dots$) then clearly

$$(\alpha, \alpha_k) = q(1, \alpha_k) \quad (2.12)$$

which can be also expressed as follows:

$$(\alpha, \alpha_k) = qP(A_k). \quad (2.13)$$

It follows by passing to the limit from (2.12) that

$$(\alpha, \alpha) = q(1, \alpha) \quad (2.14)$$

and from (2.13) that

$$(\alpha, \alpha) = q^2. \quad (2.15)$$

It follows that

$$q = (1, \alpha) \quad (2.16)$$

and therefore that

$$(\alpha, \alpha) = (1, \alpha)^2 \quad (2.17)$$

i.e.,

$$\int_{\Omega} \alpha^2 dP = \left(\int_{\Omega} \alpha dP \right)^2. \quad (2.18)$$

This implies that α is constant almost everywhere and thus by (2.15)

$$\alpha \equiv q. \quad (2.19)$$

The case $q = 0$ is trivial.

We should like to add the following remark:

In view of Theorem 1, Theorem 3 is a special case of the following.

Theorem: *A bounded sequence $\{\alpha_n\}$ ($n = 1, 2, \dots$) of elements of a Hilbert space H is weakly convergent if and only if the limits $\lim_{n \rightarrow +\infty} (\alpha_n, \alpha_k)$ exist for $k = 1, 2, \dots$.*

The proof of this assertion is exactly the same as that of Theorem 3. This useful theorem, which is due to E. Schmidt (see Schmeidler, 1954) is well known in Hilbert space theory; e.g. the proof in Szökefalvi-Nagy, (1942, p. 10) of the theorem that every bounded set is weakly compact, is based essentially on this fact.¹

Let us add that if $\{A_n\}$ is a stable sequence of events and α_n the indicator of A_n , then the sequence α_n converges strongly in H only in the trivial case when the weak limit of α_n is almost everywhere equal either to 1 or to 0, e.g., in the case mentioned in Example 1. As a matter of fact a necessary and sufficient condition of the strong convergence of α_n to α is $\lim_{n \rightarrow +\infty} \|\alpha_n\| = \|\alpha\|$. But

$$\lim_{n \rightarrow +\infty} \|\alpha_n\|^2 = \lim_{n \rightarrow +\infty} (\alpha_n, 1) = \int_{\Omega} \alpha dP$$

and $\|\alpha\|^2 = \int_{\Omega} \alpha^2 dP$. Thus α_n is strongly convergent to α if and only if $\int_{\Omega} \alpha(1-\alpha) dP = 0$ i.e. if $\alpha(1-\alpha) = 0$ almost everywhere.

In view of Theorem 4 and of the well-known theorem of Hilbert space theory according to which every bounded set is weakly compact, the following theorem holds :

Theorem 5 : Any sequence $\{A_n\}$ of events contains a subsequence which is stable.

An interesting feature of the stability of a sequence of events is that unlike such properties as independence, equivalence etc., it remains invariant when the underlying measure is replaced by another which is absolutely continuous with respect to the original measure. Moreover the local density of a stable sequence of events remains also unchanged.

Theorem 6 : Let $[\Omega, \mathcal{A}, P] = \mathcal{S}$ be a probability space and $\{A_n\}$ a stable sequence of events in $\mathcal{S}$. Let P^* be another probability measure on $\mathcal{A}$ which is absolutely continuous with respect to P . Then the sequence $\{A_n\}$ is stable on the probability space $\mathcal{S}^* = [\Omega, \mathcal{A}, P^*]$ also, with the same local density, i.e. if (2.1) and (2.4) hold, one has also

$$\lim_{n \rightarrow +\infty} P^*(A_n B) = \int_B \alpha dP^*. \quad (2.20)$$

Proof of Theorem 6 : By supposition

$$P^*(A) = \int_A \rho dP \quad \text{for } A \in \mathcal{A} \quad (2.21)$$

where $\rho = \rho(\omega)$ is a nonnegative random variable and $\int_{\Omega} \rho dP = 1$. It follows that

$$P^*(A_n, B) = \int_B \alpha_n \rho dP = (\alpha_n, \rho\beta) \quad (2.22)$$

where β is the indicator of the event $B \in \mathcal{A}$. Thus the existence of the limit (2.20) follows evidently from the remark made in course of proving Theorem 1 that the limit (2.2) exists not only if $\eta \in H$ but also under the single condition that $E(\eta)$ exists and that we have in this case also $A(\eta) = (\eta, \alpha)$. Thus it follows that

$$\lim_{n \rightarrow +\infty} P^*(A_n B) = (\alpha, \rho\beta) = \int_B \alpha dP^*.$$

¹ Prof. B. Sz. Nagy has kindly called my attention to this proof.

This proves Theorem 6. Let us mention that for mixing sequences a more general result supposing only the semi-continuity of P^* with respect to P has been proved by Sucheston (1962).

We want to make some further general remarks. It is impossible, except in trivial cases that the convergence in (2.1) should be uniform in B for all $B \in \mathcal{A}$. As a matter of fact, putting $B = A_n$ one has

$$P(A_n B) - Q(B) = P(A_n) - Q(A_n) = \int_0^1 (1 - \alpha) \alpha_n dP$$

and this difference tends to $\int_0^1 \alpha(1 - \alpha) dP$. Thus the convergence in (2.1) can be uniform only if the local density α is almost everywhere equal to 1 or 0 as in the trivial case of Example 1 in Section 3. Nevertheless the convergence in (2.1) may be uniform in B for $B \in \mathcal{B}$ where $\mathcal{B}$ is some proper subset of $\mathcal{A}$ which does not contain the sets A_n themselves or only a finite number of them. For instance, if there exist events B which are independent from all the events A_n , then these may all be contained in $\mathcal{B}$. If B is such an event then clearly the indicator β of B is uncorrelated with the local density α of the sequence $\{A_n\}$.

3. EXAMPLES OF STABLE SEQUENCES OF EVENTS

Example 1: A sequence of identical events $A_n = A$ ($n = 1, 2, \dots$) is evidently stable. Note that in this case the local density $\alpha(\omega)$ is equal to 1 for $\omega \in A$ and to 0 for $\omega \in \bar{A}$. Let us mention that the sequence $A, A, \dots$ is trivially mixing if $P(A) = 0$ or $P(A) = 1$ but not if $0 < P(A) < 1$.

More generally, if A'_n is a mixing sequence of events with density α , and A any event, the sequence $A_n = A'_n A$ is a stable sequence of events, with local density equal to α on A and 0 on $\bar{A}$.

Example 2: Let $\{A_n\}$ be a sequence of equivalent events (called also symmetrically dependent events) i.e. suppose

$$P(A_{i_1} A_{i_2} \dots A_{i_k}) = W_k \quad \dots (3.1)$$

for any choice of the different indices $i_1 < i_2 < \dots < i_k$ and for $k = 1, 2, \dots$ where W_k depends on k only, but not on the choice of the indices $i_1, i_2, \dots, i_k$. Such a sequence $\{A_n\}$ is evidently stable. As a matter of fact, it is sufficient to suppose the independence of W_k from the indices $i_1, i_2, \dots, i_k$ for $k = 2$ only. This follows clearly from Theorem 3.

Thus sequences of equivalent events are always stable. Note that in view of Theorem 4 a sequence of equivalent events is mixing if and only if

$$W_2 = W_1^2. \quad \dots (3.2)$$

It is easy to see however that (3.2) is satisfied if and only if the sequence $\{A_n\}$ is a sequence of independent events.

As a matter of fact according to a well-known theorem due to Khintchine (1952) if $\{A_n\}$ is a sequence of equivalent events and W_k is defined by (3.1) then there exists a distribution function $G(x)$ in the interval $[0, 1]$ such that

$$W_k = \int_0^1 x^k dG(x). \quad \dots (3.3)$$

As a matter of fact this follows from the following theorem of Hausdorff (1923). If a sequence $\{W_k\}$ is monotonic of every order, i.e. putting $W_0 = 1$

$$\sum_{j=1}^k (-1)^j \binom{k}{j} W_{n+j} \geq 0$$

for all $n \geq 0$ and $k \geq 0$ then W_k can be represented in the form (3.3). Now clearly $W_k = W_1^k$ means by (3.3) that

$$\int_0^1 x^2 dG(x) = \left(\int_0^1 x dG(x) \right)^2$$

which implies evidently that $G(x)$ is the distribution function of a constant c , i.e.

$$G(x) = \begin{cases} 1 & \text{for } x > c \\ 0 & \text{for } x \leq c \end{cases}$$

where of course $c = W_1$; but then according to (3.3) $W_k = W_1^k$ that is

$$P(A_{i_1} A_{i_2} \dots A_{i_k}) = \prod_{j=1}^k P(A_{i_j})$$

for every sequence $i_1 < i_2 < \dots < i_k$ and therefore the events are independent. Thus we have proved the following theorem.

Theorem 7 : *A sequence of equivalent events is always stable, but it is mixing if and only if the events are completely independent.*

Example 3 : Let Ω be the interval $(0, 1)$, $\mathcal{A}$ the set of measurable subset of Ω , and P the Lebesgue-measure. Let the set A_n be defined as the union of the intervals $\left(\frac{k}{n}, \frac{k+\lambda(k/n)}{n}\right)$ ($k = 0, 1, \dots, n-1$) where $\lambda(x)$ is a continuous function in the interval $[0, 1]$ such that $0 \leq \lambda(x) \leq 1$. Then clearly the sequence $\{A_n\}$ is stable with local density $\lambda(x)$.

This follows evidently as for any subinterval I of $[0, 1]$ we have

$$P(A_n I) = \frac{1}{n} \sum_{(k/n) \in I} \lambda\left(\frac{k}{n}\right) + O\left(\frac{1}{n}\right) \quad (3.4)$$

and the first term on the right of (3.4) is a Riemann sum of the integral $\int_I \lambda(x) dx$.

$$\text{Thus} \quad \lim_{n \rightarrow +\infty} P(A_n I) = \int_I \lambda(x) dx. \quad \dots (3.5)$$

It follows easily (e.g. by Theorem 3) that

$$\lim_{n \rightarrow +\infty} P(A_n B) = \int_B \lambda(x) dx \quad (3.6)$$

for every measurable set B , which proves our assertion.

Example 4 : Let us consider a stationary Markov chain with a finite number of states $1, 2, \dots, s$. Let ξ_0 , the state of the chain at time $t = 0$, have an arbitrary distribution over the set of states. Let ξ_n denote the state of the chain at time $t = n$ ($n = 1, 2, \dots$). Let A_n denote the event that the value of ξ_n belongs to a set E where E is a proper subset of the set of states. Let $p_{ij}^{(k)}$ denote the probability of a transition from state i into state j in k steps. Let us suppose that the limits

$$\lim_{k \rightarrow +\infty} p_{ij}^{(k)} = \pi_{ij}$$

exist for all i and j ; π_{ij} may depend in general on i . It follows that

$$\lim_{n \rightarrow +\infty} P(A_n A_k) = \sum_{i=1}^j W_i \left[\sum_{j \in E} p_{ij}^{(k)} \left(\sum_{h \in E} \pi_{jh} \right) \right] \quad (3.7)$$

where W_i is the probability that the chain started at time $t = 0$ in the state i . Thus by Theorem 3 the sequence $\{A_n\}$ is stable. Note that in case π_{ij} does not depend on i , the sequence $\{A_n\}$ is mixing.

Example 5: Let $S = [\Omega, \mathcal{A}, P]$ be a probability space. Suppose that $\Omega = \sum_{j=1}^{\infty} \Omega_j$; where $\Omega_j \in \mathcal{A}$ and $P(\Omega_j) > 0$ ($j = 1, 2, \dots$). Let $S_j = [\Omega_j, \mathcal{A}_j, P_j]$ be the probability space obtained by putting

$$P_j(A) = P(A | \Omega_j) \quad \text{for } A \in \mathcal{A}_j, \quad j = 1, 2, \dots$$

where $\mathcal{A}_j$ denotes the set of all $A \in \mathcal{A}$ such that $A \subset \Omega_j$.

Let $\{A_n^{(j)}\}$ be a mixing sequence of sets in the space S_j , with density α_j , and put $A_n = \sum_{j=1}^{\infty} A_n^{(j)} \Omega_j$. Then $\{A_n\}$ is a stable sequence of sets in S , with local density $\alpha(\omega) = \alpha_j$ for $\omega \in \Omega_j$ ($j = 1, 2, \dots$).

Clearly, Example 5 covers all cases in which the local density α of a stable sequence of sets has a discrete distribution. As a matter of fact let $[\Omega, \mathcal{A}, P]$ be a probability space and $\{A_n\}$ a stable sequence in this space with local density α where α is a discrete random variable, taking on the different values α_j ($j = 1, 2, \dots$) with positive probabilities. Let Ω_j denote the set of those ω for which $\alpha(\omega) = \alpha_j$. Put $P_j(A) = P(A | \Omega_j)$ for $j = 1, 2, \dots$. Then clearly for any $B \in \mathcal{A}$

$$\lim_{n \rightarrow +\infty} P_j(A_n B) = \lim_{n \rightarrow +\infty} \frac{P(A_n B \Omega_j)}{P(\Omega_j)} = \frac{Q(B \Omega_j)}{P(\Omega_j)} = \alpha_j P_j(B).$$

Thus the sequence $\{A_n\}$ is mixing in the probability space $[\Omega, \mathcal{A}, P_j]$ with density α_j ($j = 1, 2, \dots$).

Remarks: One can generalize Example 5 by splitting the probability space into a non-denumerable instead of a denumerable set of probability spaces, but in this case some care is necessary to avoid measure-theoretical difficulties. However, in this way we arrive at a decomposition of a stable sequence of events into the union of mixing sequences of events, in the most general case. This can be seen as follows. Let $\{A_n\}$ be a stable sequence of sets with local density $\alpha(\omega)$. Then one can define as usual the conditional probability of the event B with respect to a given value of α , which will be denoted by $P_\alpha(B)$. $P_\alpha(B)$ is a random variable such that

$$P(AB) = \int_A P_\alpha(B) dP \quad \text{for every } B \in \mathcal{A}$$

and every $A \in \mathcal{A}_\alpha$ where $\mathcal{A}_\alpha$ is the least σ -algebra on which α is measurable. By other words $P_\alpha(B)$ is the Radon-Nykodim derivative of the set function $P(AB)$ with B fixed with respect to $P(A)$ on the σ -algebra $\mathcal{A}_\alpha$.

As well known, while in case $B_k \in \mathcal{A}$, $B_k B_l = \phi$ for $k \neq l$ the relation

$$P_\alpha \left(\sum_{k=1}^{\infty} B_k \right) = \sum_{k=1}^{\infty} P_\alpha(B_k)$$

holds with probability 1, i.e., except for $\omega \in C$ where C is a set such that $P(C) = 0$ nevertheless one cannot say that $P_\alpha(B)$ is with probability 1 a measure, because the set C of

exceptional values of ω may depend on the sequence $\{B_k\}$ and the union of all possible such sets C may have positive measure or even be of measure 1. As however, $P_\alpha(B)$ is not uniquely determined and its value may be changed on a set of measure 0, it is often possible to find a determination of $P_\alpha(B)$ such that it is with probability one a measure. If this is the case it is easy to see that the sequence $\{A_n\}$ is almost surely mixing with respect to the measure $P_\alpha(B)$, with density α .

Such examples can be constructed by means of the theory of measurable decompositions of Lebesgue-spaces, developed by Rokhlin (1949). We do not propose to go into details here, but shall return to this question in another paper.

However, we give one example of a stable sequence of random variables constructed by the same principle as applied in the above Example 5 of stable sequence of events.

Example 6 : Let $\{\xi_n\}$ be a mixing sequence of random variables with limiting distribution $F(x)$ and η an arbitrary random variable having a discrete distribution. Let further $g(u, v)$ be a continuous function of two variables. Then the sequence of random variables

$$G_n = g(\xi_n, \eta) \quad (n = 1, 2, \dots)$$

is strictly stable. As a matter of fact if the values taken on by η with positive probability are denoted by y_k ($k = 1, 2, \dots$) and B_k denotes the event $\eta = y_k$ we have

$$\lim_{n \rightarrow +\infty} P(G_n < z | B) = \sum_{k=1}^{\infty} P(B_k | B) \int_{g(x, y_k) < z} dF(x). \quad (3.8)$$

We may take for instance $g(u, v) = u + v$ in which case we get

$$\lim_{n \rightarrow +\infty} P(G_n < z | B) = \sum_{k=1}^{\infty} P(B_k | B) F(z - y_k) \quad (3.9)$$

respectively, we may take $g(u, v) = uv$, in which case, supposing that $y_k > 0$ for $k = 1, 2, \dots$, we obtain

$$\lim_{n \rightarrow +\infty} P(G_n < z | B) = \sum_{k=1}^{\infty} P(B_k | B) F\left(\frac{z}{y_k}\right) \quad (3.10)$$

for all values of z for which the function on the right hand side of (3.9) respectively (3.10) is continuous.

REFERENCES

- HALMOS, P. (1950): *Measure Theory*. D. Van Nostrand, Princeton, N. J.
 HAUSDORFF, F. (1923): Momentenprobleme für ein endliches Intervall. *Math. Zeitschrift*, **16**, 220-224S.
 KHINTCHIN, A. (1952): O klassakh ekvivalentnykh sobytii, *Doklady Akad. Nauk. SSSR*, **85**, 713-714.
 RÉNYI, A. (1958): On mixing sequences of events. *Acta Math. Acad. Sci. Hung.*, **9**, 215-228.
 RÉNYI, A. and RÉVÉSZ, P. (1958): On mixing sequences of random variables. *Acta Math. Acad. Sci. Hung.*, **9**, 389-394.
 ROHLIN, V. A. (1949): On the fundamental notions of measure theory (in Russian). *Matem. Sbornik* **24**, 107-150.
 SUCHISTON, J. A. (1962): A zero-one property of mixing sequences of events. *Bull. Amer. Math. Soc.*, **68**, 330-332.
 SCHNEIDLER, W. (1954): *Lineare Operatoren in Hilbertschen Raum*. Teubner, Stuttgart.
 SZŐKEFALVI-NAGY, B. (1942): *Spektraldarstellung linearer Transformationen des Hilbertschen Raumes*. Springer, Berlin.

NOTE

The first systematic investigations of stable and mixing sets are due to Rényi and that of mixing random variables to Rényi and Révész.

See also [1], [2], [3], [4].

The following characterization of stable sequences is due to R. Fischler [5].

"The stable sequences are precisely those for which each subsequence contains a further subsequence for which the associated empirical measures converge weakly almost surely. From this it follows that if $\{x_j\}$ is a stable sequence and g satisfies certain continuity conditions then $\{g(x_j)\}$ is also stable."

The main area of application of this concept of mixing is the random-sum limit theorems, see the comments on papers Nos. 133, 169. (P. R.)

REFERENCES

- [1] Krengel, U. and Sucheston, L.: On mixing in infinite measure spaces, *Zeitschrift für Wahrscheinlichkeitstheorie u. verw. Geb.*, **13** (1969), 150—164.
- [2] Neveu, J.: Une démonstration élémentaire du théorème de récurrence. *Zeitschrift für Wahrscheinlichkeitstheorie u. verw. Geb.*, **4** (1965), 64—68.
- [3] Jacobs, K.: On Poincaré's recurrence theorem. *Fifth Berkeley Symposium II* 375—404.
- [4] Abbott, J. H. and Blum, J. R.: On a theorem of Rényi concerning mixing sequences of sets. *Annals of Math. Stat.*, **32/1**, 257—260.
- [5] Fischler, R.: Stable sequences of random variables and the weak convergence of the associated empirical measures. *Sankhyá, A* **33/1**, 67—72.

On the distribution of values of additive number-theoretical functions

By A. RÉNYI (Budapest)

Introduction

In our paper with P. TURÁN [1] we have given a new proof for the theorem of P. ERDŐS and M. KAC [2] according to which the distribution of the number of prime factors of the natural number n ($1 \leq n \leq N$) tends for $N \rightarrow +\infty$ to the normal distribution. Our method enabled us also to prove the conjecture of J. W. V. LE VEQUE concerning the exact order of magnitude of the remainder term in the theorem of ERDŐS—KAC. Our method consisted in using the usual methods of analytical number theory, i. e. expressing the sum of coefficients of a Dirichlet series by a contour integral, and in using certain function-theoretical properties of the ζ -function.

It is natural to guess that this powerful method yields also other known results on the distribution of values of additive number-theoretical functions. This is in fact true: however, for this purpose the technique has to be developed somewhat further. In the present paper we shall give a new proof running on the same lines as our proof of the Erdős—Kac theorem in [1], for the following theorem of P. ERDŐS [3]: *Let $f(n)$ be a real valued additive number-theoretical function, and put*

$$f^*(n) = \begin{cases} f(n) & \text{for } |f(n)| \leq 1 \\ 0 & \text{for } |f(n)| > 1. \end{cases}$$

Put

$$(1) \quad F_N(x) = \frac{1}{N} \sum_{\substack{f(n) \leq x \\ n \leq N}} 1.$$

Then the distribution-functions $F_N(x)$ tend for $N \rightarrow +\infty$ to a limiting distribution function $F(x)$ at all points of continuity of the latter¹⁾, if the following three conditions are satisfied:

1. $\sum_p \frac{f^*(p)}{p}$ is convergent,
2. $\sum_p \frac{(f^*(p))^2}{p} < +\infty$,
3. $\sum_{|f(p)| > 1} \frac{1}{p} < +\infty$.

¹⁾ It has been shown also by ERDŐS that if the series $\sum_{f(p) \neq 0} \frac{1}{p}$ is divergent then $F(x)$ is continuous, and thus $F_N(x)$ tends for $N \rightarrow +\infty$ to $F(x)$ for every value of x .

(Here and in what follows p runs over the sequence of primes). In this case the distribution function $F(x)$ has the characteristic function

$$(2) \quad g(u) = \int_{-\infty}^{+\infty} e^{iux} dF(x) = \prod_p \left(1 + \sum_{k=1}^{\infty} \frac{e^{iuf(p^k)} - e^{iuf(p^{k-1})}}{p^k} \right).$$

It has been proved later by P. ERDŐS and A. WINTNER [4] that the conditions 1), 2) and 3) are also necessary for the validity of the assertion of the theorem of ERDŐS.

Before giving in § 1 a new proof for this theorem let us mention that the theorem of ERDŐS and WINTNER shows a clear-cut resemblance to the three-series theorem of KOLMOGOROFF in probability theory. However, a proof of the Erdős—Wintner theorem, reducing it to the three-series theorem, has not been found up to now. An attempt in this direction has been made recently by E. M. PAUL [5] but he succeeded only in proving by purely probabilistic considerations that under the above conditions 1)–3) the *logarithmic* density of the numbers n , for which $f(n) < x$, exists and is equal to $F(x)$. This is, however, essentially less than the assertion that the ordinary density of these numbers equals $F(x)$. A new proof of the theorem of ERDŐS and WINTNER has recently been given by H. DELANGE [10].

In § 2. we make some remarks on the Erdős—Wintner theorem. We intend to return to other applications of the method in question (e. g. to prove a theorem of I. P. KUBILIUS [6]) in an other paper.

§ 1. Analytic proof of the theorem of Erdős

Before going into details, we give a sketch of the proof. Let us put²⁾

$$(1.1) \quad f_N(n) = \sum_{\substack{p^k \parallel n \\ p^k \leq N}} f(p^k).$$

Then clearly

$$(1.2) \quad f_N(n) = f(n) \quad \text{for } n \leq N$$

In order to prove the theorem in question, it would be sufficient, — according to the well known continuity theorem concerning characteristic functions — to show that for all real u one has

$$(1.3) \quad \lim_{N \rightarrow +\infty} \frac{1}{N} \sum_{n=1}^N e^{iuf(n)} = g(u),$$

where $g(u)$ is defined by (2). In view of (1.2) we can write (1.3) in the form

$$(1.4) \quad \lim_{N \rightarrow +\infty} \frac{1}{N} \sum_{n=1}^N e^{iuf_N(n)} = g(u).$$

²⁾ $p^k \parallel n$ means that n is divisible by p^k but not by p^{k+1} .

Now clearly

$$(1.5) \quad \lambda_N(s, u) = \sum_{n=1}^{\infty} \frac{e^{iuf_N(n)}}{n^s} = \prod_p \left(1 + \sum_{\substack{p^k \leq N \\ k \geq 1}} \frac{e^{iuf(p^k)}}{p^{ks}} + \sum_{p^k > N} \frac{1}{p^{ks}} \right),$$

and thus

$$(1.6) \quad \lambda_N(s, u) = \zeta(s) \mu_N(s, u)$$

where, putting $k(N, p) = \left\lceil \frac{\log N}{\log p} \right\rceil$, we have

$$(1.7) \quad \mu_N(s, u) = \prod_p \left(1 + \sum_{\substack{p^k \leq N \\ k \geq 1}} \frac{e^{iuf(p^k)} - e^{iuf(p^{k-1})}}{p^{ks}} + \frac{1 - e^{iuf(p^{k(N, p)+1})}}{p^{(k(N, p)+1)s}} \right).$$

As $\mu_N(s, u)$ is a Dirichlet-polynomial, it is an entire function, and its values can be easily estimated. Thus the behaviour of $\lambda_N(s, u)$ is sufficiently known in order to evaluate the sum of its first N coefficients. However carrying out this program in a straightforward manner leads to a proof of (1.4) only in the special case if instead of 1) the much more restrictive condition

$$1'. \quad \sum_p \frac{|f^*(p)|}{p} < +\infty$$

is satisfied, i. e. we get in this way not the full theorem of ERDŐS, only the special case which was previously obtained by I. J. SCHÖNBERG [7].

To get the full theorem we have to introduce the following modification of the method: we put

$$(1.8) \quad N^* = N^{\varepsilon_N}$$

where ε_N is a sequence of positive numbers, tending to 0 for $N \rightarrow +\infty$, such that

$$(1.9) \quad \varepsilon_N \sim \frac{\alpha}{e^{(\log \log N)^\beta}} \quad \text{with } \alpha > 0, \beta > \frac{1}{2}$$

and prove first

$$(1.10) \quad \lim_{N \rightarrow +\infty} \frac{1}{N} \sum_{n=1}^N e^{iuf_{N^*}(n)} = g(u).$$

As a matter of fact, we prove more, namely we obtain also an estimate (see (1.17)) of the remainder term in (1.10), and from this relation we can already deduce (1.4). The situation is still somewhat complicated, because for technical reasons we consider instead of the sum $\frac{1}{N} \sum_{n=1}^N e^{iuf_{N^*}(n)}$ the related sum

$$(1.11) \quad g_N(u, N^*) = \frac{1}{N} \sum_{n=1}^N e^{iuf_{N^*}(n)} \cdot \log \frac{N}{n}.$$

Let us pass now to the details. We have (see [8])

$$(1.12a) \quad g_N(u, N^*) = \frac{1}{2\pi i} \int_{(c)} \frac{\zeta(s) \mu_{N^*}(s, u) N^{s-1} ds}{s^2}.$$

and thus

$$(1.12b) \quad g_N(u, N^*) = \frac{\mu_{N^*}(1, u)}{2\pi i} \int_{(c)} \frac{N^{s-1} ds}{s^2(s-1)} + \\ + \frac{1}{2\pi i} \int_{(c)} \left(\zeta(s) - \frac{1}{s-1} \right) \frac{\mu_{N^*}(s, u) N^{s-1} ds}{s^2} + \frac{1}{2\pi i} \int_{(c)} \frac{(\mu_{N^*}(s, u) - \mu_{N^*}(1, u) N^{s-1}) ds}{(s-1)s^2}$$

where $\int_{(c)}$ denotes that the integration has to be carried out on the line $s = c + it$ from $t = -\infty$ to $t = +\infty$ and c is a real number, $c > 1$. Now according to the theorem of residues

$$(1.13) \quad \frac{1}{2\pi i} \int_{(c)} \frac{N^{s-1} ds}{(s-1)s^2} = 1 - \frac{1 + \log N}{N}.$$

On the other hand evidently under conditions 1)–3)

$$(1.14) \quad \lim_{N \rightarrow +\infty} \mu_{N^*}(1, u) = g(u)$$

for all real u . Thus the first term on the right hand side of (1.12) tends to $g(u)$; it remains to prove that the other two terms tend sufficiently rapidly to 0. As the integrand in both terms is regular for $s = \sigma + it$, $\sigma > 0$, the path of integration can in both integrals be shifted to the line $s = 1 + it$ i. e. we may take $c = 1$.

Now we have evidently for $s = 1 + it$

$$|\mu_{N^*}(s, u)| = O\left(e^{|u| \cdot \sum_{p \leq N^*} \frac{|f^*(p)|}{p}}\right)$$

and by the Cauchy inequality and condition 2) we obtain

$$\sum_{p \leq N^*} \frac{|f^*(p)|}{p} = O(\sqrt{\log \log N}).$$

Thus

$$(1.15) \quad |\mu_{N^*}(s, u)| \leq e^{|u| A \sqrt{\log \log N}}$$

where A is a positive constant. It is easy to see, that (1.15) holds not only for $s = 1 + it$ but also for $s = \sigma + it$ where $1 - \frac{1}{\log N^*} \leq \sigma \leq 1$.

Similarly we obtain (denoting by $\mu'_{N^*}(s, u)$ the derivative of $\mu_{N^*}(s, u)$ with respect to s) for $s = 1 + it$

$$(1.16) \quad |\mu'_{N^*}(s, u)| = O(\varepsilon_N \cdot \log N \cdot e^{A|u| \sqrt{\log \log N}})$$

where A is a positive constant. Thus we obtain by partial integration, taking into account the well-known estimates (see [8])

$$|\zeta(1 + it)| = O(\log |t|)$$

$$\left| \frac{\zeta'(1 + it)}{\zeta(1 + it)} \right| = O(\log |t|)$$

that the second term on the right of (1.12) is of order $O(\varepsilon_N \cdot e^{A|u|} \sqrt{\log \log N})$ and thus tends to 0 for $N \rightarrow +\infty$. As regards the third term of the right of (1.12) the path of integration can be transformed into the broken line $\mathfrak{L}$ consisting of the 5 segments

$$\mathfrak{L}_1: s = 1 + it \quad -\infty < t \leq -1,$$

$$\mathfrak{L}_2: s = \sigma - i \quad 1 \geq \sigma \geq 1 - \frac{1}{\log N^*},$$

$$\mathfrak{L}_3: s = 1 - \frac{1}{\log N^*} + it \quad -1 \leq t \leq +1,$$

$$\mathfrak{L}_4: s = \sigma + i \quad 1 - \frac{1}{\log N^*} \leq \sigma \leq 1,$$

$$\mathfrak{L}_5: s = 1 + it \quad 1 \leq t \leq +\infty.$$

Now as (1.15) holds for $s = 1 - \frac{1}{\log N^*} + it$ the contribution of the line $\mathfrak{L}_3$ to the third term on the right of (1.12) is of order

$$O(\log N \cdot e^{-\frac{1}{\varepsilon_N}}) = O(\varepsilon_N e^{A|u|} \sqrt{\log \log N}).$$

On $\mathfrak{L}_1$ and $\mathfrak{L}_5$ we can again apply partial integration, and use the estimates (1.15) resp. (1.16) and thus obtain that the contributions of the segments $\mathfrak{L}_1$ and $\mathfrak{L}_5$ are also of order $O(\varepsilon_N e^{A|u|} \sqrt{\log \log N})$.

Finally, in view of

$$\int_{1 - \frac{1}{\log N^*}}^1 N^{\sigma-1} d\sigma = O\left(\frac{1}{\log N}\right)$$

the contribution of the segments $\mathfrak{L}_3$ and $\mathfrak{L}_5$ is of order $O\left(\frac{e^{A|u|} \sqrt{\log \log N}}{\varepsilon_N \log N}\right) = O(\varepsilon_N e^{A|u|} \sqrt{\log \log N})$. Thus collecting all estimates, we obtain

$$(1.16) \quad g_N(u, N^*) = \mu_{N^*}(1, u) + O(\varepsilon_N \cdot e^{A|u|} \sqrt{\log \log N}).$$

Now let us apply (1.16) for N and $N' = \left\lfloor N \left(1 + \frac{1}{\log N}\right) \right\rfloor$ but with the same N^* and consider the difference of the two expressions. We obtain

$$(1.17) \quad \frac{1}{N} \sum_{n=1}^N e^{iuf_{N^*}(n)} = \mu_{N^*}(1, u) + O(\varepsilon_N e^{A|u|} \sqrt{\log \log N}).$$

Now let us consider the difference

$$(1.18) \quad d_N = \frac{1}{N} \sum_{n=1}^N e^{iuf_{N^*}(n)} - \frac{1}{N} \sum_{n=1}^N e^{iuf(n)}.$$

We have evidently

$$d_N = \frac{1}{N} \sum_{n=1}^N e^{iu f_{N^*}(n)} \cdot \left(e^{\frac{iu}{N^*} \sum_{N^* < p^k \leq N} f(p^k)} - 1 \right).$$

Now let us collect the terms in which there occurs in the exponent a prime power p^k with $k \geq 2$; the sum of these terms does not exceed

$$\frac{1}{N} \sum_{N^* \leq p^k, k \geq 2} \left[\frac{N}{p^k} \right] = O \left(\sum_{p \leq \sqrt{N^*}} \frac{1}{p^2} \right).$$

Thus the sum of these terms tends to 0. It follows that

$$(1.19) \quad d_N = \frac{1}{N} \sum_{n=1}^N e^{iu f_{N^*}(n)} \left(e^{\frac{iu}{N^*} \sum_{N^* < p \leq N} f(p)} - 1 \right) + o(1).$$

We can further disregard the terms in which there occurs in the exponent a p such that $|f(p)| > 1$, because the contribution of these terms is of order $O \left(\sum_{\substack{|f(p)| > 1 \\ p > N^*}} \frac{1}{p} \right)$.

Thus we have

$$(1.20) \quad d_N = \frac{1}{N} \sum_{n=1}^N e^{iu f_{N^*}(n)} \left(e^{\frac{iu}{N^*} \sum_{N^* < p \leq N} f^*(p)} - 1 \right) + o(1).$$

As

$$(1.21) \quad e^{i\alpha} = 1 + i\alpha + \frac{\theta \alpha^2}{2} \quad \text{where} \quad |\theta| \leq 1$$

we have

$$(1.22) \quad d_N = D_N + R_N + o(1),$$

where

$$D_N = \frac{iu}{N} \sum_{n=1}^N e^{iu f_{N^*}(n)} \left(\sum_{\substack{p|n \\ N^* < p \leq N}} f^*(p) \right)$$

and

$$|R_N| \leq \frac{u^2}{2N} \sum_{n=1}^N \left(\sum_{\substack{p|n \\ N^* < p \leq N}} f^*(p) \right)^2.$$

Clearly

$$|R_N| = O \left(\sum_{N^* < p} \frac{f^{*2}(p)}{p} + \left(\sum_{N^* < p < N} \frac{f^*(p)}{p} \right)^2 \right)$$

Thus in view of conditions 1), 2) and 3) it follows that

$$(1.23) \quad \lim_{N \rightarrow +\infty} R_N = 0,$$

and thus

$$(1.24) \quad d_N = D_N + o(1).$$

Let us consider now the term D_N . We have evidently

$$(1.25) \quad D_N = \frac{iu}{N} \sum_{N^* < p \leq N} f^*(p) \cdot \left[\sum_{m=1}^{\left[\frac{N}{p}\right]} e^{iuf_{N^*}(m)} \right].$$

Now let us consider first the contribution of those terms to D_N in which $p > \sqrt{N}$. The contribution of these terms clearly does not exceed $|u| \cdot \sum_{\sqrt{N} < p \leq N} \frac{|f^*(p)|}{p}$. As we have

$$\sum_{\sqrt{N} < p \leq N} \frac{|f^*(p)|}{p} \leq \sqrt{\left(\sum_{\sqrt{N} < p} \frac{f^{*2}(p)}{p} \right) \cdot \left(\sum_{\sqrt{N} < p \leq N} \frac{1}{p} \right)} = o(1),$$

we obtain

$$(1.26) \quad D_N = \frac{iu}{N} \sum_{N^* < p \leq \sqrt{N}} f^*(p) \cdot \left(\sum_{m=1}^{\left[\frac{N}{p}\right]} e^{iuf_{N^*}(m)} \right) + o(1).$$

Now we apply (1.17) to each sum $\sum_{m=1}^{\left[\frac{N}{p}\right]} e^{iuf_{N^*}(m)}$ in (1.26). Taking into account that for $N^* < p \leq \sqrt{N}$

$$N^* = N^{\varepsilon_N} = \left(\frac{N}{p} \right)^{\varepsilon(N,p)}$$

where

$$(1.27) \quad \varepsilon(N,p) = \frac{\varepsilon_N \log N}{\log N - \log p} = \theta \varepsilon_N \quad \text{with} \quad 1 \leq \theta \leq 2$$

it follows that

$$(1.28) \quad D_N = \frac{iu}{N} \sum_{N^* < p \leq \sqrt{N}} f^*(p) \left[\frac{N}{p} \right] \mu_{N^*}(1, u) + \varrho_N,$$

where

$$|\varrho_N| \leq \left(\sum_{N^* < p \leq \sqrt{N}} \frac{|f^*(p)|}{p} \right) \cdot O(\varepsilon_N e^{A|u|\sqrt{\log \log N}}).$$

Now, applying the estimate

$$\sum_{N^* < p \leq \sqrt{N}} \frac{|f^*(p)|}{p} = O(\sqrt{\log \log N}),$$

we obtain

$$(1.29) \quad \lim_{N \rightarrow +\infty} \varrho_N = 0.$$

On the other hand we have

$$\left(\sum_{N^* < p \leq \sqrt{N}} f^*(p) \left[\frac{N}{p} \right] \frac{1}{N} \right) = \sum_{N^* < p \leq \sqrt{N}} \frac{f^*(p)}{p} + O\left(\frac{1}{\sqrt{N}} \right).$$

As by condition 1) $\sum_{N^* < p \leq \sqrt{N}} \frac{f^*(p)}{p}$ tends to 0 and by (1.14) $\mu_{N^*}(1, u)$ tends to the limit $g(u)$ and thus is bounded, it follows that

$$(1.30) \quad \lim_{N \rightarrow +\infty} D_N = 0.$$

Thus we have proved that

$$(1.31) \quad \lim_{N \rightarrow +\infty} d_N = 0$$

and therefore (1.17) implies the validity of (1.3), which was to be proved. Thus the proof of the theorem of Erdős is completed.

§ 2. Some remarks on the Erdős—Wintner theorem

In the course of the proof of the theorem of Erdős in § 1 we have made use of the evident fact, that in case the conditions 1)–3) are satisfied the infinite product

$$(2.1) \quad g(u) = \prod_p \left(1 + \sum_{k=1}^{\infty} \frac{e^{iuf(p^k)} - e^{iuf(p^{k-1})}}{p^k} \right)$$

is convergent for every real u . Conversely it is easy to see that the convergence of this product for all real u implies the fulfilment of conditions 1)–3).

This can be shown as follows. If the infinite product (2.1) is convergent, then clearly the series

$$(2.2) \quad \sum_p \frac{e^{iuf(p)} - 1}{p}$$

is convergent too. Thus the real part of the series, i. e. the series with non-negative terms

$$(2.3) \quad \sum_p \frac{1 - \cos uf(p)}{p}$$

is convergent for every real u . Thus both of the series

$$(2.4) \quad \sum_{|f(p)| > 1} \frac{1 - \cos uf(p)}{p}$$

and

$$(2.5) \quad \sum_p \frac{1 - \cos uf^*(p)}{p}$$

are convergent too.

Now the convergence of (2.5) clearly implies the convergence of the series $\sum_p \frac{f^{*2}(p)}{p}$. On the other hand, it can be shown that the convergence of the series (2.4) implies the convergence of the series $\sum_{|f(p)| > 1} \frac{1}{p}$. To show this we need the following

Lemma. If the series $\sum_{n=1}^{\infty} b_n(1 - \cos a_n x)$ where $b_n \geq 0$ and $a_n \geq 1$ ($n=1, 2, \dots$) is convergent for every real x , then the series $\sum_{n=1}^{\infty} b_n$ is convergent.

PROOF OF LEMMA ³⁾. Let us put

$$(2.6) \quad S(x) = \sum_{n=1}^{\infty} b_n(1 - \cos a_n x).$$

As $S(x)$ is finite for every real x , and is a measurable function of x , there exists a set E of positive measure lying in a finite interval I on which $S(x)$ is bounded, $S(x) \leq K$. Denoting by $e(x)$ the indicator of the set E (i. e. $e(x)=1$ for $x \in E$ and $e(x)=0$ otherwise), and integrating the series (2.6) on the set E (the integration can be carried out term by term owing to BEPPO LEVI's theorem) we obtain

$$\sum_{n=1}^{\infty} b_n \int_I (1 - \cos a_n x) e(x) dx \leq K|E|$$

where $|E|$ denotes the measure of the set E . Now evidently $G(a) = \int_I (1 - \cos ax) e(x) dx$ as a function of a is bounded from below by a positive constant for $1 \leq a < +\infty$. (As a matter of fact, $G(a)$ is everywhere positive, continuous and by Riemann's lemma $\lim_{a \rightarrow +\infty} G(a) = |E| > 0$.) It follows, putting

$\min_{1 \leq a < +\infty} G(a) = g$, that

$$g \sum_{n=1}^{\infty} b_n \leq K \cdot |E|.$$

This proves the Lemma.

Now the convergence of the series $\sum_p \frac{f^{*2}(p)}{p}$ and $\sum_{|f(p)| > 1} \frac{1}{p}$, together with that of the series (2.2) imply by (1.21) the convergence of the series $\sum_p \frac{f^*(p)}{p}$. Thus conditions 1)–3) are satisfied.

Therefore the theorem of ERDŐS and WINTNER can also be formulated as follows: for the existence of the limiting distribution of the values of an additive arithmetic function $f(n)$ the convergence of the infinite product (2.1) is necessary and sufficient.

This reformulation of their theorem has been already given by ERDŐS and WINTNER themselves in [4]; however, they deduced this form of the theorem from the original one in another, indirect way, by using the theory of infinite convolutions.

³⁾ This Lemma can be proved in exactly the same way as the theorem of DENJOY–LUSIN (see [9], p. 232); nevertheless, for the sake of the convenience of the reader, I give here the proof.

Bibliography

- [1] A. RÉNYI—P. TURÁN, On a theorem of Erdős and Kac, *Acta Arithmetica* 1 (1957), 71—84.
- [2] P. ERDŐS—M. KAC, The Gaussian law of errors in the theory of additive number-theoretic functions, *Amer. J. Math.* 62 (1940), 738—742.
- [3] P. ERDŐS, On the density of some sequences of numbers, III. *J. London Math. Soc.* 13 (1938), 119—127.
- [4] P. ERDŐS—A. WINTNER, Additive arithmetic functions and statistical independence, *Amer. J. Math.* 61 (1939), 713—721.
- [5] I. P. KUBILIUS, Probabilistic methods in number theory, 2nd edition (in Russian), Vilnius, 1962.
- [6] E. M. PAUL, Density in the light of probability theory, *Sankhyā* 24 (1962), 103—114.
- [7] I. J. SCHÖNBERG, On the asymptotic distribution of arithmetical functions, *Trans. Amer. Math. Soc.* 39 (1936), 315—330.
- [8] E. C. TITCHMARSH, The theory of the Riemann Zeta-function. Oxford, 1951.
- [9] A. ZYGMUND, Trigonometric series, I., Cambridge, 1959.
- [10] H. DELANGE, Un théorème sur les fonctions arithmétiques multiplicatives et ses applications, *Ann. Sci. Ecole Norm. Sup.* 78 (1961), 1—29.

251

NOTE

As to the problem, mentioned in the paper, of finding a purely probabilistic proof of the Erdős—Wintner theorem, the reader is referred to the work by Novoselov (*Izv. Akad. Nauk SSSR, Ser. Math.*, 28 (1964), 307—364) and also papers by Jogesh Babu (e.g. *Acta Arithm.*, vol. 23, No. 4.) where actual use is made of the three series theorem of Kolmogorov. J. Galambos, starting off with the method of proof of Rényi's paper No. 251 which is a further simplified version of the present one, gave another probabilistic interpretation. (See his survey article in *Ann. Inst. Henri Poincaré, Section B*, VI, 4 (1970), 281—305.) (G. H.)

A study of sequences of equivalent events as special stable sequences

By A. RÉNYI and P. RÉVÉSZ (Budapest)

Introduction

Let $\{\Omega, S, P\}$ be a probability space and $A_1, A_2, \dots$ be a finite or infinite sequence of events (i. e. $A_1, A_2, \dots$ are subsets of Ω belonging to the σ -algebra S) in this space. The events A_n are called equivalent (or symmetrically dependent, see [1]) if the probability of the event¹⁾ $A_{i_1}A_{i_2}\dots A_{i_k}$ ($i_j \neq i_l$ if $j \neq l$) depends only on k and it does not depend on the indices $i_1, i_2, \dots, i_k$. The simplest examples of sequences of equivalent events are the sequences of mutually independent events having the same probability. A more general example is the following: Let $A_n(t)$ ($0 \leq t \leq 1$; $n=1, 2, \dots$) for every fixed t be a sequence of independent events, such that $P(A_n(t))=t$ ($n=1, 2, \dots$) and let $\lambda(\omega)$ be a random variable with values in the interval $[0, 1]$. Then $A_n(\lambda)$ is a sequence of equivalent events, provided that $A_n(\lambda) = \bigcup_{0 \leq t \leq 1} (A_n(t) \cap \{\lambda(\omega)=t\})$ are events ($n=1, 2, \dots$) i. e. they are elements of S .

One can ask which sequences of equivalent events can be represented in this form. In connection with this question an important result is due to DE FINETTI [2]. (See also [3], [4] and for generalisations [5].) It is the following:

Theorem 1. *Let $A_1, A_2, \dots$ be an infinite sequence of equivalent events and put*

$$P(A_1A_2\dots A_k) = \omega_k.$$

Then there exists a distribution function $F(x)$ such that

$$F(0)=0, \quad F(1+0) = 1$$

and

$$\omega_k = \int_0^{1+0} x^k dF(x) \quad (k=1, 2, \dots).$$

In view of this theorem a very natural conjecture is the following: every infinite sequence of equivalent events can be represented in the mentioned form; or with other words: if $A_1, A_2, \dots$ is an infinite sequence of equivalent events, then there exists a random variable $\lambda(\omega)$ ($0 \leq \lambda(\omega) \leq 1$) such that the events $A_1, A_2, \dots$ are

¹⁾ Here and in what follows the product of events denotes the joint occurrence of these events (that is the intersection of the corresponding sets).

under the condition $\lambda(\omega) = x$ independent, and have the probability x , i. e.

$$\mathbf{P}(A_{i_1} A_{i_2} \dots A_{i_k} | \lambda(\omega) = x) = x^k \quad (\text{with probability } 1).$$

In § 2. of this paper we prove the above mentioned conjecture (Theorem 2.). Before doing this in § 1 we give a new proof of DE FINETTI's theorem. § 3. contains some remarks on equivalent random variables.

§ 1. A new proof of de Finetti's theorem

We recall some definitions and results of paper [6]. A sequence of events $A_1, A_2, \dots$ is called a *stable* sequence if

$$(1.1) \quad \lim_{n \rightarrow \infty} \mathbf{P}(A_n B) = \mathbf{Q}(B)$$

exists for every event $B \in \mathcal{S}$. It is easy to see that $\mathbf{Q}(B)$ is a measure which is absolutely continuous with respect to $\mathbf{P}$. Let the Radon—Nikodym derivative of $\mathbf{Q}$ with respect to $\mathbf{P}$ be $\lambda(\omega)$, i. e.

$$\mathbf{Q}(B) = \int_B \lambda(\omega) d\mathbf{P}, \quad \text{for } B \in \mathcal{S}.$$

The random variable $\lambda(\omega)$ is called the *local density* of the stable sequence $A_1, A_2, \dots$. Clearly $0 \leq \lambda(\omega) \leq 1$.

In [6] it is proved that if $\{A_n\}$ is a stable sequence of events with the indicator functions $\alpha_n(\omega)$, i. e.

$$\alpha_n(\omega) = \begin{cases} 1 & \text{if } \omega \in A_n \\ 0 & \text{if } \omega \in \bar{A}_n \end{cases}$$

then α_n converges to λ weakly i. e. for every element g of the Hilbert-space $L^2_{\mathbf{P}}(\Omega)$

$$(1.2) \quad \lim_{n \rightarrow \infty} (g, \alpha_n) = \lim_{n \rightarrow \infty} \int_{\Omega} g \alpha_n d\mathbf{P} = \int_{\Omega} g \lambda d\mathbf{P} = (g, \lambda).$$

If λ is constant (with probability 1) the stable sequence $A_1, A_2, \dots$ is called *mixing* (see [10]). It is shown further in [6] that in order that a sequence $\{A_n\}$ should be stable it is sufficient that the limit

$$\lim_{n \rightarrow \infty} \mathbf{P}(A_k A_n) = \mathbf{Q}(A_k)$$

should exist for each $k = 1, 2, \dots$. It follows evidently that every sequence of equivalent events is stable. Using these facts a very simple proof of DE FINETTI's theorem can be given.

THE PROOF OF DE FINETTI'S THEOREM. Let the local density of the sequence $A_1, A_2, \dots$ of equivalent events be $\lambda(\omega)$, and we denote the indicator function of A_n by α_n . Then we have

$$\omega_k = \mathbf{P}(A_{i_1} A_{i_2} \dots A_{i_k}) = \int_{\Omega} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k} d\mathbf{P} = (\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_{k-1}}, \alpha_{i_k}).$$

Thus by (1.2)

$$\omega_k = \lim_{i_k \rightarrow \infty} (\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_{k-1}}, \alpha_{i_k}) = (\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_{k-1}}, \lambda) = (\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_{k-2}} \lambda, \alpha_{i_{k-1}}).$$

Applying the same argument again, we obtain

$$\omega_k = \lim_{i_{k-1} \rightarrow \infty} (\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_{k-2}} \lambda, \alpha_{i_{k-1}}) = (\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_{k-2}} \lambda, \lambda).$$

Applying the same argument again $k-2$ times, we obtain that

$$(1.3) \quad \omega_k = \mathbf{P}(A_{i_1} A_{i_2} \dots A_{i_k}) = \int_{\Omega} \lambda^k(\omega) d\mathbf{P} = \int_0^1 x^k dF_{\lambda}(x)$$

where $F_{\lambda}(x)$ is the distribution function of $\lambda(\omega)$. Thus the theorem of DE FINETTI is proved.

As a matter of fact we have proved somewhat more, namely that for any $k \geq 1$, for any set of k different positive integers $i_1, i_2, \dots, i_k$ and for any r with $0 \leq r \leq k$ we have

$$(1.4) \quad \mathbf{P}(A_{i_1} A_{i_2} \dots A_{i_k}) = \int_{\Omega A_{i_1} A_{i_2} \dots A_{i_r}} \lambda^{k-r}(\omega) d\mathbf{P}.$$

Clearly (1.4) reduces for $r=0$ to (1.3), while in the other extreme case $r=k$ (1.4) is trivial. We shall need (1.4) in the course of the proof of Theorem 2 in § 2.

Now we show how to any distribution function $F(x)$ such that $F(0)=0$ and $F(1+0)=1$ a sequence $\{A_n\}$ of equivalent events can be constructed such that

$$\mathbf{P}(A_{i_1} A_{i_2} \dots A_{i_k}) = \omega_k = \int_0^1 x^k dF(x)$$

for any $k=1, 2, \dots$ and any set of different integers $i_1, i_2, \dots, i_k$. Such a sequence $\{A_n\}$ can easily be constructed in any nonatomic probability space, by using the evident fact that the sequence $\{\omega_k\}$ is absolutely monotonic, i. e. (putting $\omega_0=1$)

$$\Delta^r \omega_n = \sum_{j=0}^r \binom{r}{j} (-1)^j \omega_{n+j} = \int_0^1 x^n (1-x)^r dF(x) \geq 0, \quad \text{for } r \geq 0, n \geq 0.$$

However, our example gives much more, as it exhibits explicitly the local density $\lambda(\omega)$ and shows that the events A_n are in fact conditionally independent under the condition $\lambda(\omega)=x$ and have the probability x , for any x with $0 < x < 1$.

Let the probability space Ω be the unit square of the plane, i. e.

$$\Omega = I_1 \times I_2$$

where I_1 and I_2 are unit intervals. Let the probability measure $\mathbf{P}$ on Ω be the product measure

$$\mathbf{P} = \mu_1 \times \mu_2$$

where μ_1 is the Lebesgue—Stieltjes measure on I_1 defined by the distribution function $F(x)$ and μ_2 is the ordinary Lebesgue-measure on I_2 .

To define the events A_n we need first to define a set of polynomials

$$p_k^{(n)}(x) \quad (k=0, 1, 2, \dots, 2^n; n=1, 2, \dots)$$

as follows: $p_0^{(n)}(x) \equiv 0$, and

$$p_{k+1}^{(n)}(x) = \sum_{j=0}^k x^{\alpha_n(j)} (1-x)^{\beta_n(j)} \quad \text{for } k=0, 1, \dots, 2^n-1$$

where $\alpha_n(j)$ resp. $\beta_n(j)$ denote the number of zeros resp. ones in the dyadic expansion of $j/2^n$; more exactly if

$$\frac{j}{2^n} = \sum_{i=1}^n \frac{\varepsilon_i}{2^i} \quad \text{where } \varepsilon_i \text{ is 0 or 1}$$

then

$$\beta_n(j) = \sum_{i=1}^n \varepsilon_i \quad \text{and} \quad \alpha_n(j) = n - \beta_n(j).$$

Thus — for instance —

$$p_0^{(3)}(x) \equiv 0 \quad p_4^{(3)}(x) = x^3 + 2x^2(1-x) + x(1-x)^2$$

$$p_1^{(3)}(x) = x^3 \quad p_5^{(3)}(x) = x^3 + 3x^2(1-x) + x(1-x)^2$$

$$p_2^{(3)}(x) = x^3 + x^2(1-x) \quad p_6^{(3)}(x) = x^3 + 3x^2(1-x) + 2x(1-x)^2$$

$$p_3^{(3)}(x) = x^3 + 2x^2(1-x) \quad p_7^{(3)}(x) = x^3 + 3x^2(1-x) + 3x(1-x)^2$$

$$p_8^{(3)}(x) = x^3 + 3x^2(1-x) + 3x(1-x)^2 + (1-x)^3 \equiv 1.$$

In general we have $p_{2^n}^{(n)}(x) \equiv 1$ for $n=1, 2, \dots$.

Now let $B_k^{(n)}$ be the set of all points (x, y) for which $p_{2k}^{(n)}(x) \leq y < p_{2k+1}^{(n)}(x)$ and let A_n be the union of the sets $B_k^{(n)}$ ($k=0, 1, 2, \dots, 2^{n-1}-1$).

It is easy to verify that the events A_n are equivalent and

$$P(A_{i_1} A_{i_2} \dots A_{i_k}) = \omega_k = \int_0^1 x^k dF(x) \quad \text{for } k=1, 2, \dots \text{ and } i_1 < i_2 < \dots < i_k.$$

Clearly $\lambda(x, y) = x$ and the events A_n are independent under the condition $\lambda = x$ and all have the probability x ($0 < x < 1$).

Let us mention that the well known theorem of HAUSDORFF [9] — according to which a necessary and sufficient condition for a sequence $\{\omega_k\}$ to be absolutely monotonic is that ω_k should be the k -th moment of a distribution function in the interval $(0, 1)$ — follows easily from DE FINETTI's theorem. Thus the theorem of HAUSDORFF in question can be proved in a purely probabilistic way.

§ 2. The general form of a sequence of equivalent events

The aim of this § is to prove the following

Theorem 2. *Let $A_1, A_2, \dots$ be a sequence of equivalent events. Let $\lambda(\omega)$ be the local density of the sequence $\{A_n\}$ considered as a stable sequence. Then we have²⁾*

$$(2.1) \quad \mathbf{P}(A_{i_1} A_{i_2} \dots A_{i_k} | \lambda(\omega)) = \lambda^k(\omega) \quad \text{with probability 1}$$

for $k=1, 2, \dots$ and $i_1 < i_2 < \dots < i_k$.

PROOF. First of all we prove (2.1) for $k=1$. Let us assume that

$$(2.2) \quad \mathbf{P}(A_n | \lambda) = \lambda(\omega) + \varepsilon_n(\omega).$$

Here $\varepsilon_n(\omega)$ is a Baire-function of $\lambda(\omega)$ by the definition of conditional probability (see [7]). Put $\varepsilon_n(\omega) = g_n(\lambda(\omega))$ and let $\alpha_n(\omega)$ denote the indicator function of A_n . Let us denote by $\mathbf{M}(\xi)$ the expectation of the random variable ξ and by $\mathbf{M}(\xi|\eta)$ the conditional expectation of ξ with respect to the random variable η . In what follows we shall use repeatedly the following well known properties of conditional expectations (see [7]): for any ξ for which $\mathbf{M}(\xi)$ exists and any η

$$(2.3) \quad \mathbf{M}(\xi) = \mathbf{M}(\mathbf{M}(\xi|\eta))$$

further

$$(2.4) \quad \mathbf{M}(g(\eta)\xi|\eta) = g(\eta)\mathbf{M}(\xi|\eta)$$

where $g(x)$ is a Baire function. Now we have by (1.3), (2.2) and (2.3)

$$\mathbf{P}(A_n) = \int_{\Omega} \lambda d\mathbf{P} = \mathbf{M}(\mathbf{M}(\alpha_n|\lambda)) = \mathbf{M}(\lambda + \varepsilon_n)$$

therefore $\mathbf{M}(\varepsilon_n) = 0$ ($n=1, 2, \dots$).

Similarly, using (1.4), (2.2), (2.3) and (2.4) we have

$$\begin{aligned} \mathbf{P}(A_k A_l) &= \int_{\Omega} \lambda^2 d\mathbf{P} = \int_{A_k} \lambda d\mathbf{P} = \mathbf{M}(\lambda \alpha_k) = \mathbf{M}(\mathbf{M}(\lambda \alpha_k | \lambda)) = \\ &= \mathbf{M}(\lambda \mathbf{M}(\alpha_k | \lambda)) = \mathbf{M}(\lambda(\lambda + \varepsilon_k)) = \mathbf{M}(\lambda^2) + \mathbf{M}(\lambda \varepsilon_k). \end{aligned}$$

Therefore $\mathbf{M}(\lambda \varepsilon_k) = 0$ ($k=1, 2, \dots$). Similarly we obtain

$$\mathbf{M}(\lambda^n \varepsilon_k) = \int_0^1 x^n g_k(x) dF_{\lambda}(x) = 0 \quad (n=0, 1, 2, \dots; k=1, 2, \dots)$$

where $F_{\lambda}(x)$ is the distribution function of $\lambda(\omega)$. The fact that the sequence $\{x^n\}$ is a complete sequence in the space $L^2_{F_{\lambda}}(0, 1)$ (the space of functions in the interval $[0, 1]$ which are square integrable with respect to the measure defined by the distribution function $F_{\lambda}(x)$) ([8]), implies that $g_n(x)$ is equal to 0 almost everywhere with respect to the measure defined by $F_{\lambda}(x)$; thus we have

$$\mathbf{P}(\varepsilon_r = 0) = 1 \quad (r=1, 2, \dots)$$

²⁾ $\mathbf{P}(B|\lambda)$ denotes the conditional probability of the event B under the condition that the random variable λ takes on a fixed value.

The proof for $k=2$ is completely similar to the above proof. Let us put

$$\mathbf{P}(A_i A_j | \lambda) = \lambda^2 + \varepsilon_{ij}$$

where ε_{ij} is a Baire-function of λ . With these notations we have

$$\mathbf{P}(A_i A_j) = \mathbf{M}(\alpha_i \alpha_j) = \int_{\Omega} \lambda^2 d\mathbf{P} = \mathbf{M}[\mathbf{M}(\alpha_i \alpha_j | \lambda)] = \mathbf{M}(\lambda^2 + \varepsilon_{ij})$$

and therefore

$$\mathbf{M}(\varepsilon_{ij}) = 0.$$

Similarly

$$\begin{aligned} \mathbf{P}(A_i A_j A_k) &= \int_{\Omega} \lambda^3 d\mathbf{P} = \int_{A_i A_j} \lambda d\mathbf{P} = \mathbf{M}(\alpha_i \alpha_j \lambda) = \mathbf{M}[\mathbf{M}(\alpha_i \alpha_j \lambda | \lambda)] = \\ &= \mathbf{M}(\lambda(\mathbf{M}(\alpha_i \alpha_j | \lambda))) = \mathbf{M}(\lambda(\lambda^2 + \varepsilon_{ij})) = \mathbf{M}(\lambda^3) + \mathbf{M}(\lambda \varepsilon_{ij}) \end{aligned}$$

so

$$\mathbf{M}(\lambda \varepsilon_{ij}) = 0$$

and in general we obtain

$$\mathbf{M}(\varepsilon_{ij} \lambda^n) = 0 \text{ for } n=0, 1, \dots \text{ i. e. } \mathbf{P}(\varepsilon_{ij}=0) = 1.$$

The proof of (2.1) for any value of k is essentially the same.

§ 3. Equivalent random variables

Let $\xi_1, \xi_2, \dots$ be a finite or infinite sequence of random variables. The random variables $\{\xi_n\}$ are called equivalent if the distribution function

$$F_n(x_1, x_2, \dots, x_n) = \mathbf{P}\{\xi_{i_1} < x_1, \xi_{i_2} < x_2, \dots, \xi_{i_n} < x_n\}$$

depends only on n and $x_1, x_2, \dots, x_n$, and it does not depend on the sequence of different integers $i_1, i_2, \dots, i_n$. One can ask what are the generalizations of Theorems 1. and 2. for equivalent random variables.

A sequence $\{\xi_n\}$ of random variables is called a stable sequence (see [6]) if the sequence of events $A_n(x) = \{\xi_n < x\}$ ($n=1, 2, \dots$) is stable for every x belonging to a set X which is everywhere dense on the real line. Let $\lambda_x(\omega)$ denote the local density of the stable sequence $\{A_n(x)\}$. If $\lambda_x(\omega)$ is a constant for every $x \in X$, the sequence is mixing (see [11]). Clearly any sequence of equivalent random variables is stable in the above sense.

Let us denote the event $\{\xi_n < x\}$ by $A_n(x)$. It is evident that $A_n(x)$ ($n=1, 2, \dots$) is a sequence of equivalent events for every x , if $\{\xi_n\}$ is a sequence of equivalent random variables. Let the local density of the sequence $A_n(x)$ be $\lambda_x(\omega)$.

The following result is valid (see [2] and [5])

Theorem 3. *If $\xi_1, \xi_2, \dots$ is an infinite sequence of equivalent random variables then*

$$\mathbf{P}(\xi_{i_1} < x_1, \xi_{i_2} < x_2, \dots, \xi_{i_n} < x_n) = F_n(x_1, \dots, x_n) = \int \lambda_{x_1}(\omega) \dots \lambda_{x_n}(\omega) d\mathbf{P}.$$

Clearly $\lambda(\omega)$ as a function of x is a distribution function for almost all ω . The proof of this theorem is exactly the same as the proof of Theorem 1.

The evident generalization of Theorem 2 is the following statement: the equivalent random variables $\xi_1, \xi_2, \dots$ are independent and identically distributed with respect to F where F is the least σ -algebra containing all the σ -algebras A_x ($-\infty < x < +\infty$) where A_x is the smallest σ -algebra with respect to which $\lambda_x(\omega)$ is measurable.

Bibliography

- [1] B. DE FINETTI, *Mem. della R. Acc. Naz. dei Lincei* (6), 4, **86** (1930).
- [2] B. DE FINETTI, La prévision: ses lois logiques, ses sources subjectives, *Ann. Inst. H. Poincaré*, **7** (1937), 1-68.
- [3] А. Я. ХИНИЧИН, о классах эквивалентных событий, *Математический Сборник*, **39** (1932), 40-43.
- [4] А. Я. ХИНИЧИН, О классах эквивалентных событий, *Доклады Акад. наук СССР* **85** (1952) 713-714.
- [5] E. HEWITT — L. J. SAVAGE, Symmetric measures on Cartesian products, *Trans. Amer. Math. Soc.*, **80** (1955), 470-501.
- [6] A. RÉNYI, On stable sequences of events, *SANKHYA* (in print).
- [7] A. KOLMOGOROFF, *Grundbegriffe der Wahrscheinlichkeitsrechnung*. Berlin, 1933.
- [8] G. ALEXITS, Convergence problems of orthogonal series, *Budapest*, 1961.
- [9] F. HAUSDORFF, Momentprobleme für ein endliches Intervall, *Math. Z.* **16** (1923), 220-248.
- [10] A. RÉNYI, On mixing sequences of events, *Acta Math. Acad. Sci. Hungar.* **9** (1958), 215-228.
- [11] A. RÉNYI—P. RÉVÉSZ, On mixing sequences of random variables, *Acta Math. Acad. Sci. Hungar.* **9** (1958), 389-394.

NOTE

A useful new treatment of exchangeable (equivalent) events has been made by D. G. Kendall [1].

For different limit distribution theorems for exchangeable events and random variables see e.g. [1], [2], [3] and [4]. [P. R.]

REFERENCES

- [1] Kendall, D. G.: On finite and infinite sequences of exchangeable events. *Studia Sci. Math. Hung.*, **2** (1967), 319-327.
- [2] Benczur, A.: On sequences of equivalent events and the compound Poisson process. *Studia Sci. Math. Hung.*, **3** (1968), 451-458.
- [3] Révész, P.: A central limit theorem for equivalent random variables. *Publicationes Mathematicae, Debrecen*, **12** (1965), 295-302.
- [4] Billingsley, P.: *Convergence of Probability Measures*. John Wiley & Sons Inc. New York, 212.

ON „SMALL” COEFFICIENTS OF THE POWER SERIES OF ENTIRE FUNCTIONS

By

ALFRÉD RÉNYI and CATHERINE RÉNYI

Department of Theory of Probability and Analysis of the Eötvös Loránd University Budapest

(Received May 6, 1963)

§ 1. Introduction

The second named author has proved (see [1]) some years ago the following

THEOREM A. *Let $f(z)$ be a transcendental entire function and let*

$$f(z) = \sum_{n=0}^{\infty} a_n z^n$$

and

$$f(z) = \sum_{n=0}^{\infty} b_n (z-1)^n$$

be the power series of $f(z)$ around the points¹ $z=0$ and $z=1$ respectively. Let $Z_0(n)$ resp. $Z_1(n)$ denote the number of zeros in the sequence $a_0, a_1, \dots, a_{n-1}$ resp. $b_0, b_1, \dots, b_{n-1}$. Then

$$\liminf_{n \rightarrow \infty} \frac{Z_0(n) + Z_1(n)}{n} \leq 1.$$

Theorem A can be formulated somewhat vaguely in the following way: if there are „many” zeros among the coefficients of the power series of a transcendental entire function about the point $z=0$, then there can not be „too many” zeros among the coefficients of its power series about the point $z=1$.

In the present paper we shall prove a generalization of Theorem A, whose statement can be expressed somewhat vaguely as follows: if „many” of the coefficients of the power series of an entire transcendental function about the point $z=0$ are „small”, then there can not be „too many” „small” coefficients in the power series of the same function about the point $z=1$. Of course one has to give a precise meaning to the word „small” in this context.

Roughly speaking we shall call a coefficient of the power series of an entire function $f(z)$ „small” if it is smaller in absolute value than the corresponding coefficient of the power series of an other entire function $g(z)$ which is of smaller order of magnitude than $f(z)$. To make this definition quite definite, we have to decide how to compare the orders of magnitude of the entire functions $f(z)$ and $g(z)$. This could be done for example by comparing the rate of increase for $r \rightarrow \infty$ of the maximum modulus $M_f(r) = \max_{|z|=r} |f(z)|$ of $f(z)$ with that of $g(z)$, i. e. with $M_g(r) = \max_{|z|=r} |g(z)|$.

¹ The theorem remains valid if we consider the power series of $f(z)$ around two arbitrary different points α and β .

For our purposes it is however more convenient to compare the orders of magnitude of $f(z)$ and $g(z)$ by comparing the maximal terms of their power series. We shall prove the following

THEOREM 1. Let $f(z) = \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} b_n (z-1)^n$ be a transcendental entire function and $g(z) = \sum_{n=0}^{\infty} c_n z^n$ be an arbitrary entire function. Put

$$\mu_f(r) = \max_n |a_n| r^n$$

and

$$\mu_g(r) = \max_n |c_n| r^n.$$

Let us suppose that there exists a number δ such that $0 < \delta < 1$ and

$$(1.1) \quad \liminf_{r \rightarrow \infty} \frac{\mu_g(r^{1/\delta})}{\mu_f(r)} < \infty.$$

Let $S_0(n)$ denote the number of indices $k < n$ for which $|a_k| \leq |c_k|$ and $S_1(n)$ the number of indices $k < n$ for which $|b_k| \leq |c_k|$. Then we have²

$$(1.2) \quad \liminf_{n \rightarrow \infty} \frac{S_0(n) + S_1(n)}{n} \leq 1 + 2\delta.$$

Let us make some remarks.

REMARK 1. If we choose $g(z) \equiv 0$, then (1.1) holds for any $\delta > 0$, further in this case $S_0(n) = Z_0(n)$ and $S_1(n) = Z_1(n)$, where $Z_0(n)$ resp. $Z_1(n)$ denote the number of zeros in the sequence $a_0, a_1, \dots, a_{n-1}$ resp. $b_0, b_1, \dots, b_{n-1}$. Thus in this special case Theorem 1 reduces to Theorem A, i. e. Theorem 1 is a generalization of Theorem A.

REMARK 2. If $f(z)$ is an entire function of order ρ_f and $g(z)$ an entire function of order ρ_g , then according to a well known theorem (see e. g. [2], Chapter IV. Problem 51)

$$\limsup_{r \rightarrow \infty} \frac{\log \log \mu_f(r)}{\log r} = \rho_f$$

and similarly

$$(1.3) \quad \limsup_{r \rightarrow \infty} \frac{\log \log \mu_g(r)}{\log r} = \rho_g.$$

Thus if $\rho_g < \rho_f$ and we choose a sequence r_k ($k = 1, 2, \dots$) such that $\lim_{k \rightarrow \infty} r_k = \infty$

and $\lim_{k \rightarrow \infty} \frac{\log \log \mu_f(r_k)}{\log r_k} = \rho_f$ then we have for any δ with $\delta > \frac{\rho_g}{\rho_f}$

$$\lim_{k \rightarrow \infty} \frac{\mu_g(r_k^{1/\delta})}{\mu_f(r_k)} = 0.$$

² Clearly only the case $\delta < \frac{1}{2}$ is interesting as otherwise (1.2) is trivial.

It follows that the conditions of Theorem 1 hold with any δ for which $\delta > \frac{\varrho_g}{\varrho_f}$ and thus we obtain

$$(1.4) \quad \liminf_{n \rightarrow \infty} \frac{S_0(n) + S_1(n)}{n} \leq 1 + 2 \frac{\varrho_g}{\varrho_f}.$$

In case $\varrho_g = 0$ and $\varrho_f > 0$ further also in case $\varrho_f = \infty$ and $\varrho_g < \infty$ it follows

$$\liminf_{n \rightarrow \infty} \frac{S_0(n) + S_1(n)}{n} \leq 1.$$

We shall show later (Theorem 4) that (1.4) can be improved, namely the factor 2 on the right hand side of (1.4) is unnecessary.

Of course, Theorem 1 can also be applied to certain pairs of entire functions which are either both of order 0 or both of order ∞ .

REMARK 3. Clearly instead of considering the power series of $f(z)$ about $z=0$ and $z=1$ we could consider its power series about $z=\alpha$ and $z=\beta$ where α and β are arbitrary complex numbers and $\alpha \neq \beta$. As a matter of fact in this case we have to apply Theorem 1 to the function $f[(\beta-\alpha)z+\alpha]$ instead of $f(z)$ and $g[(\beta-\alpha)z]$ instead of $g(z)$.

§ 2 contains estimations of certain interpolatory polynomials. In § 3 we give the proof of Theorem 1, further of the related Theorems 2, 3 and 4. The method of proof of Theorem 1 is the same as that of Theorem A given in [1] but besides the tools used there, the results of § 2 are also needed. § 4 contains the discussion of an example, which shows that our results are not far from being best possible.

§ 2. Estimates of certain interpolatory polynomials

Let $Q_n(z)$ ($n=1, 2, \dots$) be the unique polynomial of degree $2n-1$ which satisfies the following conditions:

$$(2.1) \quad \frac{Q_n^{(j)}(0)}{j!} = p_j \quad \text{for} \quad j = 0, 1, \dots, n-1$$

and

$$(2.2) \quad \frac{Q_n^{(j)}(1)}{j!} = q_j \quad \text{for} \quad j = 0, 1, \dots, n-1$$

where p_j and q_j ($j=0, 1, \dots, n-1$) are arbitrary complex numbers. An explicit formula for $Q_n(z)$ has been given by P. JOHANSEN [3]; this can be written as follows:

$$(2.3) \quad \begin{aligned} Q_n(z) = & (1-z)^n \sum_{k=0}^{n-1} z^k \left[\sum_{s=0}^k p_{k-s} \binom{n+s-1}{s} \right] + \\ & + z^n \sum_{k=0}^{n-1} (z-1)^k \left[\sum_{s=0}^k (-1)^s q_{k-s} \binom{n+s-1}{s} \right]. \end{aligned}$$

Formula (2.3) can be transformed as follows:

$$(2.4) \quad Q_n(z) = \sum_{m=0}^{2n-1} z^m \left\{ \sum_{k=0}^{n-1} \binom{n}{m-k} (-1)^{m-k} \left[\sum_{s=0}^k p_{k-s} \binom{n+s-1}{s} \right] \right\} + \\ + \sum_{t=0}^{n-1} z^{n+t} \left\{ \sum_{k=t}^{n-1} \binom{k}{t} (-1)^{k-t} \left[\sum_{s=0}^k (-1)^s q_{k-s} \binom{n+s-1}{s} \right] \right\}.$$

Thus we obtain

$$\frac{Q_n^{(n)}(z)}{n!} = \sum_{t=0}^{n-1} z^t \binom{n+t}{n} Q_{n,t}$$

where

$$Q_{n,t} = (-1)^n \sum_{k=t}^{n-1} \binom{n}{n+t-k} (-1)^{k-t} \left[\sum_{s=0}^k p_{k-s} \binom{n+s-1}{s} \right] + \\ + \sum_{k=t}^{n-1} \binom{k}{t} (-1)^{k-t} \left[\sum_{s=0}^k (-1)^s q_{k-s} \binom{n+s-1}{s} \right].$$

Now evidently

$$|Q_{n,t}| \leq \left(\max_{0 \leq u \leq n-1} |p_u| \right) \sum_{k=t}^{n-1} \binom{n}{n+t-k} \left[\sum_{s=0}^k \binom{n+s-1}{s} \right] + \\ + \left(\max_{0 \leq v \leq n-1} |q_v| \right) \sum_{k=t}^{n-1} \binom{k}{t} \left[\sum_{s=0}^k \binom{n+s-1}{s} \right].$$

As however

$$\sum_{s=0}^k \binom{n+s-1}{s} = \binom{n+k}{k} < 2^{n+k}$$

we obtain

$$\sum_{k=t}^{n-1} \binom{n}{n+t-k} \left[\sum_{s=0}^k \binom{n+s-1}{s} \right] < 2^{n+t} \cdot 3^n < 12^n$$

further

$$\sum_{k=t}^{n-1} \binom{k}{t} \left[\sum_{s=0}^k \binom{n+s-1}{s} \right] < 8^n.$$

Thus we obtain

$$|Q_{n,t}| < 12^n \left(\max_{0 \leq u \leq n-1} |p_u| + \max_{0 \leq v \leq n-1} |q_v| \right) \quad \text{for } t = 0, 1, \dots, n-1.$$

Thus we have proved the following

LEMMA 1. Let $Q_n(z)$ ($n=1, 2, \dots$) be the unique polynomial of degree $2n-1$ determined by the conditions (2.1) and (2.2). Then we have

$$\max_{|z|=e} \frac{|Q_n^{(n)}(z)|}{n!} < 12^n \left(\max_{0 \leq u \leq n-1} |p_u| + \max_{0 \leq v \leq n-1} |q_v| \right) \sum_{t=0}^{n-1} \binom{n+t}{n} e^t.$$

§ 3. Proof of Theorems 1–4

We can suppose without the restriction of generality, that $f(z)$ is real for real z , i. e. that all the coefficients a_n (and thus all the b_n) are real. As a matter of fact suppose that Theorem 1 is already proved for such functions. If $f(z) = \sum_{n=0}^{\infty} a_n z^n$ is an arbitrary entire function, put $f_1(z) = \sum_{n=0}^{\infty} a'_n z^n$ resp. $f_2(z) = \sum_{n=0}^{\infty} a''_n z^n$ where a'_n and a''_n denotes the real and imaginary part of a_n respectively ($n=0, 1, \dots$). Clearly

$$\mu_f(r) \leq \mu_{f_1}(r) + \mu_{f_2}(r)$$

thus if $f(z)$ satisfies (1.1), at least one of the functions $f_1(z)$ and $f_2(z)$ satisfies it too. Suppose e. g. that $f_1(z)$ satisfies (1.1) i. e.

$$\liminf_{r \rightarrow \infty} \frac{\mu_g(r^{1/\delta})}{\mu_{f_1}(r)} < \infty.$$

Put $f(z) = \sum_{n=0}^{\infty} b_n (z-1)^n$, further $b_n = b'_n + ib''_n$; now if $|a_n| \leq |c_n|$ then $|a'_n| \leq |c_n|$, and similarly if $|b_n| \leq |c_n|$ then $|b'_n| \leq |c_n|$. Thus if $S'_0(n)$ resp. $S'_1(n)$ denotes the number of indices $k < n$ for which $|a'_k| \leq |c_k|$ resp. $|b'_k| \leq |c_k|$ then $S_0(n) \leq S'_0(n)$ and $S_1(n) \leq S'_1(n)$. As by supposition the statement of Theorem 1 is valid for $f_1(z)$, it follows that it is valid for $f(z)$ too. Therefore in what follows we shall suppose that $f(z)$ is real on the real axis, i. e. that the coefficients a_n and b_n are all real numbers.

To prove Theorem 1 we shall need the following Lemma A, which has been used in proving Theorem A in [1].

LEMMA A. *If $h(x)$ is a real function which has n continuous derivatives in the closed interval $[0, 1]$ and if $N(n)$ denotes the number of zeros of $h^{(n)}(x)$ in the interval $[0, 1]$ further $Z_0(n, h)$ and $Z_1(n, h)$ denotes the number of zeros in the sequence $h(0), h'(0), \dots, h^{(n-1)}(0)$ and in the sequence $h(1), h'(1), \dots, h^{(n-1)}(1)$ respectively, then we have*

$$Z_0(n, h) + Z_1(n, h) - n \leq N(n).$$

We shall apply Lemma A to the function

$$(3.1) \quad h_n(z) = f(z) - Q_n(z) \quad (n = 1, 2, \dots)$$

where $Q_n(z)$ is the unique polynomial of order $2n-1$ defined by the following conditions:

$$(3.2a) \quad \frac{Q_n^{(j)}(0)}{j!} = \begin{cases} 0 & \text{for } 0 \leq j < \delta'n \\ a_j & \text{if } \delta'n \leq j \leq n-1 \text{ and } |a_j| \leq |c_j| \\ 0 & \text{if } \delta'n \leq j \leq n-1 \text{ and } |a_j| > |c_j| \end{cases}$$

$$(3.2b) \quad \frac{Q_n^{(j)}(1)}{j!} = \begin{cases} 0 & \text{for } 0 \leq j < \delta'n \\ b_j & \text{if } \delta'n \leq j \leq n-1 \text{ and } |b_j| \leq |c_j| \\ 0 & \text{if } \delta'n \leq j \leq n-1 \text{ and } |b_j| > |c_j|. \end{cases}$$

Here δ' is an arbitrary number such that $\delta < \delta' < 1$.

Clearly if $h_n(z)$ is defined by (3.1) and $Q_n(z)$ by (3.2a-b) we have

$$(3.3) \quad S_0(n) \leq Z_0(n, h_n) + \delta' n$$

and

$$(3.4) \quad S_1(n) \leq Z_1(n, h_n) + \delta' n.$$

Thus it follows by Lemma A that denoting by $N_n(n)$ the number of zeros of $h_n^{(n)}(z)$ in the interval $[0, 1]$, we have

$$(3.5) \quad S_0(n) + S_1(n) \leq N_n(n) + n(1 + 2\delta').$$

Now we shall need Jensen's theorem which we shall use in the following form (see [4], p. 127, formula (13)):

LEMMA B. Let $H(z)$ be an analytic function which is regular in a circle $|z| \leq R$ ($R > 1$) and $H(0) \neq 0$. Let $\mathcal{N}_0$ denote the number of zeros of $H(z)$ in the (closed) unit circle, and choose a number ϱ with $1 < \varrho < R$. Then

$$(3.6) \quad \mathcal{N}_0 \leq \frac{\max_{|z|=\varrho} \log \left| \frac{H(z)}{H(0)} \right|}{\log \varrho}.$$

It follows from (3.5) and (3.6) that if $h_n^{(n)}(0) \neq 0$, then for any $\varrho > 1$ we have

$$(3.7) \quad \frac{S_0(n) + S_1(n)}{n} \leq \frac{\max_{|z|=\varrho} \log \left| \frac{h_n^{(n)}(z)}{h_n^{(n)}(0)} \right|}{n \log \varrho} + (1 + 2\delta').$$

Now let us choose a sequence r_s of positive numbers, such that $\lim_{s \rightarrow \infty} r_s = \infty$ and

$$\lim_{s \rightarrow \infty} \frac{\mu_g \left(r_s^{\frac{1}{\delta}} \right)}{\mu_f(r_s)} = G < \infty.$$

Such a sequence r_s exists by supposition. Let n_s denote the index of the maximal term of the series $\sum_{n=0}^{\infty} a_n z^n$ for $|z| = r_s$, i. e. suppose

$$(3.8) \quad |a_{n_s}| r_s^{n_s} \geq |a_m| r_s^m \quad \text{for} \quad m = 0, 1, \dots$$

It follows by Lemma 1 that

$$(3.9) \quad \left| \frac{Q_{n_s}^{(n_s)}(0)}{f^{(n_s)}(0)} \right| \leq \frac{2 \max_{t \approx \delta' n_s} |c_t|}{|a_{n_s}|} 12^{n_s} \leq C_1 (12 \lambda_{n_s})^{n_s}$$

where $C_1 > 0$ is a constant and

$$\lambda_{n_s} = \frac{1}{r_s^{\frac{\delta' - \delta}{\delta}}}.$$

As clearly

$$(3.10) \quad \lim_{s \rightarrow \infty} \lambda_{n_s} = 0$$

it follows that

$$(3.11) \quad \lim_{s \rightarrow \infty} \left| \frac{Q_{n_s}^{(n_s)}(0)}{f^{(n_s)}(0)} \right| = 0$$

and thus also $h_{n_s}^{(n_s)}(0) \neq 0$ for sufficiently large s .

By Lemma 1 we have also for $|z| = \varrho > 1$

$$\left| \frac{Q_{n_s}^{(n_s)}(z)}{f^{(n_s)}(0)} \right| \leq \frac{2 \left(\max_{t \geq \delta' n} |c_t| \right) 12^{n_s} \sum_{j=0}^{n_s-1} \binom{n_s+j}{j} \varrho^j}{|a_{n_s}|}$$

Similarly as in (3.9) we obtain

$$\max_{|z|=\varrho} \left| \frac{Q_{n_s}^{(n_s)}(z)}{f^{(n_s)}(0)} \right| \leq C_2 (12\lambda_{n_s}\varrho)^{n_s} \sum_{j=0}^{n_s-1} \binom{n_s+j}{j} \varrho^j.$$

where $C_2 > 0$ is a constant.

Now if s is sufficiently large, we have $12\lambda_{n_s}\varrho < 1$ and therefore

$$\max_{|z|=\varrho} \left| \frac{Q_{n_s}^{(n_s)}(z)}{f^{(n_s)}(0)} \right| \leq \frac{C_2}{(1 - 12\lambda_{n_s}\varrho)^{n_s+1}}.$$

It follows by (3.10) that

$$(3.12) \quad \lim_{s \rightarrow \infty} \frac{\max_{|z|=\varrho} \log \left| \frac{Q_{n_s}^{(n_s)}(z)}{f^{(n_s)}(0)} \right|}{n_s} = 0.$$

Finally we have for $|z| = \varrho$ by (3.8)

$$\left| \frac{f^{(n_s)}(z)}{f^{(n_s)}(0)} \right| \leq \sum_{l=0}^{\infty} \left| \frac{a_{n_s+l}}{a_{n_s}} \right| \binom{n_s+l}{l} \varrho^l \leq \frac{1}{\left(1 - \frac{\varrho}{r_s}\right)^{n_s+1}}$$

and thus

$$(3.13) \quad \lim_{s \rightarrow \infty} \frac{\max_{|z|=\varrho} \log \left| \frac{f^{(n_s)}(z)}{f^{(n_s)}(0)} \right|}{n_s} = 0.$$

As we have evidently

$$(3.14) \quad \max_{|z|=\varrho} \left| \frac{h_{n_s}^{(n_s)}(z)}{h_{n_s}^{(n_s)}(0)} \right| \leq \frac{\max_{|z|=\varrho} \left| \frac{f^{(n_s)}(z)}{f^{(n_s)}(0)} \right| + \max_{|z|=\varrho} \left| \frac{Q_{n_s}^{(n_s)}(z)}{f^{(n_s)}(0)} \right|}{1 - \left| \frac{Q_{n_s}^{(n_s)}(0)}{f^{(n_s)}(0)} \right|}$$

comparing (3.11), (3.12), (3.13) and (3.14) it follows that

$$(3.15) \quad \lim_{s \rightarrow \infty} \frac{\max_{|z|=e} \log \left| \frac{h_{n_s}^{(n_s)}(z)}{h_{n_s}^{(n_s)}(0)} \right|}{n_s} = 0.$$

Combining (3.7) with (3.15) we obtain

$$(3.16) \quad \limsup_{s \rightarrow \infty} \frac{S_0(n_s) + S_1(n_s)}{n_s} \leq 1 + 2\delta'$$

and as (3.16) holds for any $\delta' > \delta$, we obtain finally

$$\liminf_{s \rightarrow \infty} \frac{S_0(n) + S_1(n)}{n} \leq 1 + 2\delta.$$

Thus Theorem 1 is proved.

Now we prove the following

THEOREM 2. Let $f(z) = \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} b_n (z-1)^n$ be a transcendental entire function and $g(z) = \sum_{n=0}^{\infty} c_n z^n$ an arbitrary entire function for which the suppositions of Theorem 1 hold. Let $Z_0(n)$ denote the number of zeros in the sequence $a_0, a_1, \dots, a_{n-1}$ and $S_1(n)$ the number of indices $k < n$ for which $|b_k| \leq |c_k|$. Then

$$\liminf_{n \rightarrow \infty} \frac{Z_0(n) + S_1(n)}{n} \leq 1 + \delta.$$

The proof of Theorem 2 is almost the same as that of Theorem 1; as however we do not use now (3.3), only (3.4), we get δ instead of 2δ .

The following result contains each of Theorem 1 and Theorem 2 as special cases.

THEOREM 3. Let $f(z) = \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} b_n (z-1)^n$ be a transcendental entire function, further $g_1(z) = \sum_{n=0}^{\infty} c_n z^n$ and $g_2(z) = \sum_{n=0}^{\infty} d_n z^n$ be entire functions, such that putting

$$\mu_{g_1}(r) = \max_n |c_n| r^n$$

and

$$\mu_{g_2}(r) = \max_n |d_n| r^n$$

we have for some δ_1 and δ_2 ($\delta_1 > 0$, $\delta_2 > 0$, $\delta_1 + \delta_2 < 1$)

$$\liminf_{r \rightarrow \infty} \frac{\mu_{g_1}(r^{1/\delta_1}) + \mu_{g_2}(r^{1/\delta_2})}{\mu_f(r)} < \infty.$$

Let $S_0(n)$ denote the number of indices $k < n$ for which $|a_k| \leq |c_k|$ and $S_1(n)$ the number of indices $k < n$ for which $|b_k| \leq |c_k|$. Then

$$\liminf_{n \rightarrow \infty} \frac{S_0(n) + S_1(n)}{n} \leq 1 + \delta_1 + \delta_2.$$

The proof of Theorem 3 is essentially the same as that of Theorem 1; the only differences consist in that now we define the polynomial $Q_n(z)$ of order $2n-1$ ($n=1, 2, \dots$) as follows:

$$\frac{Q_n^{(j)}(0)}{j!} = \begin{cases} 0 & \text{for } 0 \leq j < \delta'_1 n \\ a_j & \text{if } \delta'_1 n \leq j \leq n-1 \text{ and } |a_j| \leq |c_j| \\ 0 & \text{if } \delta'_1 n \leq j \leq n-1 \text{ and } |a_j| > |c_j| \end{cases}$$

$$\frac{Q_n^{(j)}(1)}{j!} = \begin{cases} 0 & \text{for } 0 \leq j < \delta'_2 n \\ b_j & \text{if } \delta'_2 n \leq j \leq n-1 \text{ and } |b_j| \leq |d_j| \\ 0 & \text{if } \delta'_2 n \leq j \leq n-1 \text{ and } |b_j| > |d_j|. \end{cases}$$

Here δ_1 is an arbitrary number for which $\delta_1 < \delta'_1 < 1$ and δ'_2 an arbitrary number for which $\delta_2 < \delta'_2 < 1$.

Evidently if we choose $g_1(z) = g_2(z) = g(z)$, then Theorem 3 reduces to Theorem 1, while if $g_1(z) \equiv 0, g_2(z) = g(z)$, then Theorem 3 reduces to Theorem 2.

Now we shall prove the following Theorem 4, which gives a sharper inequality than (1.4).

THEOREM 4. If $f(z) = \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} b_n (z-1)^n$ is an entire function of order ρ_f ($0 < \rho_f \leq \infty$) and $g(z) = \sum_{n=0}^{\infty} c_n z^n$ an entire function of order ρ_g where $0 \leq \rho_g < \rho_f$, and if $S_0(n)$ denotes the number of indices $k < n$ for which $|a_k| \leq |c_k|$ and $S_1(n)$ the number of indices $k < n$ for which $|b_k| \leq |c_k|$ then

$$\liminf_{n \rightarrow \infty} \frac{S_0(n) + S_1(n)}{n} \leq 1 + \frac{\rho_g}{\rho_f}.$$

PROOF OF THEOREM 4. Let us put

$$\varphi(z) = \sum_{|a_n| \leq |c_n|} a_n z^n$$

and

$$f^*(z) = f(z) - \varphi(z) = \sum_{|a_n| > |c_n|} a_n z^n = \sum_{n=0}^{\infty} a_n^* z^n = \sum_{n=0}^{\infty} b_n^* (z-1)^n.$$

Then clearly $f^*(z)$ has the same order ρ_f as $f(z)$ further $\varphi(z)$ is at most of order ρ_g . Let $Z_0^*(n)$ denote the number of zeros in the sequence $a_0^*, a_1^*, \dots, a_{n-1}^*$, then clearly

$$(3.17) \quad Z_0^*(n) = S_0(n)$$

We can without restricting the generality suppose that $c_n \geq 0$ as evidently $\sum_{n=0}^{\infty} |c_n| z^n$ is an entire function of the same order as $g(z)$ [This follows e. g. by (1.3)]. Put

$$g^*(z) = 2 \sum_{n=0}^{\infty} z^n \left[\sum_{m=n}^{\infty} \binom{m}{n} c_m \right] = \sum_{n=0}^{\infty} c_n^* z^n.$$

It is easy to see that $g^*(z)$ is also an entire function of order ϱ_g . As a matter of fact, one has

$$g^*(z) = 2g(z+1).$$

Now as

$$f^*(z) = \sum_{n=0}^{\infty} \left[b_n - \sum_{\substack{m=n \\ |a_m| \leq |c_m|}}^{\infty} \binom{m}{n} a_m \right] (z-1)^n$$

we obtain

$$|b_k^*| \leq |b_k| + \sum_{m=k}^{\infty} \binom{m}{k} c_k \quad (k = 0, 1, \dots).$$

Thus if $|b_k| \leq |c_k|$ we have $|b_k^*| \leq |c_k^*|$. It follows that if $S_1^*(n)$ denotes the number of indices $k < n$ for which $|b_k^*| \leq |c_k^*|$, then

$$(3.18) \quad S_1(n) \leq S_1^*(n).$$

Now we can apply Theorem 2 to the function $f^*(z)$ of order ϱ_f and the function $g^*(z)$ of order ϱ_g with any $\delta > \frac{\varrho_g}{\varrho_f}$ and thus we obtain, taking (3.17) and (3.18) into account

$$\liminf_{n \rightarrow \infty} \frac{S_0(n) + S_1(n)}{n} \leq \liminf_{n \rightarrow \infty} \frac{Z_0^*(n) + S_1^*(n)}{n} \leq 1 + \frac{\varrho_g}{\varrho_f}$$

Thus Theorem 4 is proved.

§ 4. An example

We shall discuss now an example, which shows that Theorem 4 is in a certain sense best possible.

Let us consider the function

$$f(z) = \sum_{n=0}^{\infty} \frac{z^{a^n}}{(a^n)!}$$

where $a > 1$ is an integer. Clearly $f(z)$ is an entire transcendental function of order 1. Let us choose for $g(z)$ the function

$$g(z) = \sum_{n=0}^{\infty} \frac{z^n}{(n!)^{1/\vartheta}}$$

where $\frac{1}{a} < \vartheta < 1$. It is easy to see that $g(z)$ is an entire function of order ϑ .

We consider now the power series of $f(z)$ around the point $z = 1$; we have

$$f(z) = \sum_{n=0}^{\infty} \frac{[1 + (z-1)]^{a^n}}{(a^n)!} = \sum_{m=0}^{\infty} b_m (z-1)^m$$

where

$$b_m = \frac{1}{m!} \sum_{a^n \geq m} \frac{1}{(a^n - m)!}.$$

Let us compare now b_m with

$$c_m = \frac{1}{(m!)^{1/\vartheta}}$$

for a value of m which lies in the interval

$$a^{n-1} \leq m < \frac{a^n \vartheta}{1 + \varepsilon} \quad (n = 1, 2, \dots)$$

where ε is an arbitrary positive number.

We have clearly for any m satisfying (4.1)

$$b_m \leq \frac{2}{m! \left[\left(\frac{1 + \varepsilon}{\vartheta} - 1 \right) m \right]}.$$

It follows by *Stirling's* formula that if $n \geq n_0$ where n_0 is a suitably chosen large number and if m satisfies (4.1) we have

$$b_m \leq c_m.$$

It follows that

$$(4.2) \quad \liminf_{n \rightarrow \infty} \frac{S_0(n) + S_1(n)}{n} \geq 1 + \frac{\frac{\vartheta}{1 + \varepsilon} - \frac{1}{a}}{1 - \frac{1}{a}}.$$

As for ε we can choose an arbitrary small positive number and a can be chosen arbitrarily large, it follows that the lower bound in (4.2) can be arbitrarily near to $1 + \vartheta$. As however by Theorem 4

$$(4.3) \quad \liminf_{n \rightarrow \infty} \frac{S_0(n) + S_1(n)}{n} \leq 1 + \vartheta$$

it follows that Theorem 4 (and thus also Theorem 2) is best possible in the sense that $1 + \vartheta$ can not be replaced in general by any smaller number in (4.3).

Literature

- [1] C. RÉNYI, On a conjecture of G. Pólya, *Acta Math. Acad. Sci. Hung.*, **7** (1956), 145 – 150.
- [2] G. PÓLYA und G. SZEGŐ, *Aufgaben und Lehrsätze aus der Analysis*, Vol. 2., Berlin, Springer 1925.
- [3] P. JOHANSEN, Über osculierende Interpolation, *Skandinavisk Aktuarietidskrift*, 1931.
- [4] P. ERDŐS and A. RÉNYI, On the number of zeros of successive derivatives of analytic functions, *Acta Math. Acad. Sci. Hung.*, **7** (1956), 125 – 144.

ON TWO PROBLEMS OF INFORMATION THEORY

by

PAUL ERDŐS and ALFRÉD RÉNYI

§ 1. Introduction

The first problem¹ which will be discussed in this paper can be formulated as follows: Suppose we are given n coins, which look quite alike, but of which some are false. (For instance suppose that the right coins consist of gold, while the false coins consist mainly of silver and are covered only by a thin layer of gold.) The false coins have a smaller weight than the right coins; the weights a and $b < a$ of both the right and false coins are known. A scale is given by means of which any number $\leq n$ of coins can be weighed together. Thus if we select an arbitrary subset of the coins and put them together on the scale, then the scale shows us the total weight of these coins, from which it is easy to compute the number of false coins among those weighed. The question is what is the minimal number $A(n)$ of weighings by means of which the right and false coins can be separated? It can be seen by an elementary information-theoretical argument that (denoting by $\log_2 x$ the logarithm with base 2 of x)

$$(1.1) \quad A(n) \geq \frac{n}{\log_2(n+1)}.$$

As a matter of fact, the amount of information needed is $\log_2 2^n = n$ bits, because the subset of the coins consisting of the false coins may be any of the 2^n subsets of the set of all n coins; on the other hand if we put $k \leq n$ coins on the balance, the number of false coins among them may have the values $0, 1, \dots, k$ and thus the amount of information given by each weighing can not exceed $\log_2(k+1) \leq \log_2(n+1)$. Thus s weighings can give us at most $s \log_2(n+1)$ bits, and thus to get the necessary amount of information (that is n bits) it is necessary that $s \log_2(n+1)$ should be not less than n ; thus we obtain (1.1). On the other hand, a trivial upper estimate is

$$(1.2) \quad A(n) \leq n$$

because if we put the coins one by one after another on the scale then clearly these n weighings are sufficient. The inequality (1.2) is best possible for $n = 1, 2$ and 3 , but already for $n = 4$ we have $A(4) = 3$. As a matter of fact

¹ This problem was proposed for $n = 5$ by H.S. SHAPIRO [1] and for arbitrary n by N.J. FINE [2].

if we label the 4 coins by the numbers 1, 2, 3, 4 then the following 3 weighings are always sufficient: we put first the coins 1, 2, 3 on the scale, then the coins 1, 3, 4 and finally the coins 1, 2 and 4. Let the number of false coins among the coins 1, 2, 3 be f_1 , that among 1, 3, 4 be f_2 and that among 1, 2, 4 be f_3 . The following table gives us the false coins:

f_1	f_2	f_3	1	2	3	4
0	0	0	—	—	—	—
1	1	1	+	—	—	—
1	0	1	—	+	—	—
1	1	0	—	—	+	—
0	1	1	—	—	—	+
2	1	2	+	+	—	—
2	2	1	+	—	+	—
1	2	2	+	—	—	+
2	1	1	—	+	+	—
1	1	2	—	+	—	+
1	2	1	—	—	+	+
3	2	2	+	+	+	—
2	2	3	+	+	—	+
2	3	2	+	—	+	+
2	2	2	—	+	+	+
3	3	3	+	+	+	+

Note that among the possible 64 triples f_1, f_2, f_3 ($0 \leq f_j \leq 3$, $j = 1, 2, 3$) only 16 are possible and each corresponds to a different distribution of the false coins.

It is easy to see that in general one has

$$(1.3) \quad A(nm) \leq A(n) \cdot m$$

(because if we have nm coins we may determine by $A(n)$ weighings from each group of n coins the false ones). Thus from the above example one gets

$$A(4n) \leq 3n$$

and as $A(n)$ is evidently monotonic, we obtain

$$(1.4) \quad A(n) \leq \left\lceil \frac{3n}{4} \right\rceil + 2$$

where $\{x\}$ stands for the least integer $\geq x$

It may be guessed² from this that one has

$$(1.5) \quad \lim_{n \rightarrow +\infty} \frac{A(n)}{n} = 0.$$

This is in fact true; moreover we shall prove in § 1 that the lower estimate (1.1) gives the correct order of magnitude of $A(n)$. We shall prove namely in § 2 (Theorem 1) that for any $\delta > 0$ we have for $n \geq n_0(\delta)$

$$(1.6) \quad A(n) \leq (1 + \delta) \frac{n \cdot \log_2 9}{\log_2 n}$$

It remains an open question whether the limit

$$(1.7) \quad \lim_{n \rightarrow +\infty} \frac{A(n) \log_2 n}{n} = \alpha$$

exists, and if it exists, what is its value? We shall prove in § 4 (Theorem 3) that

$$(1.8) \quad \liminf_{n \rightarrow +\infty} \frac{A(n) \log_2 n}{n} \geq 2.$$

It follows from (1.8) that if the limit α in (1.7) exists one has $2 \leq \alpha \leq \log_2 9 \approx 3.17$. We shall prove in § 5 that if the problem is modified so that we are contented with finding a method of weighing which leads to the separation of the false coins with a prescribed probability $p < 1$ which may be arbitrarily near to 1, (supposing that all the 2^n possibilities have same probability) then $\frac{2n}{\log_2 n} (1 + \varepsilon)$ weighings are sufficient for any $\varepsilon > 0$ if n is large (Theorem 4).

Let us return now to the original problem of determining $A(n)$. This problem may be formulated as follows: We have to guess an unknown sequence of n digits, each digit being equal to 0 or 1. We have the right to select arbitrary „testing” sequences of zeros and ones of length n and with respect of each such sequence we are told what is the number of places in which a 1 stands both in the sequence to be guessed and in our testing sequence. The minimal number of testing sequences by means of which the unknown sequence can be uniquely determined whatever it may be, is equal to $A(n)$.

This reformulation of our first problem shows its connection with the second problem which will be discussed in this paper and which is as follows: Suppose we want to guess an unknown sequence of n digits, each digit being either 0 or 1. Information concerning the unknown sequence may be obtained in the following way: We have the right to select arbitrarily „testing” sequences of digits consisting of zeros and ones and we are told the number of places in which the two sequences coincide. Let $B(n)$ denote the minimal number of sequences by means of which we can determine the unknown sequence, whatever it may be. The problem is to determine the asymptotic behaviour of $B(n)$. Clearly we have

$$(1.9) \quad B(n) \geq \frac{n}{\log_2 (n + 1)}.$$

² This conjecture was stated in [2].

The inequality (1.9) is obtained by a similar information-theoretical argument as that which leads us to (1.1). We have here the same trivial upper estimate

$$(1.10) \quad B(n) \leq n.$$

As a matter of fact, if we select the n testing sequences $11 \dots 1$, $011 \dots 1$, $1011 \dots 1$, $\dots$, $111 \dots 101$ then if k is the number of places in which the sequence $11 \dots 1$ and the unknown sequence coincide, then the number of coincidences between the sequence $011 \dots 1$ with the unknown sequence is either $k - 1$ or $k + 1$ according to whether the first digit of the unknown sequence is 1 or 0. Thus by the 2nd, 3rd, $\dots$, n -th testing sequences we can determine the first $n - 1$ digits of the unknown sequence; the last one can be determined because the total number k of ones in the unknown sequence is known from the first comparison. We have clearly $B(n) = n$ for $n = 1, 2, 3, 4$ and $B(5) = 4$ as can be seen from the following example: using the testing sequences

11111

11100

01010

01101

we can guess any sequence of 5 zero-or-one digits. As a matter of fact we get for the number of coincidences the following values for the 16 sequences consisting of not more than two ones:

sequence	coincidence with			
	11111	11100	01010	01101
00000	0	2	3	2
00001	1	1	2	3
00010	1	1	4	1
00100	1	3	2	3
01000	1	3	4	3
10000	1	3	2	1
00011	2	0	3	2
00101	2	2	1	4
01001	2	2	3	4
10001	2	2	1	2
00110	2	2	3	2
01010	2	2	5	2
10010	2	2	3	0
01100	2	4	3	4
10100	2	4	1	2
11000	2	4	3	2

It is unnecessary to try the other 16 sequences with 3 or more ones, because these are obtained by replacing 1 by 0 and 0 by 1 in the above 16 sequences, and this changes the number of coincidences from x to $5 - x$.

We shall prove for $B(n)$ the same inequality as obtained for $A(n)$; viz. we obtain in § 3 (Theorem 2) for any $\delta > 0$ that for $n \geq n_1(\delta)$

$$(1.11) \quad B(n) \leq (1 + \delta) \frac{n \log_2 9}{\log_2 n}.$$

Here again the question remains open whether the limit

$$(1.12) \quad \lim_{n \rightarrow +\infty} \frac{B(n) \log_2 n}{n} = \beta$$

exists, and if so what its value is. We shall show in § 4 (Theorem 5) by the same method which we have used to prove Theorem 3 that

$$(1.13) \quad \liminf_{n \rightarrow +\infty} \frac{B(n) \log_2 n}{n} \geq 2.$$

Thus if the limit β in (1.12) exists, then certainly $2 \leq \beta \leq \log_2 9 \approx 3.17$. We shall prove also in § 5 that if we modify our second problem so that we want to determine a fixed but unknown sequence of n zero-or-one digits by the number of coincidences with certain testing sequences and we are contented with finding it with probability $p < 1$ which may be arbitrarily near to 1 then $\frac{2n}{\log_2 n} (1 + \varepsilon)$ testing sequences are sufficient, (Theorem 6), for any $\varepsilon > 0$ if n is large enough.

Finally let us mention the following geometric interpretation of both problems. To any sequence of zeros and ones there corresponds a vertex of the unit cube C_n of n -dimensional space. The function $B(n)$ can be interpreted as follows: $B(n)$ denotes the least number such that by selecting $B(n)$ suitable chosen vertices of C_n each vertex of C_n is uniquely determined by its distances from the chosen $B(n)$ vertices.

Now let us interpret any sequence of n zeros and ones as a vector of the n -dimensional space leading from the origin to one of the vertices of C_n . With this interpretation $A(n)$ denotes the least number such that by selecting $A(n)$ vectors $v_1, v_2, \dots, v_{A(n)}$ leading to suitably chosen vertices of C_n each vector v leading to a vertex of C_n is uniquely determined by its projection on the $A(n)$ chosen vectors, i. e. by the $A(n)$ numbers $(v, v_1), \dots, (v, v_{A(n)})$ where (v, w) denotes the inner product of the vectors v and w .

We prove our Theorems 1 and 2 by the same method, consisting in a random selection of the testing sequences.

§ 2. An upper estimate for $A(n)$

Our first problem can be formulated as follows: What is the least value $A(n)$ of s such that there exists a matrix M having s rows and n columns and consisting of zeros and ones, such that if we select an arbitrary subset e of the set E of the columns of M , and form the row-sums of the submatrix $M(e)$ consisting of the selected columns of M , and denote by v_e the column-vector consisting of these row-sums, then the vectors v_e and $v_{e'}$ are different if e and e' are different subsets of E . We shall call such a matrix an A -matrix.

Thus $A(n)$ is the least value of s such that there exists an A -matrix with n columns and s rows. Clearly the matrix corresponding to the example given in the introduction for $n = 4$ is the A -matrix

$$(2.1) \quad \begin{array}{cccc} 1110 \\ 1011 \\ 1101 \end{array}$$

The $2^4 = 16$ possible column-vectors v_e are in this case

$$\begin{array}{cccccccccccccccc} 0 & 1 & 1 & 1 & 0 & 2 & 2 & 1 & 2 & 1 & 1 & 2 & 2 & 2 & 3 & 3 \\ 0 & 1 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 3 & 2 & 2 & 3 \\ 0 & 1 & 1 & 0 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 2 & 3 & 2 & 3 \end{array}$$

and all are different, thus the matrix (2.1) is in fact an A -matrix.

In order to estimate $A(n)$ we shall prove that if we choose M at random so that the sn elements of M are independent random variables, each taking on the values 0 and 1 with probability $\frac{1}{2}$, then the random matrix M will have the required property with positive probability (in fact with probability tending to 1 for $n \rightarrow +\infty$) provided that $s > (1 + \delta) \frac{n \log_2 9}{\log_2 n}$.

This can be proved as follows: Let $\mathbf{P}_{s,n}(A)$ denote the probability that a random matrix M of order $s \times n$ is an A -matrix, and put $\mathbf{Q}_{s,n}(A) = 1 - \mathbf{P}_{s,n}(A)$. Let $A(e_1, e_2)$ (where e_1 and e_2 are different subsets of the set E of columns of M) denote the event that the row-sum vectors v_{e_1} and v_{e_2} are identical. Evidently if $v_{e_1} = v_{e_2}$ and the sets e_1 and e_2 are not disjoint, then putting $e'_1 = e_1 - e_1 e_2$ and $e'_2 = e_2 - e_1 e_2$, we have $v_{e'_1} = v_{e'_2}$. (Here and in what follows the product of sets denotes their intersection and the difference $e - f$ of two sets e and f denotes the set of elements of e which do not belong to f). It follows that if M is not an A -matrix, then there exist disjoint subsets e_1 and e_2 of the set of its columns such that $v_{e_1} = v_{e_2}$. Thus we obtain that

$$(2.2) \quad \mathbf{Q}_{s,n}(A) \leq \sum_{e_1, e_2 = \emptyset} \mathbf{P}(A(e_1, e_2))$$

where the summation has to be extended over every pair of disjoint subsets e_1 and e_2 of the set E of the columns of M and $\emptyset$ denotes the empty set.

It follows that

$$(2.3) \quad \mathbf{Q}_{s,n}(A) \leq \sum_{1 \leq k_1 + k_2 \leq n} \frac{n!}{k_1! k_2! (n - k_1 - k_2)!} \left(\frac{\sum_{l=0}^{\min(k_1, k_2)} \binom{k_1}{l} \binom{k_2}{l}}{2^{k_1 + k_2}} \right)^s$$

By the well known identity

$$\sum_{l=0}^{\min(k_1, k_2)} \binom{k_1}{l} \binom{k_2}{l} = \binom{k_1 + k_2}{k_1}$$

we obtain

$$\mathbf{Q}_{s,n}(A) \leq \sum_{1 \leq k_1 + k_2 \leq n} \frac{n!}{k_1! k_2! (n - k_1 - k_2)!} \left(\frac{\binom{k_1 + k_2}{k_1}}{2^{k_1 + k_2}} \right)^s.$$

It follows

$$(2.4) \quad Q_{s,n}(A) \leq \sum_{r=1}^n \binom{n}{r} \sum_{k=0}^r \frac{\binom{r}{k}^{s+1}}{2^{rs}}.$$

As

$$(2.5) \quad \binom{r}{k} \leq \binom{\left\lfloor \frac{r}{2} \right\rfloor}{\left\lfloor \frac{r}{2} \right\rfloor} \quad (k = 0, 1, \dots, r)$$

further $\binom{\left\lfloor \frac{r}{2} \right\rfloor}{\left\lfloor \frac{r}{2} \right\rfloor} \leq \frac{2^r}{\sqrt{r+1}}$ for $r = 3, 4, \dots$ (this follows easily by induction) we obtain

$$(2.6) \quad Q_{s,n}(A) \leq \frac{4n^2}{2^s} + \sum_{r=3}^n \binom{n}{r} \frac{2^r}{(r+1)^{\frac{s}{2}}}.$$

Now we choose $s \sim \frac{\alpha n}{\log_2 n}$. As we have

$$\sum_{r \leq \frac{n}{\log_2^2 n}} \binom{n}{r} 2^r = O(2^{c \frac{n \log \log n}{\log^2 n}})$$

where $c > 0$ is a constant, it follows that

$$(2.7) \quad Q_{s,n}(A) \leq \sum_{r > \frac{n}{\log_2^2 n}} \binom{n}{r} \frac{2^r}{(r+1)^{\frac{s}{2}}} + o(1).$$

Taking into account that $\sum_{r=0}^n \binom{n}{r} 2^r = 3^n$, we obtain

$$(2.8) \quad Q_{s,n}(A) \leq 2^{n(\log_2 3 - \frac{\alpha}{2}) + o(n)}$$

provided that $s = s(n) \sim \frac{\alpha n}{\log_2 n}$ where $\alpha > 2 \log_2 3 = \log_2 9$. It follows

$$(2.9) \quad \lim_{n \rightarrow +\infty} Q_{s(n),n}(A) = 0.$$

Now clearly if $Q_{s(n),n}(A) < 1$ then $P_{s(n),n}(A) > 0$; as $P_{s,n}(A)$ is the probability that the random matrix M is an A -matrix, it follows that if $\delta > 0$ and $s > \frac{n \log_2 9}{\log_2 n}$ then for $n \geq n_0(\delta)$ there exists an A -matrix of order $s \times n$ which implies $A(n) \leq s$. Thus we proved the following

Theorem 1. For any $\delta > 0$ we have for $n \geq n_0(\delta)$

$$(2.10) \quad A(n) \leq (1 + \delta) \frac{n \log_2 9}{\log_2 n}.$$

§ 3. An upper estimate for $B(n)$

Let $u = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$ and $u' = (\varepsilon'_1, \varepsilon'_2, \dots, \varepsilon'_n)$ be row-vectors consisting of n components, each of which is either 0 or 1. Let us put $c(u, u') = n - \sum_{i=1}^n (\varepsilon_i - \varepsilon'_i)^2$. Thus $c(u, u')$ is the number of „coincidences” of the vectors u and u' , i.e. the number of columns of the $2 \times n$ matrix $\begin{pmatrix} \varepsilon_1 & \dots & \varepsilon_n \\ \varepsilon'_1 & \dots & \varepsilon'_n \end{pmatrix}$ which consist of equal elements. By the usual notation $\|u\|^2 = \sum_{i=1}^n \varepsilon_i^2$ we have

$$(3.1) \quad c(u, u') = n - \|u - u'\|^2.$$

Let now M be a matrix having s rows and n columns, and consisting of elements 0 and 1. Let $u_1, \dots, u_s$ be the rows of M interpreted as vectors. Let u be an arbitrary row-vector consisting of n components which are either 0 or 1. Let U denote the set consisting of all 2^n such vectors u . To any u there corresponds a vector W_u consisting of the numbers $c(u, u_1), \dots, c(u, u_s)$. The matrix M will be called a B -matrix if the 2^n vectors W_u corresponding to different elements u of U are all different from each other. Thus if M is a B -matrix, then each vector $u \in U$ is uniquely determined by the s numbers $c(u, u_1), \dots, c(u, u_s)$ (and thus also by the distances $\|u - u_j\|$, $j = 1, 2, \dots, s$). Let $P_{s,n}(B)$ denote the probability that the random matrix M of order $s \times n$ (whose elements are independent random variables each taking on the values 0 and 1 with probability $\frac{1}{2}$) should be a B -matrix, and put $Q_{s,n}(B) = 1 - P_{s,n}(B)$.

Let $u = (\varepsilon_1, \dots, \varepsilon_n)$ and $u' = (\varepsilon'_1, \dots, \varepsilon'_n)$ be two arbitrary different row-vectors consisting of n components each of which is either 0 or 1. Let H and $\bar{H}$ denote the set of those indices k ($1 \leq k \leq n$) for which $\varepsilon_k = 1$ and $\varepsilon_k = 0$, respectively and similarly let H' and $\bar{H}'$ denote the set of those indices k ($1 \leq k \leq n$) for which $\varepsilon'_k = 1$ and $\varepsilon'_k = 0$ respectively. Let k_1, k_2, k_3 and k_4 denote the number of elements of the sets HH' , $H\bar{H}'$, $\bar{H}H'$ and $\bar{H}\bar{H}'$ respectively. Let $u_j = (\vartheta_{j1}, \dots, \vartheta_{jn})$ be the j -th row of the random matrix M and let l_{j1}, l_{j2}, l_{j3} and l_{j4} denote the number of those indices k which belong to the sets HH' , $H\bar{H}'$, $\bar{H}H'$ and $\bar{H}\bar{H}'$ respectively and for which $\vartheta_{jk} = 1$. Clearly we have $c(u, u_j) = c(u', u_j)$ if and only if

$$l_{j1} + l_{j2} + k_3 - l_{j3} + k_4 - l_{j4} = l_{j1} + l_{j3} + k_2 - l_{j2} + k_4 - l_{j4}$$

that is if

$$(3.2) \quad 2(l_{j2} - l_{j3}) = k_2 - k_3.$$

It follows that a necessary condition for $c(u, u_j) = c(u', u_j)$ is that $k_2 - k_3$ should be even, and further that

$$(3.3) \quad Q_{s,n}(B) \leq \sum_{\substack{k_2 + k_3 \equiv 0 \pmod{2} \\ 1 \leq k_2 + k_3 \leq n}} \frac{n!}{k_2! k_3! (n - k_2 - k_3)!} \left(\frac{\sum_{l=0}^{\frac{k_2 + k_3}{2}} \binom{k_2}{l} \binom{k_3}{l - \frac{k_2 - k_3}{2}}}{2^{k_2 + k_3}} \right)^s.$$

Now

$$\sum_{l=0}^{\frac{k_2+k_3}{2}} \binom{k_2}{l} \binom{l}{l - \frac{k_2 - k_3}{2}} = \binom{k_2 + k_3}{\frac{k_2 + k_3}{2}}$$

and thus

$$(3.4) \quad Q_{s,n}(B) \leq \sum_{r=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n}{2r} 2^{2r} \left(\frac{\binom{2r}{r}}{2^{2r}} \right)^s.$$

It follows similarly as in § 2 that if $s = s(n) \sim a \frac{n}{\log_2 n}$ where $a > \log_2 9$ then

$$(3.5) \quad \lim_{n \rightarrow +\infty} Q_{s(n),n}(B) = 0.$$

Clearly if $Q_{s(n),n}(B) < 1$ then $P_{s(n),n}(B) > 0$ and thus there exists a B -matrix of order $s(n) \times n$ and therefore $B(n) \leq s(n)$. Thus we have proved the following

Theorem 2. For any $\delta > 0$ and $n \geq n_1(\delta)$ one has

$$(3.6) \quad B(n) \leq (1 + \delta) \frac{n \log_2 9}{\log_2 n}.$$

§ 4. Lower bounds for $A(n)$ and $B(n)$

In this § we prove the following results

Theorem 3. One has

$$(4.1) \quad \liminf_{n \rightarrow +\infty} \frac{A(n) \log_2 n}{n} \geq 2.$$

Theorem 4. One has

$$(4.2) \quad \liminf_{n \rightarrow +\infty} \frac{B(n) \log_2 n}{n} \geq 2.$$

Proof of Theorem 3. Let M be now an arbitrary A -matrix of order $s \times n$. Let us divide the row-vectors of M in two classes. A row-vector u of M belongs to the first class if it contains less than h elements equal to 1, where $h = \sqrt{n \log n}$; otherwise it belongs to the second class. We shall give first an upper estimate for the number of different column-vectors v_e consisting of the row-sums of the submatrix $M(e)$ of M consisting of the columns of M belonging to the set e ; here e is an arbitrary subset of the set E of columns of M . Clearly any component of v_e corresponding to a row belonging to the first class may take on at most h different values. On the other hand if a row u_j of M belongs to the second class, and contains m ones ($m \geq h$) then the number of possible choices of the subset e of the columns for which the sum of the elements of the row u_j standing in the selected columns does not lie between the bounds $\frac{m}{2} \pm \lambda \sqrt{m \log m}$ (where the positive constant λ will be chosen later) is equal to

$$(4.3) \quad 2^{n-m} \sum_{\left| k - \frac{m}{2} \right| > \lambda \sqrt{m \log m}} \binom{m}{k}.$$

According to the Moivre—Laplace theorem we have

$$(4.4) \quad \sum_{\left|k - \frac{m}{2}\right| > \lambda \sqrt{m \log m}} \binom{m}{k} = O\left(\frac{2^m}{m^{2\lambda^2}}\right).$$

Let us call a subset e of the set E of columns a „bad” subset, if there exists a row u_j belonging to the second class and containing m ones, for which the sum of the elements of u_j standing in the columns belonging to e lies outside the bounds $\frac{m}{2} \pm \lambda \sqrt{m \log m}$. Otherwise we call e a „good” subset. Clearly by

(4.4) if N denotes the number of bad subsets we have

$$(4.5) \quad N = O\left(\frac{n 2^n}{h^{2\lambda^2}}\right) = O\left(\frac{2^n}{n^{(\lambda^2-1)} (\log n)^{\lambda^2}}\right).$$

Thus if $\lambda^2 \geq 1$ we have

$$(4.6) \quad N = O\left(\frac{2^n}{\log n}\right).$$

On the other hand, denoting by V the number of different values of the vector v_e if e runs over the good subsets, we have

$$(4.7) \quad V \leq h^x [2\lambda \sqrt{n \log n}]^{s-x} \leq (2\lambda \sqrt{n \log n})^s.$$

As M is by supposition an A -matrix, the inequality

$$(4.8) \quad V \geq 2^n - N$$

has to be valid, which implies by (4.6) and (4.7)

$$(4.9) \quad (2\lambda \sqrt{n \log n})^s \geq 2^n \left(1 - O\left(\frac{1}{\log n}\right)\right).$$

Thus we obtain that the inequality

$$(4.10) \quad s \geq \frac{2n}{\log_2 n + O(\log \log n)}$$

holds, from which Theorem 3 immediately follows.

Proof of Theorem 4. Theorem 4 can be proved in a similar way as we proved Theorem 3. The only difference is that the distinction between rows of the first and second class is now unnecessary. Let M be a B -matrix of order $s \times n$. Let U denote again the set of all possible rows of n elements each of which is equal either to 0 or to 1. Let $u_1, u_2, \dots, u_s$ denote the rows of the matrix M . An element u of U will be called „bad” if there is a row u_j of M such that the number of coincidences $c(u, u_j)$ of u and u_j , does not lie in the interval $\frac{n}{2} \pm \lambda \sqrt{n \log n}$; otherwise u will be called „good”. If N denotes the number of „bad” elements u of U we have by Chebyshev’s inequality

$$(4.11) \quad N = O\left(\frac{2^n}{\log n}\right).$$

On the other hand if W denotes the number of possible values of the vector $w_u = (c(u, u_1), \dots, c(u, u_s))$ where u runs over the „good” elements of U , we have

$$(4.12) \quad W \leq (2 \sqrt{n \log n})^s.$$

As M is a B -matrix, we have

$$(4.13) \quad W \geq 2^n - N.$$

Thus it follows from (4.11) and (4.12) that

$$(4.14) \quad s \geq \frac{2n}{\log_2 n + O(\log \log n)}$$

which proves Theorem 4.

§ 5. Discussion of a modified form of both problems

Let U denote again the set of all possible sequences of length n consisting of zeros and ones. Let M denote again a matrix of order $s \times n$ consisting of zeros and ones; let $u_1, \dots, u_s$ denote the rows of M . Let (u, u') where $u \in U$, $u' \in U$ denote the inner product of the vectors u and u' , i.e. the number of places in which 1 stands both in u and u' . Let $c(u, u') = n - \|u - u'\|^2$ denote the number of coincidences of the vectors u and u' , i.e. the number of places in which the same number stands both in u and u' . A matrix M will be called a p - A matrix (resp. a p - B matrix) where $0 < p < 1$ if by choosing at random an element u of U (so that each of the 2^n elements of U has the same probability to be chosen) the probability that u is uniquely determined by the sequence of numbers $(u, u_1), (u, u_2), \dots, (u, u_s)$ (resp. by the sequence $c(u, u_1), c(u, u_2), \dots, c(u, u_s)$) exceeds p . Let $s_A(n, p)$ and $s_B(n, p)$ respectively denote the minimal value of s for which a p - A matrix resp. a p - B matrix M of order $s \times n$ exists. Then the following results hold:

Theorem 5. For any fixed p with $0 < p < 1$ one has

$$(5.1) \quad \lim_{n \rightarrow +\infty} \frac{s_A(n, p)}{\left(\frac{2n}{\log_2 n} \right)} = 1.$$

Theorem 6. For any fixed p with $0 < p < 1$ one has

$$(5.2) \quad \lim_{n \rightarrow +\infty} \frac{s_B(n, p)}{\left(\frac{2n}{\log_2 n} \right)} = 1.$$

Proof of Theorems 5 and 6. Let M denote the set of all $s \times n$ matrices the elements of which are zeros and ones. Let $P_A(M)$ and $P_B(M)$ resp. denote the probability that by choosing at random an element u of U this element should be uniquely determined by the sequence $(u, u_1), (u, u_2), \dots, (u, u_s)$ resp. by the sequence $c(u, u_1), c(u, u_2), \dots, c(u, u_s)$ where $u_1, \dots, u_s$ denote the rows of the

matrix M . Clearly the assertions that $s_A(n, p) \leq s$ and $s_B(n, p) \leq s$ resp. are equivalent to the assertions that

$$(5.3) \quad \max_{M \in \mathfrak{M}} \mathbf{P}_A(M) \geq p$$

and

$$(5.4) \quad \max_{M \in \mathfrak{M}} \mathbf{P}_B(M) \geq p.$$

Evidently if $\overline{\mathbf{P}_A(M)}$ and $\overline{\mathbf{P}_B(M)}$ denote the mean value of $\mathbf{P}_A(M)$ and $\mathbf{P}_B(M)$ when M is chosen at random so that M may be equal to any element of $\mathfrak{M}$ with the same probability $\frac{1}{2^{sn}}$, then

$$(5.5) \quad \max_{M \in \mathfrak{M}} \mathbf{P}_A(M) \geq \overline{\mathbf{P}_A(M)}$$

and

$$(5.6) \quad \max_{M \in \mathfrak{M}} \mathbf{P}_B(M) \geq \overline{\mathbf{P}_B(M)}.$$

Thus if we prove that for a certain value of s we have

$$\overline{\mathbf{P}_A(M)} \geq p$$

and

$$\overline{\mathbf{P}_B(M)} \geq p,$$

it follows that the inequalities $s_A(n, p) \leq s$ and $s_B(n, p) \leq s$ hold.

Let $A(u, M)$ denote the event that the row vector $u \in U$ is uniquely determined by the sequence $(u, u_1), \dots, (u, u_s)$ and $B(u, M)$ the event that the row vector $u \in U$ is uniquely determined by the sequence $c(u, u_1), \dots, c(u, u_s)$ where $u_1, \dots, u_s$ denote the rows of M . Then evidently

$$(5.7) \quad \overline{\mathbf{P}_A(M)} = \mathbf{P}(A(u, M))$$

and

$$(5.8) \quad \overline{\mathbf{P}_B(M)} = \mathbf{P}(B(u, M))$$

where on the right hand side of (5.7) and (5.8) u is a randomly chosen element of U and M a randomly chosen element of $\mathfrak{M}$. Let us put

$$(5.9) \quad 1 - \mathbf{P}(A(u, M)) = \mathbf{Q}_A(s, n)$$

and

$$(5.10) \quad 1 - \mathbf{P}(B(u, M)) = \mathbf{Q}_B(s, n).$$

We obtain by a similar argument as that used in § 2 and § 3 resp.

$$(5.11) \quad \mathbf{Q}_A(s, n) \leq \sum_{k=0}^n \binom{n}{k} \frac{1}{2^n} \sum_{i+j>0} \binom{k}{i} \binom{n-k}{j} \left[\frac{\binom{i+j}{i}}{2^{i+j}} \right]^s$$

and

$$(5.12) \quad \mathbf{Q}_B(s, n) \leq \sum_{k=0}^n \binom{n}{k} \frac{1}{2^n} \sum_{\substack{i=j \bmod 2 \\ i+j>0}} \binom{k}{i} \binom{n-k}{j} \left[\frac{\binom{i+j}{2}}{2^{i+j}} \right]^s.$$

and therefore

$$\mathbf{Q}_A(s, n) \leq \left(\sum_{k=0}^n \binom{n}{k} \frac{1}{2^n} \right) \sum_{l=1}^n \binom{n}{l} \sum_{i=0}^l \left[\frac{\binom{l}{i}}{2^i} \right]^s$$

and

$$\mathbf{Q}_B(s, n) \leq \left(\sum_{k=0}^n \binom{n}{k} \frac{1}{2^n} \right) \sum_{l=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2l} \left[\frac{\binom{2l}{l}}{2^{2l}} \right]^s.$$

Using again the inequalities $\binom{l}{i} \leq \binom{l}{\lfloor \frac{l}{2} \rfloor} \leq \frac{2^l}{\sqrt{l+1}}$

it follows that

$$(5.13) \quad \mathbf{Q}_A(s, n) \leq \sum_{l=1}^n \frac{\binom{n}{l}}{(l+1)^{s/2-1}}$$

and

$$(5.14) \quad \mathbf{Q}_B(s, n) \leq \sum_{l=1}^{\lfloor \frac{n}{2} \rfloor} \frac{\binom{n}{2l}}{(2l+1)^{s/2}}.$$

Thus if $s \sim \frac{\alpha n}{\log_2 n}$ we obtain

$$(5.15) \quad \mathbf{Q}_A(s, n) \leq 2^{n(1-\frac{\alpha}{2}) + O\left(\frac{n \log \log n}{\log n}\right)}$$

and similarly

$$(5.16) \quad \mathbf{Q}_B(s, n) \leq 2^{n(1-\frac{\alpha}{2}) + O\left(\frac{n \log \log n}{\log n}\right)}.$$

Thus if $\alpha > 2$ we have

$$(5.17) \quad \lim_{n \rightarrow +\infty} \mathbf{Q}_A(s, n) = \lim_{n \rightarrow +\infty} \mathbf{Q}_B(s, n) = 0.$$

By (5.9) and (5.10) this implies

$$(5.18) \quad \lim_{n \rightarrow +\infty} \mathbf{P}(A(u, M)) = \lim_{n \rightarrow +\infty} \mathbf{P}(B(u, M)) = 1$$

and thus by (5.5)—(5.8) it follows

$$(5.19) \quad \lim_{n \rightarrow +\infty} \max_{M \in \mathcal{M}} \mathbf{P}_A(M) = \lim_{n \rightarrow +\infty} \max_{M \in \mathcal{M}} \mathbf{P}_B(M) = 1.$$

As mentioned above this proves Theorems 5 and 6.

REFERENCES

- [1] SHAPIRO, H. S.: „Problem E 1399.” *American Mathematical Monthly* **67** (1960) p. 82.
- [2] FINE, N. I.: „Solution of problem E 1399.” *American Mathematical Monthly* **67** (1960) p. 697.

Remark, added on september 24, 1963

Since the present paper was given to print, we have been informed that quite a number of mathematicians worked on the first problem of the present paper, and obtained results which are closely related to our results. None of these results are published but some of them are in print. As W. MOSER informed us, D. G. CANTOR has proved in a paper in print in the *Canadian Journal of Mathematics* the relation (1.5); in fact he obtained the estimate $A(n) = O\left(\frac{n \log \log n}{\log n}\right)$. L. MOSER (University of Alberta, Edmonton) informed us that, he obtained together with ABBOT, that

$$(*) \quad \limsup_{n \rightarrow +\infty} \frac{A(n) \log_2 n}{n} \leq \log_2 27.$$

While this upper bound is greater by the factor $3/2$ than our bound $\log_2 9$, the method of proof applied by ABBOTT and L. MOSER has the advantage that it is constructive; they exhibit effectively A -matrices of size $s \times n$ where $s \sim \frac{n \log_2 27}{\log_2 n}$.

The same result has been obtained by H. S. SHAPIRO and S. SÖDERBERG. Their paper is in print in the *American Mathematical Monthly*. E. R. BERLEKAMP (Bell Telephone Laboratories) has obtained by a method, essentially the same as our method, that

$$A(n) \leq \frac{n \log_2 9}{\log_2 n}.$$

This result is slightly better than our result (1.6) (by the factor $1 + \delta$). To get rid of the unnecessary factor $(1 + \delta)$ one has to use instead of the rough estimate (2.5) a sharper estimate following from Stirling's formula.

BERLEKAMP conjectured also that (1.8) holds, and gave a heuristic argument for his conjecture.

Other proofs of (1.8) have been given by B. GORDON (University of California, Los Angeles) and L. MOSER. E. MILLS has also proved that $A(n) = O\left(\frac{n}{\log n}\right)$. Quite recently B. LINDSTRÖM (University of Stockholm)

has proved the conjecture (1.7) with $\alpha = 2$. His paper will be printed in the next issue of this journal.

ON RANDOM MATRICES

by

P. ERDŐS and A. RÉNYI

Introduction

In the present paper we deal with certain random 0 — 1 matrices. Let $\mathcal{M}(n, N)$ denote the set of all n by n square matrices among the elements of which there are exactly N elements ($n \leq N \leq n^2$) equal to 1, all the other elements are equal to 0. The set $\mathcal{M}(n, N)$ contains clearly $\binom{n^2}{N}$ such matrices; we consider a matrix M chosen at random from the set $\mathcal{M}(n, N)$, so that each element of $\mathcal{M}(n, N)$ has the same probability $\binom{n^2}{N}^{-1}$ to be chosen. We ask now how large N has to be, for a given large value of n , in order that the permanent of the random matrix M should be different from zero with probability $\geq \alpha$ where $0 < \alpha < 1$. By other words if $M = (\varepsilon_{jk})$ we want to evaluate asymptotically the probability $P(n, N)$ of the event that there exists at least one permutation $j_1, j_2, \dots, j_n$ of the numbers $1, 2, \dots, n$ such that the product $\varepsilon_{1j_1} \varepsilon_{2j_2} \dots \varepsilon_{nj_n}$ should be equal to 1. A second way to formulate the problem is as follows: we shall say that two elements of a matrix are in independent position if they are not in the same row and not in the same column. Now our question is to determine the probability that the random matrix M should contain n elements which are all equal to 1 and are pairwise in independent position. A third way to state the problem is: what is the probability of the event that the permanent of the random 0 — 1 matrix M should be positive?

We prove in § 1 (Theorem 1) that if

$$(1) \quad N(n) = n \log n + cn + o(n)$$

where c is an arbitrary real constant, then

$$(2) \quad \lim_{n \rightarrow +\infty} P(n, N(n)) = e^{-2e^{-c}}.$$

This implies that if

$$(3) \quad \lim_{n \rightarrow +\infty} \frac{N_1(n) - n \log n}{n} = +\infty,$$

then

$$(4) \quad \lim_{n \rightarrow +\infty} P(n, N_1(n)) = 1,$$

while if

$$(5) \quad \lim_{n \rightarrow +\infty} \frac{N_2(n) - n \log n}{n} = -\infty,$$

then

$$(6) \quad \lim_{n \rightarrow +\infty} P(n, N_2(n)) = 0.$$

This result can be interpreted also in the following way, in terms of graph theory. Let $\Gamma_{n,N}$ be a bichromatic random graph containing n red and n blue vertices, and N edges which are chosen at random among the n^2 possible edges connecting two vertices having different colour (so that each of the $\binom{n^2}{N}$ possible choices has the same probability). Then $P(n, N)$ is equal

to the probability that the random graph $\Gamma_{n,N}$ should contain a factor of degree 1, i.e. $\Gamma_{n,N}$ should have a subgraph which contains all vertices of $\Gamma_{n,N}$ and n disjoint edges, i.e. n edges which have no common endpoint.

Clearly if the permanent of a matrix M consisting of zeros and ones is positive, then the matrix M does not contain a row or column all elements of which are equal to 0 (called in what follows for the sake of brevity a 0-row resp. 0-column), but conversely, if M does not contain a 0-row, nor a 0-column, it is not sure that its permanent is different from 0. However, from our result it follows that this is "almost" sure. As a matter of fact, Theorem 1 can be interpreted as follows: if $P(n, N)$ denotes the probability that $\text{perm}(M) > 0$ and $Q(n, N)$ the probability that M does not contain a 0-row or a 0-column, then if $N = N(n)$ is chosen so that for $n \rightarrow \infty$ we should have $Q(n, N(n)) \rightarrow 1$, then we have also $P(n, N(n)) \rightarrow 1$.

One can state this result somewhat vaguely also in the following way: if the permanent of a random matrix with elements 0 and 1 is equal to 0, then under the conditions of Theorem 1 this in most cases is due to the presence of a 0-row or a 0-column.

In § 2 we deal with a somewhat simpler variant of the problem, when the elements ε_{ij} ($1 \leq i \leq n$, $1 \leq j \leq n$) of the matrix M are *independent* random variables each taking on the values 0 and 1 with probability $1 - p$ and p respectively. The results obtained are analogous to those of § 1. In § 3 we add some remarks and mention some unsolved problems.

Besides elementary combinatorial and probabilistic arguments similar to that used by us in our previous work on random graphs (see [1], [2], [3], [4], [5]) our main tool in proving our results is the well-known theorem of D. KÖNIG (see [6]), which is nowadays well known in the theory of linear programming, according to which if M is an n by n matrix, every element of which is either 0 or 1, then the minimal number of lines (i.e. rows or columns) which contain all the 1-s, is equal to the maximal number of 1-s in independent position. As a matter of fact, for our purposes we need only the special case of this theorem, proved already by G. FROBENIUS [7], concerning the case when the maximal number of ones in independent position is equal to n .

§ 1. Random square matrices with a prescribed number of zeros and ones

Let $P(n, N)$ denote the probability of the event that the random matrix M ($M \in \mathcal{M}(n, N)$) has a positive permanent. According to the theorem of FROBENIUS—KÖNIG (see [6] and [7]) $1 - P(n, N)$ is equal to the probability that there exists a number k such that there can be found k rows and $n - k - 1$

columns of M which contain all the ones ($0 \leq k \leq n-1$). If we denote by $Q_k(n, N)$ the probability that there can be found k rows and $n-k-1$ columns or k columns and $n-k-1$ rows which contain all the ones, and k is the least number with this property, then clearly

$$(1.1) \quad 0 \leq 1 - P(n, N) = \sum_{k=0}^{\left[\frac{n-1}{2}\right]} Q_k(n, N).$$

Now we shall prove that if

$$(1.2) \quad N(n) = n \log n + cn + o(n)$$

where c is a real constant, then

$$(1.3) \quad \lim_{n \rightarrow \infty} \sum_{k=1}^{\left[\frac{n-1}{2}\right]} Q_k(n, N(n)) = 0,$$

further that

$$(1.4) \quad \lim_{n \rightarrow \infty} Q_0(n, N(n)) = 1 - e^{-2e^{-c}}.$$

Clearly (1.1), (1.3) and (1.4) imply that

$$(1.5) \quad \lim_{n \rightarrow \infty} P(n, N(n)) = e^{-2e^{-c}},$$

which is the result we want to prove. Thus it remains only to prove (1.3) and (1.4). Let us consider first (1.4). Clearly $1 - Q_0(n, N(n))$ is equal to the probability of the event that the random matrix M does not contain a 0-row or a 0-column. Thus we have

$$(1.6) \quad 1 - Q_0(n, N(n)) = \sum_{i=0}^{2n} (-1)^i S_i$$

where $S_0 = 1$ and

$$(1.7) \quad S_i = \sum_{h=0}^i \binom{n}{h} \binom{n}{i-h} \frac{\binom{(n-h)(n-i+h)}{N(n)}}{\binom{n^2}{N(n)}} \quad (i = 1, 2, \dots, 2n),$$

further for each $l \geq 0$

$$(1.8) \quad \sum_{i=0}^{2l+1} (-1)^i S_i \leq 1 - Q_0(n, N(n)) \leq \sum_{i=0}^{2l} (-1)^i S_i.$$

As clearly for each fixed value of i and for $n \rightarrow \infty$, if $N(n)$ is defined by (1.2) we have

$$(1.9) \quad S_i = \frac{2^i e^{-ci}}{i!} (1 + o(1)),$$

it follows that

$$(1.10) \quad \lim_{n \rightarrow \infty} (1 - Q_0(n, N(n))) = \sum_{i=0}^{\infty} (-1)^i \frac{2^i e^{-ci}}{i!} = e^{-2e^{-c}}.$$

Thus (1.4) is proved. Now let us prove (1.3).

Let us suppose that M is a matrix such that all the ones of M are contained in k columns and $n - k - 1$ rows ($k \geq 1$), and k is the least number with this property. Then the matrix M can be partitioned into four matrices A, B, C, D as shown by Fig. 1, so that D consists only of zeros. Then clearly each column of C contains at least two ones, because if a column of C would contain not more than a single 1, then by leaving out this column and adding the row in which this 1 is contained, we would get a system of $k - 1$ columns and $n - k$ rows which contain all the ones, in contradiction to our supposition of the minimum property of k .

$$\begin{array}{cc} & \begin{array}{c} \overbrace{\hspace{1cm}}^k \quad \overbrace{\hspace{1cm}}^{n-k} \end{array} \\ \begin{array}{c} n-k-1 \\ k+1 \end{array} \left\{ \begin{array}{|c|c|} \hline A & B \\ \hline C & D \\ \hline \end{array} \right. \end{array}$$

Fig. 1.

Thus it follows that

$$(1.11) \quad Q_k(n, N) \leq 2 \binom{n}{k} \binom{n}{k+1} \binom{k+1}{2}^k \frac{\binom{n(n-k-1) + k(k-1)}{N-2k}}{\binom{n^2}{N}}$$

and thus, that

$$(1.12) \quad Q_k(n, N(n)) \leq \left(\frac{A \log^2 n}{\sqrt{n}} \right)^k \quad \text{for } k = 1, 2, \dots, \left\lfloor \frac{n-1}{2} \right\rfloor$$

where A is a positive constant depending only on c . Thus we obtain

$$(1.13) \quad \sum_{k=1}^{\left\lfloor \frac{n-1}{2} \right\rfloor} Q_k(n, N(n)) \leq \frac{A \log^2 n}{\sqrt{n} - A \log^2 n}.$$

From (1.13) we obtain (1.3) and this completes the proof of (1.5).

Thus we obtained the following

Theorem 1. Let $\mathcal{M}(n, N)$ denote the set of all n by n square matrices, among the n^2 elements of which N are equal to 1 and the other $n^2 - N$ to 0. Let M be selected at random from the set $\mathcal{M}(n, N)$ so that each of the $\binom{n^2}{N}$ elements of the set $\mathcal{M}(n, N)$ has the same probability $\binom{n^2}{N}^{-1}$ to be selected. Let $P(n, N)$ denote

the probability of the event that the permanent of the random matrix M is positive. Then if

$$N(n) = n \log n + cn + o(n)$$

where c is any real constant, we have

$$\lim_{n \rightarrow \infty} P(n, N(n)) = e^{-2e^{-c}}.$$

§ 2. Random matrices with independent elements

In this § we prove the following theorem which is a variant of Theorem 1.

Theorem 2. Let $M_n(p)$ be a random n by n matrix whose elements ε_{ij} ($1 \leq i \leq n$; $1 \leq j \leq n$) are independent random variables such that

$$(2.1) \quad \mathbf{P}(\varepsilon_{ij} = 1) = p \quad \text{and} \quad \mathbf{P}(\varepsilon_{ij} = 0) = 1 - p.$$

Let $P_n(p)$ denote the probability of the event that the permanent of the random matrix $M_n(p)$ is positive. Then we have for

$$(2.2) \quad p_n = \frac{\log n + c}{n} + o\left(\frac{1}{n}\right)$$

$$(2.3) \quad \lim_{n \rightarrow \infty} P_n(p_n) = e^{-2e^{-c}}.$$

Proof of Theorem 2. The proof follows step by step the proof of Theorem 1. We have

$$(2.4) \quad 0 \leq 1 - P_n(p) \leq \sum_{k=0}^{\left[\frac{n-1}{2}\right]} Q_{k,n}(p)$$

where $Q_{k,n}(p)$ denotes the probability that there can be found k rows and $n - k - 1$ columns, or k columns and $n - k - 1$ rows of $M_n(p)$ which contain all the 1-s, and k is the least number with this property. In this case we have

$$(2.5) \quad 1 - Q_{0,n}(p) = \sum_{i=0}^{2n} (-1)^i S_i^*$$

where $S_0^* = 1$ and

$$(2.6) \quad S_i^* = \sum_{h=0}^i \binom{n}{h} \binom{n}{i-h} (1-p)^{in-h(i-h)}.$$

Thus we have for each fixed value of i if (2.2) holds

$$(2.7) \quad \lim_{n \rightarrow \infty} S_i^* = \frac{2^i e^{-ic}}{i!}$$

and therefore

$$(2.8) \quad \lim_{n \rightarrow \infty} (1 - Q_{0,n}(p_n)) = e^{-2e^{-c}}.$$

On the other hand we have now for $k = 1, 2, \dots, \left\lfloor \frac{n-1}{2} \right\rfloor$

$$(2.9) \quad Q_{k,n}(p) \leq 2 \binom{n}{k} \binom{n}{k+1} \binom{k+1}{2}^k p^{2k} (1-p)^{(k+1)(n-k)}$$

and thus

$$(2.10) \quad Q_{k,n}(p_n) \leq \left(\frac{B \log^2 n}{\sqrt{n}} \right)^k \quad \text{for } k = 1, 2, \dots, \left\lfloor \frac{n-1}{2} \right\rfloor,$$

where the constant B depends on c only.

Thus

$$(2.11) \quad \lim_{n \rightarrow \infty} \sum_{k=1}^n Q_{k,n}(p_n) = 0$$

and Theorem 2 follows.

§ 3. Some further remarks

The results of §§ 1 and 2 could be generalized for rectangular matrices of size m by n where $m < n$. In this case the question is: what is the probability that a random matrix of size m by n consisting of zeros and ones should contain m elements in independent position, which are all equal to 1?

Another possible generalization of our results would be to determine the probability distribution of the maximal number of ones in independent position in a random square matrix.

One may ask what can be said about the distribution of the *value* of the permanent of a random square matrix, under conditions of Theorems 1 and 2? It is easy to compute in both cases the mean value of the permanent $\text{perm}(M)$; we have evidently under conditions of Theorem 1

$$\mathbf{E}(\text{perm}(M)) = n! \frac{\binom{n^2 - n}{N(n) - n}}{\binom{n^2}{N(n)}}$$

and under conditions of Theorem 2

$$\mathbf{E}(\text{perm}(M_n(p_n))) = n! p_n^n.$$

It is easy to see, that these expressions are of the form $e^{n \log \log n + O(n)}$ and thus tend rather rapidly to $+\infty$. However one can not draw any conclusion from this fact, because as is easily seen, the variance of the permanent is still much larger than the square of the mean value. An interesting related problem is of course to evaluate under the conditions of Theorem 1 and 2 the probability of the determinant of the random matrix being different from 0.

Another problem arises in connection with the graph-theoretical interpretation of the questions discussed in the present paper: To compute the probability that a random graph having n vertices and N edges should contain a factor of the first degree? We hope to return to these problems in another paper.

(Received November 11, 1963)

REFERENCES

- [1] ERDŐS, P.—RÉNYI, A.: "On random graphs, I." *Publicationes Mathematicae (Debrecen)* **6** (1959) 290—297.
- [2] ERDŐS, P.—RÉNYI, A.: "On the evolution of random graphs." *Publ. of the Math. Inst. of the Hung. Acad. Sci.* **5** (1960) 17—61.
- [3] ERDŐS, P.—RÉNYI, A.: "On the evolution of random graphs." *International Stat. Inst.*, 32. Session, Tokyo, 1960, 119. 1—5.
- [4] ERDŐS, P.—RÉNYI, A.: "On the strength of connectedness of a random graph." *Acta Math. Acad. Sci. Hung.* **12** (1961) 261—267.
- [5] ERDŐS, P.—RÉNYI, A.: "Asymmetric graphs." *Acta Math. Acad. Sci. Hung.* (in print).
- [6] KÖNIG, D.: "Graphok és matrixok." *Matematikai és Fizikai Lapok* **38** (1931) 116—119.
- [7] FROBENIUS, G.: "Über zerlegbare Determinanten." *Sitzungsberichte der Berliner Akademie* 1917, S. 274—277.

AN ELEMENTARY INEQUALITY BETWEEN THE PROBABILITIES OF EVENTS

P. ERDÖS, J. NEVEU, A. RENYI

Introduction and summary.

For every positive integer n and any real number α in the open interval $(0, 1)$, let $\varepsilon_n(\alpha)$ be the least real number ε with the following property.

PROPERTY (P₁): *For any sequence $\{A_i, 1 \leq i \leq n\}$ of n events in an arbitrary probability space $(\Omega, \mathcal{A}, P)$ such that $P(A_i A_j) \leq \alpha^2$ for all i, j ($i \neq j$), the following inequality holds:*

$$(1) \quad \sum_{i=1}^n [P(A_i) - \alpha] \leq \varepsilon.$$

The exact value of the constant $\varepsilon_n(\alpha)$ is given in Section 2; however, the essential fact is that it tends to a finite limit as n goes to infinity. More precisely, it is found that $\varepsilon_n(\alpha) = \frac{1}{2}(1 - \alpha)$ provided $n\alpha$ or $(n - 1)\alpha$ is an integer (hence $\varepsilon_n(\frac{1}{2}) = \frac{1}{4}$ for every n) and that $\varepsilon_n(\alpha) = \frac{1}{2}(1 - \alpha) + O(n^{-1})$ for fixed α . It is also shown that it is possible to find, for every n and α , a sequence $\{A_i^*, 1 \leq i \leq n\}$ such that

$$P(A_i^*) = \alpha + \varepsilon_n(\alpha)/n, \quad P(A_i^* A_j^*) = \alpha^2 \quad (i \neq j);$$

for this sequence (1) is an equality. Such an extremal sequence is constructed in $[0, 1]$, for the case $\alpha = \frac{1}{2}$, $n \equiv 3 \pmod{4}$ by use of the method of quadratic residues; this example originated the present study.

After having completed this work, we became aware of a paper by S. Zubrzycki [2] which deals with the same problem in the special case when $P(A_i) = \omega_1$ for $i = 1, \dots, n$ and $P(A_i A_j) = \omega_2$ for $i \neq j$; the inequality which he obtains between ω_1 and ω_2 is essentially equivalent with our Corollary 1. Among the extremal cases where the inequality becomes an equality are those in which the $P(A_i)$ and the $P(A_i A_j)$ have the constant values mentioned above and already found by Zubrzycki. Despite the overlapping of the results and the similarity of the methods we have considered the publication of the present paper worth while not

Received March 22, 1963.

only because of the somewhat greater generality of our results but also because of the difference in point of view.

1.

In order to be able to calculate $\varepsilon_n(\alpha)$ easily, we shall first establish the following results.

THEOREM 1. *For every n and α , the constant $\varepsilon_n(\alpha)$ is also the least real number ε having the following property:*

PROPERTY (P_2): *For any random variable N defined on an arbitrary probability space $(\Omega, \mathcal{A}, P)$ and with values in the interval $\{0, 1, \dots, n\}$ of integers, such that $E[N(N-1)] \leq n(n-1)\alpha^2$, the following inequality holds:*

$$E(N) \leq n\alpha + \varepsilon.$$

PROOF. Suppose first that ε is a real number having property (P_2). Given a sequence $\{A_i, 1 \leq i \leq n\}$ of n events, let $N = \sum_{i=1}^n 1_{A_i}$, where 1_A denotes the indicator of A ; then N is a random variable taking its values in $\{0, 1, \dots, n\}$ and satisfying the relations

$$E[N] = \sum_i P(A_i), \quad E[N(N-1)] = \sum_{i \neq j} P(A_i A_j).$$

Hence if the sequence $\{A_i\}$ is such that

$$\sum_{i \neq j} P(A_i A_j) \leq n(n-1)\alpha^2,$$

and a fortiori, if $P(A_i A_j) \leq \alpha^2$ for every i, j ($i \neq j$), then by property (P_2)

$$\sum_1^n [P(A_i) - \alpha] = E[N] - n\alpha \leq \varepsilon.$$

This shows that ε has property (P_1).

Conversely, suppose that ε is a real number having property (P_1) and let $\{p_i, 0 \leq i \leq n\}$ be a probability law on the set $\{0, 1, \dots, n\}$. Then it is possible to construct a sequence $\{A_i, 1 \leq i \leq n\}$ of n events in a suitable probability space $(\Omega, \mathcal{A}, P)$ such that a) the random variable $N = \sum_{i=1}^n 1_{A_i}$ has $\{p_i, 0 \leq i \leq n\}$ for probability law; b) the sequence $\{A_i\}$ is symmetrically dependent, that is, $P(A_{i_1} \dots A_{i_e})$ depends only on the number e of different indices $i_1, \dots, i_e$. In order to construct such a sequence, let $\{A_i, 1 \leq i \leq n\}$ be a sequence of independent equiprobable events in a suitably chosen probability space $(\Omega, \mathcal{A}, Q)$ and define a new probability P on $(\Omega, \mathcal{A})$ by

$$P(A) = \sum_{k=0}^n p_k Q[A \mid N=k];$$

it is then obvious that $P[N=k]=p_k$; moreover $P[A_{i_1} \dots A_{i_e} \mid N=k]$ depends only on the number of different indices $i_1, \dots, i_e$, because $Q[A_{i_1} \dots A_{i_e} \mid N=k]$ has this property for every k .

If the given law $\{p_i\}$ is such that $\sum_k k(k-1)p_k \leq n(n-1)\alpha^2$, then the sequence $\{A_i\}$ constructed above is such that for every i_0, j_0 ($i_0 \neq j_0$)

$$\begin{aligned} P(A_{i_0} A_{j_0}) &= \frac{1}{n(n-1)} \sum_{i \neq j} P(A_i A_j) \\ &= \frac{1}{n(n-1)} \sum_{k=0}^n k(k-1)p_k \leq \alpha^2. \end{aligned}$$

Hence, by the property (P_1) of ε ,

$$\sum_k k p_k = \sum_i P(A_i) \leq n\alpha + \varepsilon_n(\alpha).$$

This shows that ε has property (P_2) and finishes the proof of the theorem.

COROLLARY 1. *For every n and α , the constant $\varepsilon_n(\alpha)$ is the least real number ε having the following property:*

PROPERTY (P_1') : *For any sequence $\{A_i, 1 \leq i \leq n\}$ of n events in an arbitrary probability space $(\Omega, \mathcal{A}, P)$ such that*

$$\frac{1}{n(n-1)} \sum_{i \neq j} P(A_i A_j) \leq \alpha^2,$$

the following inequality holds:

$$(1) \quad \sum_{i=1}^n [P(A_i) - \alpha] \leq \varepsilon.$$

PROOF. If a real number ε satisfies property (P_1') , it clearly satisfies (P_1) . The first part of the proof of the preceding theorem also shows that if an ε satisfies (P_2) , it satisfies (P_1') . The corollary then follows from the equivalence of (P_1) and (P_2) .

2.

In this section, we compute the supremum S of $E(N)$ when N varies in the class of random variables taking their values in the set $\{0, 1, \dots, n\}$ and such that $E[N(N-1)] \leq C$ for a given constant C . In virtue of Theorem 1 this will give us the constant $\varepsilon_n(\alpha)$ by letting $C = n(n-1)\alpha^2$ and $S = n + \varepsilon_n(\alpha)$.

Let ν be the unique positive integer and θ the unique real number in the semi-closed interval $[-1, 1[$ such that $C = \nu(\nu + \theta)$. Then $S = \nu + \frac{1}{2}(1 + \theta)$. Moreover the random variable N^* with probability law given by

$$p_\nu^* = \frac{1}{2}(1 - \theta), \quad p_{\nu+1}^* = \frac{1}{2}(1 + \theta), \quad p_m^* = 0 \text{ otherwise}$$

is such that $E(N^*) = S$, $E[N^*(N^* - 1)] = C$.

To prove this result, first let ν be the largest integer inferior or equal to S and let $\sigma = S - \nu$. Then notice that the supremum S of $E(N)$ when $E[N(N - 1)] \leq C$ may only be attained by random variables N with law concentrated on the two point set $\{\nu, \nu + 1\}$; for suppose that N gives this extremum and let λ (resp. μ) be the smallest (resp. largest) integral value taken by N with positive probability, then, if λ were strictly less than ν it would be possible to modify the law of N making p_λ and p_μ decrease and p_ν increase keeping $E[N(N - 1)]$ constant and thus, by the convexity of the function $x(x - 1)$, causing $E(N)$ to increase; since this is impossible, one has $\lambda = \nu$ and for a similar reason $\mu = \nu + 1$ (except if $\sigma = 0$, in which case $\mu = \nu$). Obviously a variable N attaining the supremum S is such that $E[N(N - 1)] = C$ (this could be proved, if necessary, by slightly modifying the preceding argument).

By what precedes, the supremum S is attained by the variable N^* concentrated on $\{\nu, \nu + 1\}$ and with expectation $E(N^*) = \nu + \sigma$; this variable is unique and its law is given by

$$p_\nu^* = 1 - \sigma, \quad p_{\nu+1}^* = \sigma, \quad p_m^* = 0 \text{ otherwise};$$

moreover $C = E[N^*(N^* - 1)] = \nu(\nu + 2\sigma - 1)$.

Finally, let $\theta = 2\sigma - 1$ to obtain the result indicated above. The representation of the constant C as $\nu(\nu + \theta)$ is unique for it follows from $-1 \leq \theta < 1$ that ν is the largest integer such that $\nu(\nu - 1) \leq C$; equivalently ν is the largest integer such that $\nu \leq \frac{1}{2} + (C + \frac{1}{4})^{\frac{1}{2}}$. It may also be remarked that

$$S = \frac{1}{2} + (\nu + \frac{1}{2}\theta) = \frac{1}{2} + (C + \frac{1}{4}\theta^2)^{\frac{1}{2}}$$

so that for large C , one has

$$S = C^{\frac{1}{2}} + \frac{1}{2} + O(C^{-\frac{1}{2}}).$$

The following final result will be obtained by letting $C = n(n - 1)\alpha^2$ and $\varepsilon_n(\alpha) = S - n\alpha$.

Let ν be the largest integer such that $\nu(\nu - 1) \leq n(n - 1)\alpha^2$. Then

$$\varepsilon_n(\alpha) = \frac{1}{2}(1 - \alpha) + \frac{[n\alpha - \nu][(n - 1)\alpha - \nu]}{2\nu}.$$

The second term vanishes when $n\alpha$ or $(n-1)\alpha$ is an integer (for then ν equals $n\alpha$ or $(n-1)\alpha$, respectively); for $n \rightarrow \infty$, it is of the order of $1/n$.

The value of $\varepsilon_n(\alpha)$ given above is obtained by elementary computations from the equations

$$\varepsilon_n(\alpha) = S - n\alpha; \quad S = \nu + \frac{1}{2}(1 + \theta); \quad \theta = (C - \nu^2)/\nu; \quad C = n(n-1)\alpha^2.$$

When $n\alpha$ is an integer, it follows from $C = n\alpha(n\alpha - \alpha)$ that $\nu = n\alpha$ and that $\theta = -\alpha$; similarly if $(n-1)\alpha$ is an integer, then $\nu = (n-1)\alpha$ and $\theta = \alpha$; in both cases $\varepsilon_n(\alpha)$ reduces to $\frac{1}{2}(1 - \alpha)$. When n increases to infinity, $[n(n-1)\alpha^2]^{\frac{1}{2}} = n\alpha - \frac{1}{2}\alpha + O(1/n)$; hence

$$\varepsilon_n(\alpha) = [n(n-1)\alpha^2]^{\frac{1}{2}} + \frac{1}{2} - n\alpha + O(1/n) = \frac{1}{2}(1 - \alpha) + O(1/n).$$

3. An example.

Using well known properties of quadratic residues we can construct explicit examples which are extremal in the sense of the preceding paragraph, for $\alpha = \frac{1}{2}$. We shall need the following

THEOREM 2. *Let p be a prime number such that $p \equiv 3 \pmod{4}$. Put $p = 4k - 1$. Let $r_1, r_2, \dots, r_{2k-1}$ be all the quadratic residues mod p . Then if d is any of the numbers $1, 2, \dots, p-1$, there are among the numbers $r_j + d$, $j = 1, 2, \dots, 2k-1$, exactly $k-1$ which are congruent to some r_h , $1 \leq h \leq 2k-1$ (and k which are not).*

Let us now define a sequence of subsets of the interval $[0, 1)$ as follows. Let A_0 be the union of the intervals

$$\left[0, \frac{3}{4p}\right] \quad \text{and} \quad \left[\frac{r_j}{p}, \frac{r_{j+1}}{p}\right), \quad j = 1, 2, \dots, 2k-1.$$

Let further A_d be obtained from A_0 by shifting it mod 1 by the distance d/p , $d = 1, 2, \dots, p-1$. For $p = 7$, the sets $A_0, A_1, \dots, A_6$ are shown in Fig. 1. Denoting by $P(A)$ the Lebesgue measure of the set A we have

$$(2) \quad P(A_j) = \frac{p-1}{2p} + \frac{3}{4p} = \frac{1}{2} + \frac{1}{4p}.$$

On the other hand, according to the theorem on quadratic residues mentioned above we have

$$(3) \quad P(A_j A_{j+d}) = P(A_0 A_d) = \frac{p-3}{4p} + \frac{3}{4p} = \frac{1}{4}$$

for $d = 1, 2, \dots, p-1-j$; $j = 0, 1, \dots, p-2$. As a matter of fact the interval $[(r_j + d)/p, (r_j + d + 1)/p)$ belonging to A_d coincides (mod 1) with an

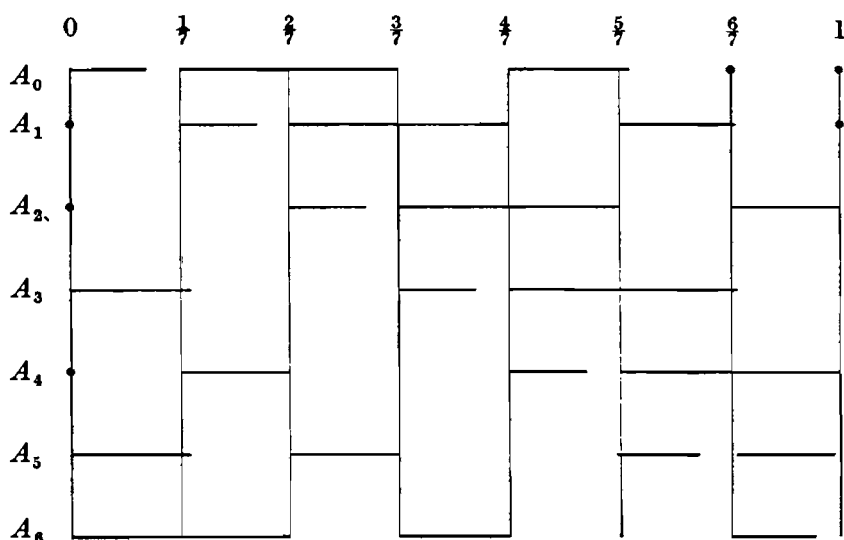


Fig. 1.

interval of A_0 if and only if $r_j + d$ is a quadratic residue, and thus for $k-1 = (p-3)/4$ values of j ; further, if d is a quadratic residue then the interval $[d/p, (d + \frac{3}{4})/p]$ belonging to A_d coincides with $\frac{3}{4}$ of an interval belonging to A_0 , while if d is not a quadratic residue then $p-d$ is a quadratic residue mod p (p being of the form $4k-1$) and thus the interval $(0, 3/(4p))$ belonging to A_0 coincides with $\frac{3}{4}$ of an interval belonging to A_d (namely of that obtained from the interval

$$[(p-d)/p, (p-d+1)/p]$$

by shifting it by d/p). Thus our system of sets $A_0, A_1, \dots, A_{p-1}$ satisfies the conditions $P(A_j A_k) = \frac{1}{4}$ for $j \neq k$ and

$$P(A_j) = \frac{1}{2} + \frac{1}{4p} \quad \text{for } j = 0, 1, \dots, p-1.$$

Hence if we consider the sets $A_0, \dots, A_{p-1}$ as events in the probability space $(\Omega, \mathcal{A}, P)$ where Ω is the interval $[0, 1)$, $\mathcal{A}$ the set of all measurable subsets of $\mathcal{A}$, and P the Lebesgue measure, then $\{A_0, \dots, A_{p-1}\}$ is an extremal system of events (for $\alpha = \frac{1}{2}$, $n = p$) of the required type.

REFERENCES

1. O. Perron, *Bemerkung über die Verteilung der quadratischen Reste*, Math. Z. 56 (1952), 122-130.
2. S. Zubrzycki, *Les inégalités entre les moments des variables aléatoires équivalentes*, Studia Math. 14 (1954), 232-242.

147, 181, 303

NOTE

Very simple estimates of the sums $\sum P(A_i)$ and $\sum P(A_i A_j)$ are given by Rényi No. (303). (P. R.)

ASYMMETRIC GRAPHS

By

P. ERDŐS and A. RÉNYI (Budapest), members of the Academy

Dedicated to T. GALLAI, at the occasion of his 50th birthday

Introduction

We consider in this paper only non-directed graphs without multiple edges and without loops. The number of vertices of a graph G will be called its order, and will be denoted by $N(G)$. We shall call such a graph symmetric, if there exists a non-identical permutation of its vertices, which leaves the graph invariant. By other words a graph is called symmetric if the group of its automorphisms has degree greater than 1. A graph which is not symmetric will be called *asymmetric*. The degree of symmetry of a symmetric graph is evidently measured by the degree of its group of automorphisms. The question which led us to the results contained in the present paper is the following: how can we measure the degree of asymmetry of an asymmetric graph?

Evidently any asymmetric graph can be made symmetric by deleting certain of its edges and by adding certain new edges connecting its vertices. We shall call such a transformation of the graph its symmetrization. For each symmetrization of the graph let us take the sum of the number of deleted edges — say r — and the number of new edges — say s ; it is reasonable to define the degree of asymmetry $A[G]$ of a graph G , as the minimum of $r+s$ where the minimum is taken over all possible symmetrizations of the graph G . (In what follows if in order to make a graph symmetric we delete r of its edges and add s new edges, we shall say that we *changed* $r+s$ edges.) Clearly the asymmetry of a symmetric graph is according to this definition equal to 0, while the asymmetry of any asymmetric graph is a positive integer.

The question arises: how large can be the degree of asymmetry of a graph of order n (i. e. a graph which has n vertices)? We shall denote by $A(n)$ the maximum of $A[G]$ for all graphs G of order n ($n=2, 3, \dots$). We put further $A(1) = +\infty$. It is evident that $A(2)=A(3)=0$.

Now let $\bar{G}$ denote the complementary graph of G , that is the graph which consists of the same vertices as G and of those and only those edges which do not belong to G ; then we have evidently

LEMMA 1.

$$(1) \quad A[G] = A[\bar{G}].$$

As a matter of fact the complementary graph of a symmetric graph is evidently also symmetric (i. e. (1) holds if $A[G]=0$) and if a transformation T , consisting in deleting r edges and adding s new edges, makes G symmetric, then the transformation $\bar{T}$, consisting in adding those s edges which are deleted by T and deleting those r edges which are added by T , is clearly a symmetrization of $\bar{G}$, and thus Lemma 1 follows.

We shall need also the following evident fact:

LEMMA 2. *If a graph G is not connected and its components are $G_1, G_2, \dots, G_c$ then we have*

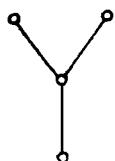
$$(2) \quad A[G] \leq \min_{1 \leq i \leq c} A[G_i].$$

Let us mention further that a graph containing more than one isolated point is symmetric.

Now we can prove that $A(4)=0$ and $A(5)=0$. Let us first consider $A(4)$. Clearly any not connected graph of order 4 is symmetric by Lemma 2, further by Lemma 1 we may restrict ourselves to graphs



Fig. 1



of order 4 having not more than $\frac{1}{2}\binom{4}{2} = 3$ edges, because if the graph has more than 3 edges, the complementary graph has less than 3 edges. But the only connected graphs of order 4 with not more than 3 edges are the path and the star shown on Fig. 1

which are clearly symmetric. Thus $A(4)=0$. Now we show $A(5)=0$. Again we can restrict ourselves to graphs of order 5 which are connected and which contain not more than $\frac{1}{2}\binom{5}{2} = 5$ edges. These belong however all to one of the 8 types shown on Fig. 2 which are evidently all symmetric.

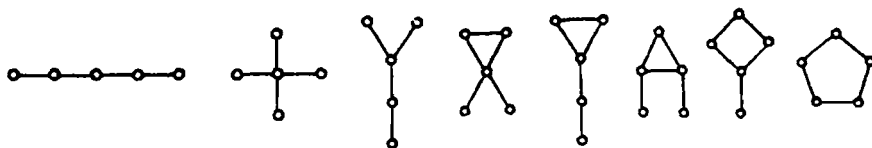


Fig. 2

(We have drawn the graphs so that each is symmetric with respect to its vertical axis.)

Now we shall show that $A(6)=1$. Here again we may restrict ourselves to consider connected graphs having not more than $\left\lfloor \frac{1}{2}\binom{6}{2} \right\rfloor = 7$ edges.* Among these we find four asymmetric types, shown by Fig. 3.

All have their degree of asymmetry equal to 1. As a matter of fact, each can be made symmetric by deleting the edge which is indicated by a thick line. It is easy to see that any of these graphs can also be made symmetric

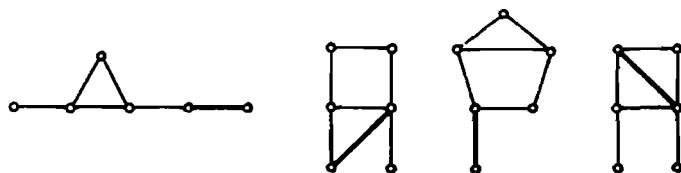


Fig. 3

* Here and in what follows $[x]$ denotes the integral part of the real number x .

by adding a suitably chosen edge, as shown on Fig. 4, where the edge to be added is indicated by a dotted line.

However it is not true in general that if a graph can be made symmetric by omitting one edge, it can also be made symmetric by adding one edge. For instance Fig. 5 shows a graph of order 10 which can be made symmetric by omitting one edge (that which is drawn by a thick line) but can not be made symmetric by adding one new edge. (Of course if by omitting an edge an involutory symmetry is produced, then the same symmetry can be produced by adding (instead of omitting) a suitably chosen edge.)

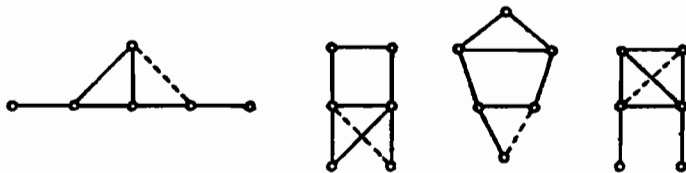


Fig. 4

In § 1 we shall show (Theorem 1) by a simple argument that the asymmetry of a graph of order n can not exceed $\frac{n-1}{2}$ if n is odd, while if n is even the asymmetry can not exceed $\frac{n}{2} - 1$; in § 2 we prove (Theorem 2) that this estimate is asymptotically best possible, that is for any $\varepsilon > 0$ there can be found an integer $n_0(\varepsilon)$ such that for any $n > n_0(\varepsilon)$ there exists a graph G_n of order n for which $A[G_n] > \frac{n}{2}(1 - \varepsilon)$.

In other words we have

$$(3) \quad \lim_{n \rightarrow +\infty} \frac{A(n)}{n} = \frac{1}{2}.$$

We can prove still more, namely that there exists a positive constant C such that

$$A(n) > \frac{n}{2} - C\sqrt{n \log n}.$$

However we do not know whether there exist graphs G_n of even resp. odd order n for which

$$A[G_n] = \frac{n}{2} - 1 \text{ resp. } A[G_n] = \frac{n-1}{2};$$

we can prove that this is impossible if $n \equiv 3 \pmod{4}$ and we guess that this is impossible for all n .

In view of (3) it is reasonable to introduce the quantity

$$(4) \quad a[G] = \frac{A[G]}{\left\lceil \frac{N(G)-1}{2} \right\rceil}$$

for any graph G with $N(G) \geq 3$, and call it the relative asymmetry of G . It follows from our results that for any graph G with $N(G) \geq 3$ one has

$$(5) \quad 0 \leq a[G] \leq 1.$$

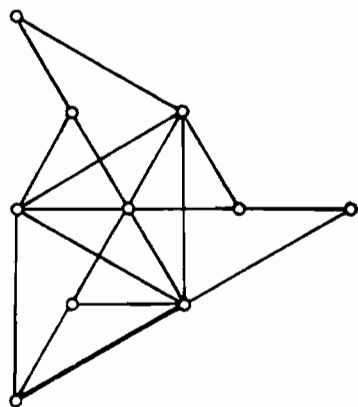


Fig. 5

The proof of Theorem 2 is not constructive, only a proof of existence. It uses probabilistic considerations. This method gives however more than stated above: it shows that for large values of n most graphs of order n are asymmetric, the degree of asymmetry of most of them being near to $\frac{n}{2}$.

An other interesting question is to investigate the asymmetry or symmetry of a graph for which not only the number of vertices but also the number N of edges is fixed, and to ask that if we choose one of these graphs at random, what is the probability of its being asymmetric. We have solved this question too, and have shown that if $N = \frac{n}{2} \log n + \omega(n)n$ where $\omega(n)$ tends arbitrarily slowly to $+\infty$ for $n \rightarrow +\infty$, then the probability that a graph with n vertices and N edges chosen at random (so that any such graph has the same probability $\left(\frac{\binom{n}{2}}{N}\right)^{-1}$ to be chosen) should be asymmetric, tends to 1 for $n \rightarrow +\infty$. This and some further related results will be published in an other forthcoming paper.

In § 3 we deal with (denumerably) infinite graphs, more exactly with random infinite graphs Γ defined as follows. Let $P_1, P_2, \dots, P_n, \dots$ be an infinite sequence of vertices. Let us suppose that for each j and k ($j \neq k$) if E_{jk} denotes the event that P_j and P_k are connected by an edge, then the events E_{jk} are independent and each has the probability $\frac{1}{2}$. We prove the simple but surprising fact that Γ is symmetric with probability 1 (Theorem 3).

Thus there is a striking contrast between finite and infinite graphs: while „almost all” finite graphs are asymmetric, „almost all” infinite graphs are symmetric.

In § 4 we deal with the asymmetry of graphs of order n in which the total number N of edges is fixed.

In § 5 we deal with some related unsolved problems.

Our thanks are due to T. GALLAI for his valuable remarks.

§ 1. Proof of the theorem that the asymmetry of a graph of order n can not exceed $\left\lfloor \frac{n-1}{2} \right\rfloor$

In this § we prove

THEOREM 1.

$$A(n) \leq \left\lfloor \frac{n-1}{2} \right\rfloor.$$

REMARK. Of course Theorem 1 implies that if n is odd, then $A(n) \leq \frac{n-1}{2}$

and if n is even, we have $A(n) \leq \frac{n}{2} - 1$.

PROOF. Let G be an arbitrary graph of order n . We may suppose $n \geq 6$. Let $P_1, P_2, \dots, P_n$ be the vertices of G and let us denote by v_k the valency of P_k in G (i. e. v_k is the number of edges having P_k as one of their endpoints.)

Let further v_{jk} ($j \neq k$) denote the number of vertices P_h of G ($h \neq j, h \neq k$) which are connected in G both with P_j and with P_k . Let us put further $v_{jj} = 0$. Clearly $v_{kj} = v_{jk}$ and

$$(1.1) \quad \sum_{j=1}^n \sum_{k=1}^n v_{jk} = \sum_{h=1}^n v_h(v_h - 1).$$

As a matter of fact, both the left hand side and the right hand side of (1.1) are equal to the number of (ordered) pairs of edges of G which have one common endpoint. Let us choose now two distinct vertices P_j and P_k of G ($j \neq k$) and let us put

$$(1.2) \quad \Delta_{jk} = v_j + v_k - 2v_{jk} - 2\delta_{jk}$$

where $\delta_{jk} = 1$ or 0 according to whether P_j and P_k are connected by an edge in G or not. Let us put further $\Delta_{jj} = 0$. Evidently Δ_{jk} is the number of vertices of G which are in different relation with P_j and P_k (i. e. which are either connected with P_j and not connected with P_k or connected with P_k and not connected with P_j). Clearly by omitting all edges connecting P_j (resp. P_k) with some point of G which is not connected with P_k (resp. P_j) we obtain a graph G' in which P_j and P_k are connected with the same points. Thus G' has the symmetry consisting in the interchange of P_j and P_k and leaving all other points unchanged. But G' is obtained from G by deleting Δ_{jk} edges. Thus G can be made symmetric by deleting Δ_{jk} edges. It follows that

$$(1.3) \quad A[G] \leq \min_{j \neq k} \Delta_{jk} \leq \frac{\sum_{j=1}^n \sum_{k=1}^n \Delta_{jk}}{n(n-1)}.$$

On the other hand we have

$$(1.4) \quad \sum_{j=1}^n \sum_{k=1}^n \Delta_{jk} = 2 \sum_{l=1}^n v_l(n-1-v_l).$$

As a matter of fact, the left hand side of (1.4) is equal to the number of ordered triplets (P_j, P_k, P_l) of vertices such that G contains exactly one of the two possible edges $\widehat{P_j P_l}$ and $\widehat{P_k P_l}$; if we fix P_l then that among P_j and P_k which is connected with P_l can be chosen in v_l ways and the other in $n-1-v_l$ ways; this proves (1.4). ((1.4) could also be deduced from (1.1) and (1.2)).

As clearly

$$(1.5) \quad v_l(n-1-v_l) = \left(\frac{n-1}{2}\right)^2 - \left(v_l - \frac{n-1}{2}\right)^2$$

we obtain

$$(1.6) \quad 2 \sum_{l=1}^n v_l(n-1-v_l) \leq \begin{cases} \frac{n(n-1)^2}{2} & \text{if } n \text{ is odd} \\ n \frac{[(n-1)^2 - 1]}{2} & \text{if } n \text{ is even.} \end{cases}$$

It follows from (1.3), (1.4) and (1.6)

$$(1.7) \quad A(G) \leq \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd} \\ \frac{n(n-2)}{2(n-1)} & \text{if } n \text{ is even.} \end{cases}$$

Now we have evidently

$$\frac{n(n-2)}{2(n-1)} < \frac{n}{2} \quad \text{if } n > 1.$$

Thus it follows from (1.7) that

$$(1.8) \quad A[G] \leq \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd} \\ \frac{n}{2} - 1 & \text{if } n \text{ is even} \end{cases}$$

and thus for every n

$$(1.9) \quad A[G] \leq \left\lfloor \frac{n-1}{2} \right\rfloor.$$

As (1.9) holds for every graph G of order n , Theorem 1 is proved.

The problem arises, for which odd values of n does there exist a graph G of order n such that

$$(1.10) \quad \min_{j \neq k} \Delta_{jk} = \frac{n-1}{2}.$$

As by (1.3) and (1.6) we have for odd n

$$(1.11) \quad \min_{j \neq k} \Delta_{jk} \leq \frac{\sum_{j \neq k} \Delta_{jk}}{n(n-1)} \leq \frac{n-1}{2}$$

it follows that (1.10) can hold only if $\Delta_{jk} = \frac{n-1}{2}$ for all $j \neq k$. It follows from

(1.5) that in this case we have also $v_l = \frac{n-1}{2}$ for $l = 1, 2, \dots, n$. Now if $n \equiv 3 \pmod{4}$

then $\frac{n-1}{2}$ is odd, and as in any graph the number of vertices having an odd valency is even we obtain a contradiction. Thus (1.10) can hold for an odd n only if $n \equiv 1 \pmod{4}$.

We shall call a graph G of order $n \equiv 1 \pmod{4}$ for which (1.10) holds a Δ -graph.

For $n=5$ the cycle of order 5 is a Δ -graph. For $n=9$ a Δ -graph is shown by Fig. 6.

A simple way to describe the Δ -graph shown by Fig. 6 is as follows: let the 9 vertices be labelled by ordered pairs of numbers (a, b) where a and b may take on independently the values 0, 1, 2. Let us connect the vertices labelled by (a, b) and (a', b') if and only if either $a = a'$ or $b = b'$.

We can construct a Δ -graph of order p , if p is an arbitrary prime for which $p \equiv 1 \pmod{4}$, as follows: Let $P_1, P_2, \dots, P_p$ be the vertices of G and let us connect the vertices P_j and P_k if and only if $k-j$ is a quadratic residue mod p . In this case clearly each vertex P_j has valency $\frac{p-1}{2}$. We show that for each $j \neq k$ we have $\Delta_{jk} = \frac{p-1}{2}$. This follows immediately from the following well-known property of quadratic residues observed first by Lagrange (see [1] and [2]): If $r_1, r_2, \dots, r_{\frac{p-1}{2}}$ are all quadratic residues among the numbers $1, 2, \dots, p-1$, then among the num-

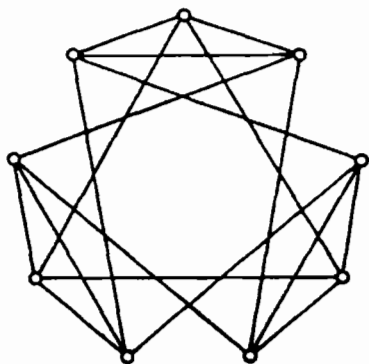


Fig. 6

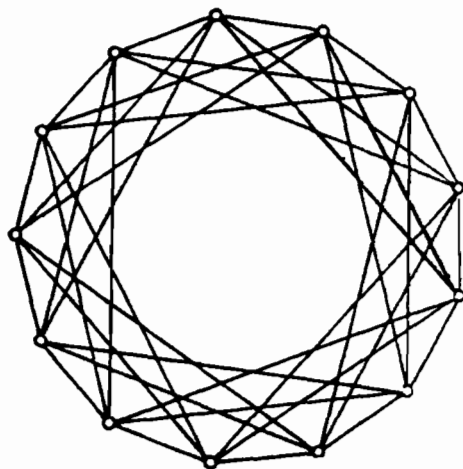


Fig. 7

bers $r_l + d \left(l=1, 2, \dots, \frac{p-1}{2} \right)$ where d is any of the numbers $1, 2, \dots, p-1$, there are exactly $\frac{p-1}{4}$ which are congruent to a quadratic non-residue mod p . As a matter of fact Δ_{jk} is equal to the number of those integers h ($h=1, 2, \dots, p$) for which $h-j$ is a quadratic residue and $h-k$ a non-residue, or $h-j$ a quadratic non-residue and $h-k$ a residue. Putting $d=k-j$ this means that Δ_{jk} is equal to the sum of the number of non-residues among the numbers $r_l + d \left(l=1, 2, \dots, \frac{p-1}{2} \right)$ and the number of non-residues among the numbers $r_l - d \left(l=1, 2, \dots, \frac{p-1}{2} \right)$ and thus $\Delta_{jk} = 2 \left(\frac{p-1}{4} \right) = \frac{p-1}{2}$.

Thus there exists a Δ -graph of every order n which is a prime of the form $4k+1$. Clearly the Δ -graph of order 5 mentioned above is the same as that obtained by the above general construction for $p=5$. For $p=13$ the Δ graph obtained by our construction is shown by Fig. 7.

We can construct also a Δ -graph of order $n=p^2$ if p is a prime of the form $p=4k+3$. The construction is as follows: let us label the vertices by the pairs of numbers (a, b) where $0 \leq a \leq p-1$, $0 \leq b \leq p-1$. Let us connect the vertices

labelled with (a, b) and (a', b') if either $a = a'$, or $(a - a')(b - b')$ is a quadratic residue mod p . In this case each vertex (a, b) has the valency $\frac{p^2 - 1}{2}$, because it is connected with the $p - 1$ vertices (a, b') where $b' \neq b$ and with the $\left(\frac{p-1}{2}\right)^2$ vertices (a', b') such that $a - a'$ and $b - b'$ are both quadratic residues mod p and the $\left(\frac{p-1}{2}\right)^2$ vertices (a', b') such that $a - a'$ and $b - b'$ are both quadratic non-residues mod p and $2\left(\frac{p-1}{2}\right)^2 + p - 1 = \frac{p^2 - 1}{2}$. Further denoting by v the number of vertices which are connected with one of the vertices (a, b) and (a', b') but not with the other, we always have $v = \frac{p^2 - 1}{2}$. This follows from the theorem (due to Lagrange) according to which if $r_1, r_2, \dots, r_{\frac{p-1}{2}}$ is a complete set of quadratic residues mod p

then exactly $\frac{p-3}{2}$ among the numbers $r_j + d \left(j = 1, 2, \dots, \frac{p-1}{2} \right)$ are congruent to a quadratic residue mod p (see [3]). Mr. A. HEPPES (oral communication) has constructed by a similar but different method a Δ -graph of order p^2 for every odd prime p .

We can construct a Δ -graph of order p^r where p is an odd prime, and r an arbitrary positive integer such that $p^r \equiv 1 \pmod{4}$ (that is, if $p \equiv 1 \pmod{4}$ then r is arbitrary, while if $p \equiv 3 \pmod{4}$ then r has to be an even number), as follows. Let us label the p^r vertices of the graph by the elements of a Galois-field $GF(p^r)$. Let us connect two vertices labelled by U and V ($U \in GF(p^r), V \in GF(p^r)$) if and only if $U - V = C^2$ where C is some element of $GF(p^r)$. Now J. B. KELLY [2] has proved that for any $GF(p^r)$ with $p^r \equiv 1 \pmod{4}$ by denoting by A the subset of those non-zero elements which are squares, and by B the subset of those elements which are not squares, it follows that any non-zero element d can be represented in exactly $\frac{p^r - 1}{2}$ ways in the form $d = a - b$ where $a \in A$ and $b \in B$. Thus it follows (exactly as in the case $r = 1$) that our graph G is a Δ -graph. Thus there exists a Δ -graph of order n if $n = p^r \equiv 1 \pmod{4}$ where p is a prime. We do not know whether there exists a Δ -graph of order n if $n \equiv 1 \pmod{4}$ and n is not a prime-power.

Let us mention that all Δ -graphs which we have constructed are symmetric; for instance the Δ -graph of order 9 shown by Fig. 6. has the automorphism which carries over the vertex labelled with (a, b) into the vertex labelled with (a', b') where $a' \equiv a + 1 \pmod{3}$ and $b' \equiv b + 1 \pmod{3}$. The Δ -graph of order p where p is a prime of the form $4k + 1$ constructed above has the symmetry which carries p_l into $p_{l'}$ where $l' = l + 1 \pmod{p}$.

Thus while there exist at least for certain odd values of n graphs for which $\min \Delta_{jk} = \frac{n-1}{2}$, we do not know any graph of (odd) order n for which $A[G] = \frac{n-1}{2}$. We guess that this is impossible.

It is possible that the following stronger conjecture holds also: all Δ graphs are symmetric.

Finally we should add the following remark: Let $C_3(G)$ denote the number of triangles contained in a graph G . A. GOODMAN [4] (see also [5] and [6]) has determined the minimum of $C_3(G_n) + C_3(\bar{G}_n)$ for all graphs of order n . For $n \equiv 1 \pmod{4}$ his result is as follows:

$$(1.12) \quad \min(C_3(G_n) + C_3(\bar{G}_n)) = \frac{n(n-1)(n-5)}{24}.$$

Let us call a graph of order n for which the minimum in (1.12) is attained, a Goodman-graph. Now it is easy to see that any Δ -graph is at the same time a Goodman-graph (but not conversely). This can be proved as follows: If G_n is a Δ -graph of order n , then the number of triangles contained in G_n and containing the edge PQ is equal to the number of vertices connected with both P and Q , and thus is equal to $\frac{n-1}{2} - \frac{n-1}{4} - 1 = \frac{n-5}{4}$. As the total number of edges of G_n is $\frac{n(n-1)}{4}$ and each triangle is counted in this way three times, $C_3(G_n) = \frac{n(n-1)(n-5)}{48}$. Clearly if G_n is a Δ -graph then $\bar{G}_n$ is a Δ -graph too; thus it follows that $C_3(G_n) + C_3(\bar{G}_n) = \frac{n(n-1)(n-5)}{24}$, i. e. that (1.12) holds for G_n .

§ 2. The asymmetry of a random graph of order n

In this § we prove the following

THEOREM 2. *Let us choose at random a graph Γ having n given vertices so that all possible $2^{\binom{n}{2}}$ graphs should have the same probability to be chosen. Let $\varepsilon > 0$ be arbitrary. Let $P_n(\varepsilon)$ denote the probability that by changing not more than $\frac{n(1-\varepsilon)}{2}$ edges of Γ it can be transformed into a symmetric graph. Then we have*

$$(2.2) \quad \lim_{n \rightarrow +\infty} P_n(\varepsilon) = 0.$$

COROLLARY. *For any ε with $0 < \varepsilon < 1$ there exists an integer $n_0(\varepsilon)$ depending only on ε , such that for $n > n_0(\varepsilon)$ there exist graphs G of order n with $A[G] > \frac{n(1-\varepsilon)}{2}$.*

REMARK. Clearly it follows from Theorem 1 and the corollary of Theorem 2 that

$$(2.3) \quad \lim_{n \rightarrow +\infty} \frac{A(n)}{n} = \frac{1}{2}.$$

The same method yields also $\frac{n}{2} - A(n) = O(\sqrt{n \log n})$ but we shall not prove this in detail.

PROOF of Theorem 2. As the proof is not simple, we first give a sketch of the proof.

Let us denote by $P_n(\varepsilon, q)$ ($q=2, 3, \dots$) the probability that a random graph of order n can be transformed by changing $m < \frac{n}{2}(1-\varepsilon)$ of its edges into a graph admitting a permutation Π as an automorphism, where Π is a permutation which leaves exactly $l = n - q$ of the n vertices of the graph unchanged, but which can not be transformed into a symmetric graph by changing less than m of its edges. Then we have

$$(2.4) \quad P_n(\varepsilon) \leq \sum_{q=2}^n P_n(\varepsilon, q).$$

We shall estimate $P_n(\varepsilon, q)$ as follows

$$(2.5) \quad P_n(\varepsilon, q) \leq \frac{A_{n,q} \cdot B_{n,q} \cdot C_{n,q}}{2^{\binom{n}{2}}}$$

where $A_{n,q}$ is the number of ways a permutation Π_q , leaving exactly $l = n - q$ of the n vertices of the graph invariant, can be chosen; $B_{n,q}$ is an upper bound for the number of graphs which are invariant under such a permutation Π_q and $C_{n,q}$ is an upper bound for the number of graphs which can be transformed into a graph admitting a given permutation Π_q by changing $m \leq \frac{n}{2}(1-\varepsilon)$ of its edges, and can not be transformed into a symmetric graph by changing less than m of its edges.

We shall deal first with the terms for which q lies in the range

$$(2.6) \quad \sqrt[4]{n} \leq q \leq n$$

then with the terms for which q lies in the range

$$(2.7) \quad 5 \leq q < \sqrt[4]{n}$$

and finally with the terms corresponding to $q=2, 3$ and 4 separately. We shall show that the sum figuring on the right hand side of (2.4) tends to 0 for $n \rightarrow +\infty$; this clearly implies the assertion of Theorem 2.

Let us go now into the details.

Let Π be an arbitrary permutation of order n having the cycle-representation

$$(2.7) \quad \Pi = (a_{1,1}, \dots, a_{1,c_1})(a_{2,1}, \dots, a_{2,c_2}) \dots (a_{r,1}, \dots, a_{r,c_r})$$

where $a_{i,j}$ ($1 \leq j \leq c_i; 1 \leq i \leq r$) are the numbers $1, 2, \dots, n$ in some order. Thus $c_1, c_2, \dots, c_r$ are the cycle-lengths of Π . The permutation Π can also be interpreted as a one-to-one mapping of the set $\{1, 2, \dots, n\}$ onto itself. Let Π , interpreted this way, map k into Πk ($k=1, 2, \dots, n$). We shall denote by Π^s the mapping obtained by applying the mapping Π s times. Clearly $\Pi a_{i,j} = a_{i,j+1}$ for $j=1, 2, \dots, c_i$ where a_{i,c_i+1} stands for $a_{i,1}$. Let us calculate first the probability that a graph Γ of order n chosen at random should admit Π as its automorphism. By choosing a graph Γ at random we mean that n vertices $P_1, \dots, P_n$ are prescribed and we choose

some set of edges connecting these vertices at random, so that each of the $2^{\binom{n}{2}}$ possible choices has the same probability $2^{-\binom{n}{2}}$.

Thus the random choice of Γ is equivalent with a sequence of $\binom{n}{2}$ independent random decisions concerning all possible $\binom{n}{2}$ edges, so that with respect to any possible edge the probability of including it into Γ is equal to $\frac{1}{2}$. An equivalent way of characterizing the random choice of Γ is as follows: let us put $\varepsilon_{j,k} = 1$ if the edge $\widehat{P_j P_k}$ is contained in Γ and $\varepsilon_{j,k} = 0$ if not ($1 \leq j < k \leq n$). Then the random choice of Γ means that the $\varepsilon_{j,k}$ with $j < k$ are independent random variables each taking on the values 1 and 0 with probability $\frac{1}{2}$. Let us put $\varepsilon_{k,j} = \varepsilon_{j,k}$ for $j < k$. Now Γ admits the automorphism Π if and only if for any pair j, k ($j \neq k$) one has $\varepsilon_{\Pi j, \Pi k} = \varepsilon_{j,k}$. Let us calculate now how many of the values $\varepsilon_{j,k}$ can still be chosen arbitrarily. An easy argument shows that if j belongs to the a -th cycle of Π (of length c_a) and k to the b -th cycle of Π (of length c_b) (where $a \neq b$) then the sequence of equations

$$\varepsilon_{j,k} = \varepsilon_{\Pi j, \Pi k} = \varepsilon_{\Pi^2 j, \Pi^2 k} = \dots = \varepsilon_{\Pi^r j, \Pi^r k} = \dots$$

contains $[c_a, c_b]$ different terms where $[A, B]$ denotes the least common multiple of A and B . Thus among the $c_a \cdot c_b$ values $\varepsilon_{j,k}$ where j belongs to the a -th cycle and k to the b -th cycle of Π we can choose only $\frac{c_a \cdot c_b}{[c_a, c_b]} = (c_a, c_b)$ values independently, where (A, B) stands for the greatest common divisor of A and B ; all other such $\varepsilon_{j,k}$ are then determined ($a \neq b$; $1 \leq a \leq r$; $1 \leq b \leq r$).

By a similar argument we get that among the $\varepsilon_{j,k}$ with both j and k belonging to the a -th cycle of Π we can choose $\left\lfloor \frac{c_a}{2} \right\rfloor$ independently, where $[x]$ denotes the integral part of x . Thus there are exactly

$$(2.8) \quad 2^{1 \leq a < b \leq r (c_a, c_b) + \sum_{a=1}^r \left\lfloor \frac{c_a}{2} \right\rfloor}$$

different graphs of order n which admit the automorphism Π , having the cycle representation (2.7), and the probability of Γ admitting the automorphism Π , i. e. of $\Pi\Gamma = \Gamma$ is

$$(2.9) \quad P(\Pi\Gamma = \Gamma) = 2^{1 \leq a < b \leq r (c_a, c_b) + \sum_{a=1}^r \left\lfloor \frac{c_a}{2} \right\rfloor - \binom{n}{2}}.$$

Now let us fix a graph G for which $\Pi G = G$ and count the number of such graphs which can be transformed into G by changing m of its edges.

Clearly the m edges to be changed can be chosen in $\binom{\binom{n}{2}}{m}$ ways. Thus the number of graphs which can be transformed into one admitting the automorphism Π by changing m edges can not exceed

$$(2.10) \quad \binom{\binom{n}{2}}{m} 2^{1 \leq a < b \leq r (c_a, c_b) + \sum_{a=1}^r \left\lfloor \frac{c_a}{2} \right\rfloor}.$$

Now let us suppose that among the cycle-lengths c_a of Π there are exactly $l = n - q$ which are equal to 1; we may suppose $c_1 = c_2 = \dots = c_l = 1$ and $c_{l+i} \geq 2$ for $i = 1, 2, \dots, r - l$. Then we have

$$q = \sum_{i=1}^{r-l} c_{l+i} \geq 2(r-l)$$

and thus

$$(2.11) \quad (r-l) \leq \frac{q}{2} = \frac{n-l}{2} \quad \text{and} \quad r \leq \frac{n+l}{2}.$$

As $(c_a, c_b) \leq \min(c_a, c_b) \leq \frac{c_a + c_b}{2}$, it follows

$$(2.12) \quad \sum_{1 \leq a < b < r} (c_a, c_b) + \sum_{a=1}^r \left[\frac{c_a}{2} \right] \leq \binom{l}{2} + (r-l) \left(\frac{n+l}{2} \right).$$

Thus

$$(2.13) \quad \sum_{1 \leq a < b \leq r} (c_a, c_b) + \sum_{a=1}^r \left[\frac{c_a}{2} \right] \leq \binom{l}{2} + \frac{n^2 - l^2}{4}.$$

Thus the probability of choosing at random such a graph which can be transformed by less than $(1 - \varepsilon) \frac{n}{2}$ changes into one admitting Π as an automorphism does not exceed

$$(2.14) \quad 2^{\frac{l^2 - n^2}{4} + O(n \log n)}.$$

As the number of permutations Π with a fixed l is less than $\binom{n}{l} (n-l)! = 2^{O(n \log n)}$ we have

$$(2.15) \quad \sum_{\sqrt[4]{n} \leq q \leq n} P_n(\varepsilon, q) \leq 2^{-\frac{n^{3/4}}{2} + O(n \log n)}.$$

Now we consider the permutations with $5 \leq q \leq \sqrt[4]{n}$. Concerning these we have to use much careful estimations.

Let us fix first the value of q ($5 \leq q < \sqrt[4]{n}$). The number of permutations which leave $n - q = l$ elements unchanged is clearly less than $\binom{n}{q} q! \leq n^{\sqrt[4]{n}}$. In estimating the number of ways in which the m edges to be changed can be chosen, we may restrict ourselves to those edges, which connect either the q points which do not remain unchanged by Π among themselves, or edges connecting such points with the invariant ones. Thus an upper bound for the number of choices of the

$m < \frac{n}{2}(1-\varepsilon)$ edges is given by

$$(2.16) \quad \sum_{m < \frac{n}{2}(1-\varepsilon)} \binom{\binom{q}{2} + q(n-q)}{m} \leq n \binom{nq}{\frac{n}{2}(1-\varepsilon)} = 2^{H(\alpha)nq + O(\log n)}$$

where $\alpha = \frac{1-\varepsilon}{2q}$ and $H(\alpha) = \alpha \log_2 \frac{1}{\alpha} + (1-\alpha) \log_2 \frac{1}{1-\alpha}$.

Now if $q \geq 5$ then $\alpha \leq \frac{1-\varepsilon}{10} < \frac{1}{10}$ and thus (as $H(x)$ is increasing for $0 < x < \frac{1}{2}$)

$$(2.17) \quad H(\alpha) < H\left(\frac{1}{10}\right) < 0.47.$$

It follows that for $5 \leq q < \sqrt[4]{n}$

$$P_n(\varepsilon, q) = 2^{O(\sqrt[4]{n} \log n) + \frac{n^2 - (n-q)^2}{4} + \binom{n-q}{2} - \binom{n}{2} + 0.47qn}$$

and thus

$$(2.18) \quad \sum_{q=5}^{\sqrt[4]{n}} P_n(\varepsilon, q) \leq 2^{-0.03qn + O(\sqrt[4]{n})}.$$

Thus it remains only to consider permutations Π for which $q=2, 3$ or 4 , i. e. which interchange not more than 4 points and leave all others untouched. Let us start with the case $q=2$. The number of such permutations is clearly $\binom{n}{2}$. The number of graphs of order n admitting such a permutation as an automorphism is (as in this case $c_1=c_2=\dots=c_{n-2}=1$, $c_{n-1}=2$) $2^{\binom{n-1}{2}+1}$, and thus the probability that a random graph admits an automorphism interchanging two points is $\leq 2^{-n+O(\log n)}$. Now, if a graph G^* can be transformed by changing m of its edges into a graph G admitting the permutation Π interchanging P_j and P_k and leaving all other points invariant, we may suppose that all edges changed have either P_j or P_k (but not both) as one of their endpoints.

It is clear that we may restrict ourselves to count those graphs, which can be transformed into G by deleting edges, because any graph G^* which can be transformed in a graph, which is invariant with respect to the permutation interchanging P_j and P_k , by changing (i. e. deleting or adding) m edges, can also be transformed in such a graph by deleting m edges. Thus the number of such graphs G^* belonging to a fixed G does not exceed

$$\sum_{m < \frac{n}{2}(1-\varepsilon)} \binom{n-2}{m} = 2^{H\left(\frac{1-\varepsilon}{2}\right)n + O(\log n)}.$$

As however $H(x) < 1$ for $x \neq \frac{1}{2}$ it follows that

$$(2.19) \quad P_n(\varepsilon, 2) \leq 2^{-c(\varepsilon)n}$$

where $c(\varepsilon)$ is a positive constant depending only on ε . Let us consider now the case $q=3$. In this case clearly $c_1 = c_2 = \dots = c_{n-3} = 1$ and $c_{n-2} = 3$ and therefore the number of graphs admitting such an automorphism is

$$2^{\binom{n-2}{2}+1}.$$

As further we can select the 3 points which are moved by the permutation in $\binom{n}{3}$ ways, and the permutation itself in two ways, the probability that a graph admits as an automorphism a permutation cyclically interchanging 3 points and leaving all others unmoved, does not exceed

$$2\binom{n}{3}2^{\binom{n-2}{2}+1-\binom{n}{2}} = 2^{-2n+O(\log n)}.$$

Now if such a graph G is fixed, all graphs which can be transformed into G by changing $m < \frac{n}{2}(1-\varepsilon)$ edges (and can not be transformed into any other graph admitting the same automorphism by changing a smaller number of edges) are obtained if we choose m among the $n-3$ points left unchanged by the permutation, and select one of the three edges connecting this point with the 3 points moved by the permutation and delete or add this edge according to whether it is or is not contained in G . Thus the number of graphs which can in this way be transformed into G is $\sum_{m < \frac{n}{2}(1-\varepsilon)} \binom{n-3}{m} 3^m = O(2^n 3^{\frac{n}{2}(1-\varepsilon)})$. Besides this, we may change some

of the 3 edges between the 3 points moved by the permutation. As the number of ways doing this is 8 we obtain that

$$(2.20) \quad P_n(\varepsilon, 3) = O\left(\left(\frac{\sqrt{3}}{2}\right)^n\right).$$

Let us consider finally the case $q=4$. Here two cases have to be distinguished: either $c_1 = c_2 = \dots = c_{n-4} = 1$ and $c_{n-3} = 4$ or $c_1 = c_2 = \dots = c_{n-4} = 1$ and $c_{n-3} = c_{n-2} = 2$. For the first case we obtain

$$\sum_{1 \leq a < b \leq r} (c_a, c_b) + \sum_{a=1}^r \left\lfloor \frac{c_a}{2} \right\rfloor = \binom{n-3}{2} + 2$$

for the second

$$\sum_{1 \leq a < b \leq r} (c_a, c_b) + \sum_{a=1}^r \left\lfloor \frac{c_a}{2} \right\rfloor = \binom{n-2}{2} + 3.$$

Thus the probabilities of a graph admitting such an automorphism are $\leq 6\binom{n}{4}2^{\binom{n-3}{2}+2-\binom{n}{2}} = 2^{-3n+O(\log n)}$ and $\leq 6\binom{n}{4}2^{\binom{n-2}{2}+3-\binom{n}{2}} = 2^{-2n+O(\log n)}$, respectively. As regards the number of graphs which can be transformed into a given graph G invariant with respect to a fixed permutation of the mentioned types by changing not more than $\frac{n}{2}(1-\varepsilon)$ edges, we obtain in the first case an upper bound

of order

$$\sum_{m \leq \frac{n(1-\varepsilon)}{2}} \sum_{l \leq \frac{m}{2}} \binom{n-4}{l} \binom{n-4-l}{m-2l} 6^l 4^{m-2l} \leq 2^{1.82n+6(\log n)}$$

and in the second case an upper bound of order

$$\sum_{l \leq m \leq \frac{n(1-\varepsilon)}{2}} \binom{n-4}{l} \binom{n-4}{m-l} 2^m \leq 2^{1.32n+O(\log n)}.$$

It follows that

$$(2.21) \quad P_n(\varepsilon, 4) \leq 2^{-0.68n+O(\log n)}.$$

Collecting the estimates (2.15), (2.18), (2.19), (2.20) and (2.21) in view of (2.4) Theorem 2 follows.

§ 3. Symmetries of infinite graphs

Let Γ_∞ denote a random infinite graph which has the vertices P_n ($n=1, 2, \dots$) and which is such that denoting by $E_{j,k}$ the event that P_j and P_k are connected by an edge ($j \neq k$) the events $E_{j,k}$ ($j, k=1, 2, \dots; j < k$) are independent and $P(E_{j,k}) = \frac{1}{2}$. We shall prove that with probability one Γ_∞ admits non-trivial automorphisms. We can construct such an automorphism as follows.

Let us denote by $A(k)$ the index of the vertex into which the automorphism carries over the vertex P_k . We put $A(1)=2$ and $A(2)=1$.

Now let us consider P_3 . This vertex can be in 4 possible relations with P_1 and P_2 (connected with both; connected with P_1 but not with P_2 ; connected with P_2 but not with P_1 ; connected neither with P_1 nor with P_2). Let $A(3)$ be the least integer (if there exists any) for which $P_{A(3)}$ is in the same relation with P_2 and P_1 as P_3 with P_1 and P_2 and put $A(A(3))=3$. If $A(n)$ is already defined for any finite number of values of n , for instance if $A(n_j)=n'_j$ and $A(n'_j)=A(n_j)$ ($j=1, 2, \dots, s$) where $n_1, n_2, \dots, n_s, n'_1, n'_2, \dots, n'_s$ are different integers, let m denote the least integer for which $A(m)$ is not yet defined. Let us define $A(m)$ as the least integer different from m and from all values n for which $A(n)$ is already defined, for which $P_{A(m)}$ is in the same relation with $P_{n'_j}$ as P_m with P_{n_j} , and in the same relation with $P_{n'_j}$ as P_m with $P_{n'_j}$ ($j=1, 2, \dots, s$), and put $A(A(m))=m$.

In this way a non-trivial automorphism of Γ_∞ is constructed step-by-step, provided that the construction can always be continued. But it is easy to see that with probability 1 the construction can always be continued. This follows from the following

LEMMA 3. *Let $i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_l$ be arbitrary different natural numbers. Then with probability 1 the number of vertices P_n which are connected in Γ_∞ with each of $P_{i_1}, P_{i_2}, \dots, P_{i_k}$ and not connected with $P_{j_1}, P_{j_2}, \dots, P_{j_l}$ is infinite for every choice of the indices $i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_l$ ($k, l=1, 2, \dots$).*

PROOF of Lemma 3. The probability of the event E_n that P_n is in the required relation with all vertices $P_{i_1}, \dots, P_{i_k}, P_{j_1}, \dots, P_{j_l}$ is clearly equal to $\frac{1}{2^{k+l}}$, further these events E_n are independent. Thus by the Borel-Cantelli lemma E_n takes place for an infinity of values of n with probability 1. As the union of a denumerable set of sets of probability 0 has probability 0 too, with probability 1 in Γ there are infinitely many vertices connected with the vertices $P_{i_1}, \dots, P_{i_k}$ and not connected with the vertices $P_{j_1}, \dots, P_{j_l}$ simultaneously for all choices of the indices $i_1, i_2, \dots, i_k, j_1, \dots, j_l$. This proves Lemma 3.

Thus we have proved that with probability 1 Γ_∞ admits a non-trivial automorphism, which moreover is involutory (i. e. $A(A(n))=n$ for every n).

This is what we wanted to prove. It can be seen from the proof that Γ_∞ admits with probability 1 an infinity of nontrivial automorphisms. As a matter of fact, instead of putting $A(1)=2$, we could have prescribed $A(1)=k$ with an arbitrary k .

It is easy to see, that our result remains also valid if instead of supposing that the edge $\widehat{P_j P_k}$ is contained in Γ_∞ with probability $\frac{1}{2}$, we suppose only that this probability $p_{j,k}$ is contained between the limits δ and $1-\delta$ where $0 < \delta < 1$, admitting that this probability should depend on j and k . The result holds also if $p_{j,k}$ is not bounded away from 0 and 1 but is such that the series

$$\sum_{n=1}^{\infty} p_{i_1,n} p_{i_2,n} \dots p_{i_k,n} (1 - p_{j_1,n}) \dots (1 - p_{j_l,n})$$

is divergent for every choice of the integers $i_1, \dots, i_k, j_1, \dots, j_l$.

§ 4. Asymmetry of graphs of order n with a fixed number N of edges

In this § we consider only such graphs of order n which contain exactly N edges. If the valencies of the vertices $P_1, \dots, P_n$ are denoted by $v_1, \dots, v_n$ then we have by supposition

$$(4.1) \quad \sum_{i=1}^n v_i = 2N.$$

For such a graph we have by Cauchy's inequality

$$(4.2) \quad \sum_{i=1}^n v_i^2 \geq \frac{1}{n} \left(\sum_{i=1}^n v_i \right)^2 = \frac{4N^2}{n}.$$

Thus it follows from (1.3) and (1.4) that for such a graph

$$(4.3) \quad A[G] \geq \frac{4N}{n} - \frac{8N^2}{n^2(n-1)}.$$

Thus we have proved the following

THEOREM 3. *If a graph G of order n has $N = \lambda n$ edges $\left(0 < \lambda < \frac{n-1}{2}\right)$ then*

$$(4.4) \quad A[G] \leq 4\lambda \left(1 - \frac{2\lambda}{n-1}\right).$$

(The maximum of the right hand side of (4.4) is clearly attained if $\lambda = \frac{n-1}{4}$, in which case it is equal to $\frac{n-1}{2}$).

We can prove with the same probabilistic method as applied in § 2 combined with methods of our paper [7] that the estimate (4.4) is asymptotically best possible if together with $n \rightarrow +\infty$ we have $\lambda \rightarrow +\infty$ in such a way that $\lim_{n \rightarrow +\infty} \frac{\lambda}{\log n} = +\infty$; moreover $A[G]$ is near to $4\lambda \left(1 - \frac{2\lambda}{n-1}\right)$ for most graphs of order n having $N = \lambda n$ edges.

The meaning of the condition $\lim_{n \rightarrow +\infty} \frac{\lambda}{\log n} = +\infty$ is that as we have shown in [7] in a random graph of order n and having $N = \lambda n$ edges the valencies of all vertices are asymptotically equal with probability tending to 1 for $n \rightarrow \infty$ if $\frac{\lambda}{\log n} \rightarrow +\infty$.

§ 5. Further remarks and unsolved problems

The following problems, closely connected with that considered in § 4 can be raised: for a fixed positive integer k , and $n > 2k + 1$ determine the least value $F(n, k)$ such that there exists a graph G of order n , having $N = F(n, k)$ edges and asymmetry $A[G] = k$; further the least value $C(n, k)$ such that there exists a *connected* graph G of order n , having $N = C(n, k)$ edges, and asymmetry $A[G] = k$. We can not give a full answer to these questions, only some partial results. We prove first

THEOREM 4. *We have $C(6, 1) = 6$ and $C(n, 1) = n - 1$ for $n \geq 7$.*

REMARK. As shown in the introduction each graph of order ≤ 5 is symmetric, thus $C(n, 1)$ is defined only for $n \geq 6$.

PROOF of Theorem 4. For $n = 6$ there are, as we have seen, in the introduction, four types of asymmetric graphs, each having the asymmetry 1; as shown by Fig. 3 among these there is one having 6 edges, the others have 7 edges or more. Thus $C(6, 1) = 6$. As any connected graph G of order n has at least $n - 1$ edges, clearly $C(n, 1) \geq n - 1$ for $n \geq 7$ with equality only if there exists an asymmetric tree of order n . Now it is easy to see that for any $n \geq 7$ there exists an asymmetric tree of order n ; such a tree for $n = 7$ is shown by Fig. 8; for any $n \geq 7$, such a tree T_n can be obtained as fol-

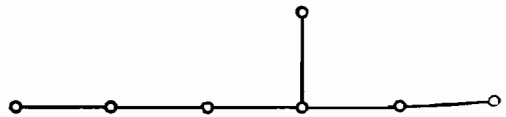


Fig. 8

lows: Let T_n consist of the vertices $P_1, \dots, P_n$ and the edges $\widehat{P_i P_{i+1}}$ ($i=1, 2, \dots, n-2$) and of the edge $\widehat{P_{n-3} P_n}$.

Thus Theorem 4 is proved. Let us add that the asymmetry of a tree can not exceed 1. As a matter of fact, let T be an arbitrary tree; we may suppose that T has at least 3 vertices, as a tree of order 2 is evidently symmetric. Let us consider a longest path with any fixed starting point P_1 in T and let P_2 be the endpoint of this path. Let P_3 be the (unique) vertex which is connected with P_2 in T . Then two cases are possible. Either $P_3 = P_1$, in this case T is a star with center P_1 , and thus is evidently symmetric; or $P_3 \neq P_1$, then again two cases are possible. Either P_3 has valency 2; in this case let P_4 be the unique vertex connected with P_3 besides P_2 ; by omitting from T the edge $P_3 P_4$ we obtain a graph which has the symmetry interchanging P_2 and P_3 . If P_3 has valency larger than 2, then any vertex P_i connected with P_3 which is not on the path $P_1 P_2$ has valency 1 because otherwise the path $P_1 P_2$ would not be the longest. In this case the tree itself is symmetric as it is invariant under the permutation interchanging P_2 and P_i . As P_1 has been chosen arbitrarily, we have incidentally proved the following

THEOREM 5. *Let T be a tree of order $n \geq 3$; let us select one of the vertices of T , say P_1 . Then either there exists a nontrivial permutation Π of the vertices of T which does not move P_1 and under which T is invariant, or one can transform T into a graph having such an automorphism by omitting one of its edges.*

We do not know the exact value of $F(n, 1)$. It is an interesting question also what is the total number of non-isomorphic asymmetric trees of order n ? We can not answer this question; we can prove however that in a certain sense „almost all” trees of order n are symmetric, if n is large. This is a consequence of Theorem 6 below. Before formulating this theorem we introduce the following definition. If a graph G contains two vertices P_1, P_2 of valency 1 which are connected with the same vertex P_3 , we shall say that G contains the cherry $\widehat{P_1 P_3 P_2}$.

A graph containing a cherry is evidently symmetric, as it is invariant under the permutation which interchanges the two vertices of order 1. Thus our assertion that almost all trees of order n are symmetric if n is large, is contained in the following

THEOREM 6. *Let us choose at random a tree from the set of all possible trees which can be formed from a given set of n labelled vertices, so that each of these trees should have the same probability to be chosen. Let γ_n denote the probability that the random tree contains at least one cherry. Then we have*

$$\lim_{n \rightarrow +\infty} \gamma_n = 1.$$

PROOF of Theorem 6. Let $P_1, \dots, P_n$ denote the vertices of our random tree T_n . Let us put $\varepsilon(i_1, i_2, j) = 1$ (i_1, i_2, j are different natural numbers not exceeding n) if $\widehat{P_{i_1} P_j P_{i_2}}$ is a cherry in the random tree, i. e. if P_{i_1} and P_{i_2} have the valency 1 in T_n and if both are connected in T_n with P_j ; let us put $\varepsilon(i_1, i_2, j) = 0$ otherwise. Taking into account that according to a well-known theorem of A. CAYLEY [8] the total number of trees which can be formed from n given labelled vertices is equal

to n^{n-2} , we obtain that

$$(5.1) \quad M(\varepsilon_{i_1, i_2, j}) = \frac{(n-2)^{n-4}}{n^{n-2}}$$

and

$$(5.2) \quad M(\varepsilon(i_1, i_2, j_1)\varepsilon(i_3, i_4, j_2)) = \begin{cases} \frac{(n-6)^{n-6}}{n^{n-2}} & \text{if } i_1, i_2, i_3, i_4, j_1, j_2 \\ & \text{are all different,} \\ \frac{(n-5)^{n-6}}{n^{n-2}} & \text{if } j_1 = j_2 = j \text{ and } i_1, i_2, i_3, i_4 \\ & \text{are different,} \end{cases}$$

$$(5.3) \quad M(\varepsilon(i_1, i_2, j_1)\varepsilon(i_3, i_4, j_2)) = \begin{cases} \frac{(n-3)^{n-4}}{n^{n-2}} & \text{if } i_1 = i_3, i_2 = i_4 \text{ and } j_1 = j_2 \\ & \text{or } i_1 = i_4, i_2 = i_3 \text{ and } j_1 = j_2 \\ 0 & \text{otherwise.} \end{cases}$$

Let Γ_n denote the number of cherries in T_n . Then by (5.1), (5.2) and (5.3) we obtain

$$M(\Gamma_n) = \frac{n}{2e^3} + O(1)$$

and

$$M(\Gamma_n^2) = \frac{n^2}{4e^6} + O(n)$$

and thus

$$D^2(\Gamma_n) = O(n).$$

It follows by the inequality of Chebyshev that for $n \geq n_0$

$$1 - \gamma_n = O\left(\frac{1}{n}\right).$$

Thus Theorem 6 is proved.

Now we prove the following

THEOREM 7. *Any connected graph of order n having n edges is either symmetric, or its asymmetry is equal to 1.*

REMARK. By other words we have $C(n, 2) > n$ for $n \geq 7$ (As we have seen any graph of order ≤ 6 is either symmetric or has the asymmetry 1.)

PROOF of Theorem 7. Any connected graph of order n having n edges has as well known the following structure: it contains exactly one cycle, and any vertex of this cycle may be the root of one or more trees. Now suppose that contrary to the assertion of Theorem 7 there exists a graph G of order n having n edges, for which $A[G] \geq 2$. In such a graph any tree attached to a vertex of the single cycle of the graph consists of a single edge only, because otherwise by Theorem 5 we would have $A[G] \leq 1$. Let us call such an edge a „thorn”. We can exclude the case when to a vertex two or more thorns are attached, because two thorns make a cherry which admits a symmetry. Now if to a vertex P of the cycle a thorn PQ is attached, then necessarily a thorn has to be attached to both neighbouring verti-

ces of the cycle too, because if P' would be a neighbour of P which is not the starting point of a thorn, then if P'' is the other neighbour of P' in the cycle by omitting the edge $P'P''$ we would obtain a graph containing a cherry $\widehat{QPP'}$. Thus either a thorn is attached to all vertices of the cycle or to none of them. As in both cases the graph has a cyclic symmetry, we obtained a contradiction, which proves Theorem 7.

It can be shown by a similar argument that $C(n, 2) > n + 1$.

Our last result is a lower estimate for $F(n, 3)$. We prove

THEOREM 8. We have $F(n, 3) \geq \frac{4n}{3} - \frac{3}{2}$.

PROOF. Let G be a graph of order n having N edges for which $A[G] = 3$. Clearly G can contain only a single vertex having the valency 1. Let n_2 be the number of vertices of G of valency 2 and n_3 the number of vertices of G of valency ≥ 3 . Clearly two vertices P_1, P_2 of valency 2 can not be connected by an edge, because if P_1 and P_2 were connected by an edge, and P_1 would be connected besides P_2 with P'_1 and P_2 besides P_1 with P'_2 , then omitting the edges $\widehat{P_1P'_1}$ and $\widehat{P_2P'_2}$ the resulting graph would admit the symmetry consisting in interchanging P_1 and P_2 .

Further no vertex with valency ≥ 3 can be connected with more than one vertex with valency 2; as a matter of fact if P_1 and P_2 were vertices with valency 2 connected with a vertex P_3 with valency ≥ 3 , then omitting the two edges connecting the vertices P_1 and P_2 with vertices different from P_3 the resulting graph would contain the cherry $\widehat{P_1P_3P_2}$.

It follows that $n_3 \geq 2n_2 - 1$. As on the other hand $n_2 + n_3 \leq n - 1$, we obtain $3n_3 \leq 2n - 3$. Now we have

$$2N \geq 2n_2 + 3n_3 \geq 2n - 2 + n_3 \geq \frac{8n - 9}{3}$$

and therefore $N \geq \frac{8n - 9}{6} = \frac{4n}{3} - \frac{3}{2}$.

Finally we mention a further unsolved problem: is it true that $C(n, k) = F(n, k)$ for $k \geq 2$?

Remarks, added on November 8, 1963. Prof. R. C. BOSE kindly informed us that in a forthcoming paper he introduced a class of graphs, called by him *strongly regular* graphs, which contains the class of Δ -graphs discussed in the present paper, as a subclass. A graph of order n is called strongly regular with parameters n, p_1, p_2 if each vertex of G_n is joined with n_1 other vertices, further any two joined vertices are both joined to exactly p_1 vertices and any two unjoined vertices are both joined to exactly p_2 other vertices. Clearly a Δ -graph of order $n \equiv 1 \pmod{4}$ is a strongly regular graph with parameters $n_1 =$
 $= p_1 = p_2 = \frac{n - 1}{2}$.

The notion of strongly regular graphs is closely connected with the concept of an association scheme with two associate classes introduced by R. C. BOSE and T. SHIMAMOTO in their paper: Classification and analysis of partially balanced

incomplete block designs with two associate classes (*Journal of the American Statistical Association*, **47** (1952), pp. 151-184).

We should like to add further that the Δ -graph of order p constructed on p. 301 is identical with the graph constructed by H. SACHS on p. 282 of his paper: Über selbstkomplementäre Graphen (*Publicationes Mathematicae*, **9** (1962), pp. 270-288). This paper was not known to us at the time when our paper was written. As shown by H. SACHS, this graph is isomorphic with its complementary graph.

References

- [1] O. PERRON, Bemerkung über die Verteilung der quadratischen Reste, *Mathematische Zeitschrift*, **56** (1952), pp. 122-130.
- [2] J. B. KELLY, A characteristic property of quadratic residues, *Proceedings of the American Mathematical Society*, **5** (1954), pp. 38-46.
- [3] A. RÉNYI, On the measure of equidistribution of point sets, *Acta Sci. Math. Szeged*, **13** (1949), pp. 77-92.
- [4] A. W. GOODMAN, On sets of acquaintances and strangers at any party, *American Math. Monthly*, **66** (1959), pp. 778-783.
- [5] I. L. SAUVÉ, On chromatic graphs, *American Math. Monthly*, **68** (1961), pp. 107-111.
- [6] P. ERDŐS, On the number of triangles contained in certain graphs, *Bulletin of the Research Council of Israel*, Section F. (in print).
- [7] P. ERDŐS and A. RÉNYI, On the evolution of random graphs, *Publications of the Math. Inst. Hung. Acad. Sci.*, **5** (1960), pp. 17-61.
- [8] A. CAYLEY, A theorem on trees, *Quarterly Journal of Pure and Applied Math.*, **23** (1889), pp. 376-378.
- [9] A. RÉNYI, Some remarks on the theory of trees, *Publ. Math. Inst. Hung. Acad. Sci.*, **4** (1959), pp. 73-85.
- [10] A. RÉNYI, On connected graphs, *Publ. Math. Inst. Hung. Acad. Sci.*, **4** (1959), pp. 385-388.

NOTE

Quintas [1] determined $F(n, 1)$ asked in No. 216. Let us remind that $F(n, k)$ was the minimal number of edges of a graph of n vertices and of asymmetry k . In the expression for $F(n, 1)$ the number of asymmetric trees [2] is used. Quintas determined also the maximal number of edges of a graph having n vertices and asymmetry $\neq 0$. Both the minima and maxima are determined for the following three further classes of graphs: connected graphs, topological graphs (there is no vertex with valency 2), connected topological graphs. In [1] the estimation of Theorem 3 of No. 216. is improved. On the other hand the concept of positive asymmetry $A^+[G]$ is introduced as the least number of edges which when adjoined to G yields a symmetric graph. $A^-[G]$ is defined similarly by deleting edges. [1] contains estimations for $A^+[G]$ and $A^-[G]$.

Baron [4] determined the minimal and maximal values of edges of a graphs of n vertices and of asymmetry > 0 for other classes, too. E.g. the class of graphs having no end-edges or the class planar graphs and some combinations.

The case of regular graphs is solved in [5], [6] and [7]. All the pairs (n, v) are determined for which there exist regular asymmetric graphs with n vertices and with valency v .

Baron [4] and Nešetřil [3] independently gave a negative answer to the last question of No. 216. $C(n, 2) = n + 2$, $F(n, 2) = n + 1$ if $n \geq 21$, thus $C(n, k) = F(n, k)$ does not hold for $k = 2$. Moreover, Nešetřil [3] tried to determine how many edges an asymmetric graph can have if the number of vertices is fixed, and $A[G] > 1$ is supposed. He has partial results.

Nešetřil [3] also proved, that for any infinite cardinal n we can have asymmetry > 0 in a graph with n vertices and m edges iff $n = m$. Moreover, there is always a graph with asymmetry-number n . Baron [4] proved the same adding the additional condition, that the graph is regular.

Weichsel [8] gives an algorithm for deciding whether a graph is asymmetric or not. In [9] Nešetřil considers the asymmetry of trees. (Gy. K.)

REFERENCES

- [1] Quintas, L. V.: Extrema concerning asymmetric graphs. *J. Combinatorial Theory*, **3** (1967), 57–82.
- [2] Harary, F. and Prins, G.: The number of homeomorphically irreducible trees and other species. *Acta Math.*, **101** (1959), 141–162.
- [3] Nešetřil, J.: Graphs with small asymmetries. *Comm. Math. Univ. Carolinae*, **11** (1970), 403–419.
- [4] Baron, G.: Über asymmetrische Graphen. *Math. Nachr.*, **46** (1970), 25–46.
- [5] Baron, G. and Imrich, W.: Asymmetrische reguläre Graphen. *Acta Math. Acad. Sci. Hung.*, **20** (1969), 135–142.
- [6] Baron, G.: Asymmetrische reguläre Graphen II. *Acta Math. Acad. Sci. Hung.*, **22** (1971/72), 1–4.
- [7] Izbicki, H.: Über asymmetrische reguläre Graphen. *Monatshefte f. Math.*, **LXXIII** (1969), 112–125.
- [8] Weichsel, P. M.: A note on asymmetric graph. *Israel J. Math.*, **10** (1971), 234–243.
- [9] Nešetřil, J.: A congruence theorem for asymmetric trees. *Pacific J. Math.*, **37** (1971), 771–778.

Über die konvexe Hülle von n zufällig gewählten Punkten. II

Von

A. RÉNYI und R. SULANKE

Einleitung

Der vorliegende Artikel ist eine Fortsetzung unserer Arbeit [I]. Wir betrachten einen endlichen konvexen Bereich K der Ebene. Seien P_i ($i = 1, 2, \dots, n$) n zufällige Punkte aus K , die unabhängig voneinander nach der Gleichverteilung gewählt werden. Durch H_n bezeichnen wir die konvexe Hülle der P_i , durch L_n die Länge des Umfanges von H_n und durch F_n den Flächeninhalt von H_n . Es ist klar, daß die mathematischen Erwartungen $E(L_n)$ bzw. $E(F_n)$ für $n \rightarrow +\infty$ gegen den Umfang L bzw. den Flächeninhalt F von K streben. Die Güte dieser Konvergenz soll im Folgenden untersucht werden.

In § 1 werden zunächst die allgemeinen Formeln zur Berechnung von $E(L_n)$ und $E(F_n)$ aufgestellt. Danach beginnen wir mit der Betrachtung des Falls, daß K eine genügend oft stetig differenzierbare Randkurve besitzt, deren Krümmung $k = k(s)$ positiv und beschränkt ist: $0 < k(s) < A$ (s bedeutet die Bogenlänge). Die in § 2 aufgestellten Näherungsformeln gestatten es uns, die Randkurve von K in der Umgebung eines ihrer Punkte durch ihren Schmiegekreis zu ersetzen. Mit Hilfe dieser Formeln gelingt es dann in § 3, das asymptotische Verhalten von $E(L_n)$ und $E(F_n)$ in dem genannten Fall zu ermitteln. Es erweist sich, daß die Abweichungen $L - E(L_n)$ und $F - E(F_n)$ beide die Gestalt $\text{const. } n^{-2/3} + o(n^{-1})$ haben; für den Flächeninhalt ist hierbei die äquiaffine Länge des Randes von K der wesentliche Teil der im Hauptglied stehenden Konstanten; im Falle des Umfanges jedoch tritt das Funktional

$$Q(K) = \int_0^L (k(s))^{4/3} ds$$

auf, das bisher in der Geometrie anscheinend noch nicht untersucht wurde. Es wäre interessant, für $Q(K)$ eine isoperimetrische Aufgabe zu behandeln.

Die Untersuchung der analogen Probleme für konvexe Polygone führte auf ziemlich unübersichtliche Rechnungen. Aus diesem Grunde betrachten wir in § 4 nur den Fall, daß K ein Quadrat ist. Hier ergibt sich die auf den ersten Blick überraschende Tatsache, daß sich Flächeninhalt und Umfang asymptotisch verschieden verhalten. Während für den Umfang die Abweichung

$$L - E(L_n) = \text{const. } n^{-1/2} + o(n^{-1})$$

größer ist als im glatten Fall, gilt für den Flächeninhalt

$$F - E(F_n) = \text{const. } \frac{\ln n}{n} + o(n^{-1});$$

diese Approximation ist also bedeutend besser als die entsprechende für einen Eibereich mit glattem Rand.

§ 1. Formeln für $E(L_n)$ und $E(F_n)$

Sei wieder $\varepsilon_{ij} = 1$, wenn $i \neq j$ und $\overline{P_i P_j}$ Randstrecke von H_n ist, und $\varepsilon_{ij} = 0$ sonst. Durch $|P_i P_j|$ bezeichnen wir den Abstand der Punkte P_i, P_j . Dann gilt

$$(1) \quad L_n = \sum_{i < j} |P_i P_j| \varepsilon_{ij}.$$

Hieraus erhält man unmittelbar $E(L_n) = \binom{n}{2} E(|P_1 P_2| \varepsilon_{12})$, also

$$(2) \quad E(L_n) = \binom{n}{2} \frac{1}{F^n} \int \cdots \int |P_1 P_2| \varepsilon_{12} dP_1 \dots dP_n.$$

Führen wir die Integration über $P_3, \dots, P_n$ aus, so ergibt sich

$$(3) \quad E(L_n) = \binom{n}{2} \frac{1}{F^2} \iint |P_1 P_2| \left\{ \left(1 - \frac{f}{F}\right)^{n-2} + \left(\frac{f}{F}\right)^{n-2} \right\} dP_1, dP_2;$$

dabei ist f der durch die Gerade $g(P_1, P_2)$ von K abgeschnittene kleinere Flächeninhalt, also $f/F \leq 1/2$. Somit gilt

$$(4) \quad E(L_n) \sim \frac{\binom{n}{2}}{F^2} \iint \left(1 - \frac{f}{F}\right)^{n-2} |P_1 P_2| dP_1 dP_2.$$

Wir führen jetzt mit denselben Bezeichnungen wie in [1], (41), die Transformation

$$(5) \quad dP_1 dP_2 = |t_1 - t_2| dt_1 dt_2 dp d\varphi$$

durch. Wegen $|t_1 - t_2| = |P_1 P_2|$ und

$$(6) \quad \iint_{g(p, \varphi) \cap K} |t_1 - t_2|^2 dt_1 dt_2 = \frac{l^4}{6}$$

wobei $l = l(p, \varphi)$, die Länge der Sehne $g(p, \varphi) \cap K$ bezeichnet, erhalten wir

$$(7) \quad E(L_n) \sim \frac{\binom{n}{2}}{6 F^2} \int_0^{2\pi} \int_0^{p(\varphi)} \left(1 - \frac{f}{F}\right)^{n-2} l^4 dp d\varphi.$$

Hierbei ist $p(\varphi)$ die Stützfunktion des Bereiches K ; als Koordinatenursprung wählen wir den Schwerpunkt von K .

Bezeichne nun $p(P_i, P_j)$ den Abstand der Geraden $g(P_i, P_j)$ vom Ursprung 0. Für den Flächeninhalt von H_n gilt dann

$$(8) \quad F_n = \frac{1}{2} \sum_{i < j} \varepsilon_{ij} |P_i P_j| p(P_i, P_j).$$

Durch ganz analoge Überlegungen wie im Falle des Umfanges erhalten wir

$$(9) \quad E(F_n) \sim \frac{\binom{n}{3}}{12 F^2} \int_0^{2\pi} \int_0^{p(\varphi)} \left(1 - \frac{f}{F}\right)^{n-2} l^4 p dp d\varphi.$$

§ 2. Die Approximation durch den Schmiegekreis

Unsere Aufgabe besteht jetzt darin, die Integrale (7) und (9) auszuwerten. In diesem und dem folgenden Paragraphen setzen wir voraus, daß K einen glatten Rand mit einer Krümmung $k(s)$, $0 < k(s) < A$ besitzt. Wir halten zunächst φ

fest und führen die Integration nach p aus. Da für das asymptotische Verhalten der Integrale offenbar nur der Anteil wichtig ist, für den f/F klein ist, können wir die Größen l, f von K durch die entsprechenden Größen $\bar{l}, \bar{f}$ desjenigen Schmiegkreises ersetzen, der mit K die Tangente $g(p(\varphi), \varphi)$ gemeinsam hat. Die Fehler, die bei dieser Ersetzung entstehen, sollen jetzt abgeschätzt werden. Dabei werden sich Verbesserungen der Formeln [1], (47) ergeben.

Anstelle von p führen wir den neuen Parameter β ein, welcher der halbe Zentriwinkel vom Zentrum Z des Schmiegkreises S_φ auf die Sehne $g(p, \varphi) \cap S_\varphi$ ist. Dann gilt (vgl. Fig. 1)

$$(10) \quad p = r(\cos \beta - 1) + p(\varphi).$$

Hierbei bezeichnet r den Krümmungsradius: $r = 1/k$. Auf der Geraden $g(\beta, \varphi)$ führen wir die Bogenlänge t als Parameter ein und bezeichnen durch t_1^-, t_1^+ die Parameter der Schnittpunkte von g mit S_φ , durch t_2^-, t_2^+ die Parameter der Schnittpunkte von g mit dem Rand von K . Wählen wir die Mitte der Sehne $g \cap S_\varphi$ als Nullpunkt der Bogenlänge t , so folgt unmittelbar

$$(11) \quad t_1^- = -r \sin \beta, \quad t_1^+ = r \sin \beta.$$

Wir wollen jetzt t_2^-, t_2^+ als Funktionen von β berechnen. Zu diesen Zweck stellen wir den Rand von K in einer Umgebung des betrachteten Punktes im begleitenden Zweibein dar. Sei $\mathbf{r}(s)$ der Ortsvektor eines variablen Punktes der Randkurve vom Berührungspunkt aus, $\mathbf{t}$ ein Tangentialvektor und $\mathbf{n}$ der Normalvektor in diesem Punkt. Wählen wir den Berührungspunkt gleichzeitig als Nullpunkt der Bogenlänge s der Randkurve, so ergibt sich aus der Taylorschen Formel unter Berücksichtigung der Frenetschen Formeln der ebenen Differentialgeometrie die folgende Darstellung:

$$(12) \quad \begin{aligned} \mathbf{r}(s) = & \mathbf{t} \cdot \left\{ s - k^2 \frac{s^3}{3!} - 3kk' \frac{s^4}{4!} + 0(s^5) \right\} + \\ & + \mathbf{n} \left\{ k \frac{s^2}{2!} + k' \frac{s^3}{3!} + (k'' - k^3) \frac{s^4}{4!} + 0(s^5) \right\}. \end{aligned}$$

Die Koeffizienten sind hierbei an der Stelle $s = 0$ zu nehmen; Striche bedeuten Differentiation nach der Bogenlänge. Die Gerade $g(\beta, \varphi)$ hat in diesem Koordinatensystem die Parameterdarstellung

$$(13) \quad \mathbf{z}(t) = \mathbf{t} \cdot t + \mathbf{n} \cdot r(1 - \cos \beta).$$

Der Vergleich mit (12) liefert uns die beiden Beziehungen

$$(14) \quad t_2 = s - k^2 \frac{s^3}{3!} - 3kk' \frac{s^4}{4!} + 0(s^5),$$

$$(15) \quad r(1 - \cos \beta) = k \frac{s^2}{2!} + k' \frac{s^3}{3!} + (k'' - k^3) \frac{s^4}{4!} + 0(s^5).$$

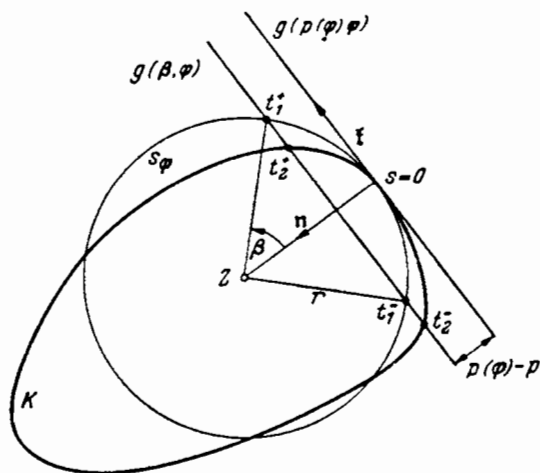


Fig. 1

Aus (15) erhalten wir s als Funktion von β :

$$(16) \quad s = r\beta - \frac{k' r^3 \beta^2}{3!} + \frac{r^4}{4!} \left\{ \frac{5}{3} k'^2 r - k'' \right\} \beta^3 + O(\beta^4).$$

Setzen wir dies in (14) ein, so folgt

$$(17) \quad t_2 = r\beta - \frac{k' r^3}{3!} \beta^2 + \left\{ \frac{5}{4!3} r^5 k'^2 - \frac{r^4 k''}{4!} - \frac{r}{3!} \right\} \beta^3 + O(\beta^4);$$

dabei gilt offenbar $t_2^- = t_2(-\beta)$, $t_2^+ = t_2(\beta)$ bei $\beta \geq 0$. Aus der Potenzreihenentwicklung von $\sin \beta$ und (11) ergibt sich

$$(18) \quad t_1 - t_2 = \frac{k' r^3}{3!} \beta^2 + \frac{r^4}{4!} \left\{ k'' - \frac{5}{3} r k'^2 \right\} \beta^3 + O(\beta^4);$$

hierbei erhalten wir wieder $t_1^+ - t_2^+$ für positives β und $t_1^- - t_2^-$ für negatives β .

Wir beachten nun, daß der Schmiegekreis einer Kurve in einem Punkt, der kein Scheitelpunkt ist, für den also $k' \neq 0$ gilt, die Kurve im Berührungspunkt durchsetzt, wie es auch unsere Abbildung zeigt. Hieraus folgt $l - \bar{l} = (t_1^- - t_2^-) - (t_1^+ - t_2^+)$, also

$$(19) \quad l - \bar{l} = \frac{r^4}{12} \left(\frac{5}{3} r k'^2 - k'' \right) \beta^3 + O(\beta^4).$$

Weil in einem Scheitelpunkt $k' = 0$ ist und eine Berührung von mindestens dritter Ordnung mit dem Schmiegekreis vorliegt, gilt (19) in diesem Fall erst recht; dies erkennt man auch unmittelbar aus (18).

Für die Flächeninhalte $f, \bar{f}$ ergibt sich durch Auswertung des Integrals

$$f - \bar{f} = \int_p^{p(\varphi)} (l - \bar{l}) dp$$

die folgende Näherungsformel:

$$(20) \quad f - \bar{f} = \frac{r^5}{60} \left(\frac{5}{3} r k'^2 - k'' \right) \beta^5 + O(\beta^6).$$

§ 3. Berechnung von $E(L_n)$ und $E(F_n)$ für einen Eibereich mit glattem Rand

Wir gehen zum Zentriwinkel $\alpha = 2\beta$ über und drücken die Integrale (7) und (9) durch α und φ aus. Wegen

$$(21) \quad l = 2r \sin \frac{\alpha}{2} \quad \text{und} \quad \bar{f} = \frac{r^2}{2} (\alpha - \sin \alpha)$$

sowie

$$(22) \quad |dp| = \left(\frac{r}{2} \sin \frac{\alpha}{2} \right) |d\alpha|$$

ergibt sich aus (19)

$$(23) \quad l^4 dp = \left[\frac{r^5 \alpha^5}{4} (1 + G \alpha^2) + O(\alpha^8) \right] d\alpha$$

wobei zur Abkürzung

$$(24) \quad G = \frac{5}{4!} \left(\frac{r^4 k'^2}{3} - \frac{r^3 k''}{5} - 1 \right)$$

gesetzt wurde. Aus (20) und (21) erhalten wir

$$(25) \quad \frac{f}{F} = \frac{r^2 \alpha^3}{12 F} + \kappa \cdot \alpha^5 + O(\alpha^6)$$

wobei

$$(26) \quad \kappa = \frac{r^2}{5! 2 F} \left[\left(\frac{r}{2} \right)^3 \left(\frac{5}{3} r k'^2 - k'' \right) - 1 \right].$$

Das Integral (7) nimmt nun die Gestalt

$$(27) \quad E(L_n) \sim \frac{\binom{2}{2}}{4! F^2} \int_0^{2\pi} r^5 d\varphi \int_0^{\alpha(\varphi)} \left(1 - \frac{r^2 \alpha^3}{12 F} - \kappa \alpha^5 - 0(\alpha^6) \right)^{n-2} \times \\ \times (\alpha^5 + G \alpha^7 + 0(\alpha^8)) d\alpha$$

an. Wir berechnen zuerst die Integrale

$$(28) \quad B_\nu = \int_0^{\alpha(\varphi)} \left(1 - \frac{r^2 \alpha^3}{12 F} - \kappa \alpha^5 - 0(\alpha^6) \right)^{n-2} \alpha^\nu d\alpha.$$

Durch die Substitution

$$(29) \quad \frac{r^2 \alpha^3}{12 F} = \frac{x}{n}$$

erhalten wir unter Berücksichtigung von

$$(30) \quad \left(1 - \frac{x}{n} - \kappa_1 \left(\frac{x}{n} \right)^{5/3} + 0 \left(\left(\frac{x}{n} \right)^2 \right)^{n-2} = e^{-x} \left(1 - \frac{\kappa_1 x^{5/3}}{n^{2/3}} + 0 \left(\frac{x^2}{n} \right) \right)$$

das Integral B_ν in der Form

$$(31) \quad B_\nu = \frac{1}{3} \left(\frac{12 F}{n r^2} \right)^{(\nu+1)/3} \int_0^{n r^2 \alpha^3(\varphi)/12 F} e^{-x} \left(1 - \kappa_1 x^{5/3} n^{-2/3} + 0 \left(\frac{x^2}{n} \right) \right) x^{(\nu-2)/3} dx.$$

Hierbei wurde

$$(32) \quad \kappa_1 = \kappa \left(\frac{12 F}{r^2} \right)^{5/3}$$

gesetzt. Integrieren wir in (31) jetzt nicht nur bis zu der angegebenen oberen Grenze, sondern bis $+\infty$, so begehen wir einen Fehler exponentieller Größenordnung, der zu vernachlässigen ist. Es folgt

$$(33) \quad B_\nu = \frac{1}{3} \left(\frac{12 F}{n r^2} \right)^{(\nu+1)/3} \cdot \left[\Gamma \left(\frac{\nu+1}{3} \right) - \frac{\kappa_1}{n^{2/3}} \Gamma \left(\frac{\nu}{3} + 2 \right) \right] + 0(n^{-(\nu+4)/3}).$$

Durch Einsetzen von (33) in (27) erhalten wir

$$(34) \quad E(L_n) = L - a(K) n^{-2/3} + 0 \left(\frac{1}{n} \right).$$

Die Konstante $a(K)$ ergibt sich durch Ausrechnung von

$$(35) \quad a(K) = \Gamma \left(\frac{11}{3} \right) \int_0^{2\pi} \kappa_1 r d\varphi - (12 F)^{2/3} \Gamma \left(\frac{8}{3} \right) \int_0^{2\pi} G r^{-1/3} d\varphi$$

unter Berücksichtigung von (24), (26) und (32) in der Gestalt

$$(36) \quad a(K) = \frac{(12 F)^{2/3} \Gamma \left(\frac{8}{3} \right)}{4!} \int_0^L \left[\frac{9}{5} k^{4/3} + \frac{3}{5} k'' k^{-5/3} - k'^2 k^{-8/3} \right] ds.$$

Dabei wurde anstelle von φ die Bogenlänge s der Randkurve von K als Parameter eingeführt; es gilt ja $d\varphi = k ds$. Durch partielle Integration folgt

$$(37) \quad \frac{3}{5} \int_0^L k'' k^{-5/3} ds = \int_0^L k'^2 k^{-8/3} ds.$$

Daher erhalten wir für $a(K)$ schließlich

$$(38) \quad a(K) = \frac{1}{12} \Gamma\left(\frac{2}{3}\right) (12 F)^{2/3} \int_0^L k^{4/3} ds.$$

Zur Berechnung von $E(F_n)$ führen wir ebenfalls die Substitution (22) durch und erhalten

$$(39) \quad E(F_n) \sim \frac{\binom{2}{2}}{12 F^2} \int_0^{2\pi} \int_0^{\alpha(\varphi)} \left(1 - \frac{r^2 \alpha^3}{12 F} - \kappa \alpha^5 - O(\alpha^6)\right)^{n-2} \times \\ \times \left[\frac{p(\varphi) r^5 \alpha^5}{4} + \left(\frac{G p(\varphi) r^5}{4} - \frac{r^6}{32} \right) \alpha^7 + O(\alpha^8) \right] d\alpha d\varphi.$$

Nach (33) ergibt sich hieraus

$$(40) \quad E(F_n) = F - b(K) n^{-2/3} + O(n^{-1}).$$

Für die Konstante $b(K)$ finden wir nach einigen Rechnungen zunächst

$$(41) \quad b(K) = \frac{1}{16} \Gamma\left(\frac{8}{3}\right) (12 F)^{2/3} \sigma(K) + c(K);$$

hierbei ist

$$(42) \quad \sigma(K) = \int_0^L k^{1/3} ds$$

die äquiaffine Bogenlänge der Randkurve von K , während $c(K)$ die Gestalt

$$(43) \quad c(K) = \frac{\Gamma\left(\frac{9}{4}\right)}{4!} (12 F)^{2/3} \int_0^{2\pi} p r^{-1/3} \left(\frac{9}{10} + \frac{3}{10} r^3 k'' - \frac{1}{2} r^4 k'^2 \right) d\varphi$$

hat. Durch einen darübergesetzten Punkt bezeichnen wir jetzt die Ableitungen nach φ und drücken k' , k'' durch r , $\dot{r}$, $\ddot{r}$ aus. Es folgt

$$(44) \quad c(K) = \frac{\Gamma\left(\frac{9}{4}\right) (12 F)^{2/3}}{4! 10} \int_0^{2\pi} p (9 r^{-1/3} + 4 \dot{r}^2 r^{-7/3} - 3 \ddot{r} r^{-4/3}) d\varphi.$$

Durch zweimalige partielle Integration erhalten wir

$$(45) \quad \int_0^{2\pi} (4 \dot{r}^2 r^{-7/3} - 3 \ddot{r} r^{-4/3}) p d\varphi = 9 \int_0^{2\pi} r^{-1/3} \ddot{p} d\varphi.$$

Dies setzen wir in (44) ein. Wegen $p + \ddot{p} = r$ (vgl. z. B. W. BLASCHKE [2], S. 30) ergibt sich wiederum ein Vielfaches von $\sigma(K)$. Unter Berücksichtigung von (41) folgt schließlich

$$(46) \quad b(K) = \frac{1}{10} \Gamma\left(\frac{8}{3}\right) (12 F)^{2/3} \sigma(K).$$

Die Ergebnisse dieses Paragraphen können wir folgendermaßen zusammenfassen:

Satz 1. Sei K ein ebener, beschränkter, konvexer Bereich, dessen Randkurve genügend oft stetig differenzierbar ist. Die Krümmung $k(s)$ des Randes genüge der Ungleichung $0 < k(s) < A$. Sei L der Umfang und F der Flächeninhalt von K . Die Länge L_n der konvexen Hülle H_n von n in K unabhängig und gleichverteilt gewählten Punkten besitzt die mathematische Erwartung

$$(47) \quad E(L_n) = L - \frac{\Gamma(2/3) (12 F)^{2/3} \int_0^L k^{4/3} ds}{12 n^{2/3}} + O(n^{-1}).$$

Für die mathematische Erwartung des Flächeninhaltes F_n von H_n gilt

$$(48) \quad E(F_n) = F - \frac{\Gamma(\frac{8}{3}) (12 F)^{2/3} \sigma(K)}{10 n^{2/3}} + O(n^{-1})$$

wobei $\sigma(K)$ nach (42) die äquiaffine Länge des Randes von K bedeutet.

§ 4. Berechnung von $E(L_n)$ und $E(F_n)$ für ein Quadrat

Sei nun K ein Quadrat mit der Seitenlänge a . Den Koordinatenursprung legen wir in den Mittelpunkt von K und die Nullrichtung $\varphi = 0$ gehe von 0 zu einer Seitenmitte. Wir haben wieder die Integrale (7) und (9) auszuwerten. Aus Symmetriegründen genügt es, die Integration über φ von 0 bis $\pi/4$ auszuführen und entsprechend mit 8 zu multiplizieren. Für die Integration nach p unterscheiden wir zwei Fälle. 1. Die Gerade $g(p, \varphi)$ trifft zwei gegenüberliegende Seiten des Quadrates. Das tritt ein, wenn

$$(49) \quad 0 \leq p \leq p_1(\varphi) = \frac{a}{2} (\cos \varphi - \sin \varphi)$$

gilt. Für l und f ergibt sich

$$(50) \quad l = l(\varphi) = \frac{a}{\cos \varphi}, \quad f = f(p, \varphi) = \frac{a^2}{2} - \frac{a p}{\cos \varphi}.$$

2. Die Gerade $g(p, \varphi)$ trifft zwei aneinandergrenzende Seiten des Quadrates. In diesem Fall ist

$$(51) \quad p_1(\varphi) \leq p \leq p(\varphi) = \frac{a}{2} (\cos \varphi + \sin \varphi).$$

Ferner gilt

$$(52) \quad l = l(p, \varphi) = \frac{p(\varphi) - p}{\cos \varphi \sin \varphi}, \quad f = f(p, \varphi) = \frac{(p(\varphi) - p)^2}{2 \sin \varphi \cos \varphi}.$$

Auf Grund dieser Fallunterscheidung erscheinen die Integrale (7) und (9) jetzt als Summen

$$(53) \quad E(L_n) \sim I_1 + I_2, \quad E(F_n) \sim J_1 + J_2$$

und wir haben die folgenden vier Ausdrücke auszuwerten:

$$(54) \quad I_1 = \frac{4}{3} \binom{n}{2} \int_0^{\pi/4} \int_0^{p_1(\varphi)} \left(\frac{1}{2} + \frac{p}{a \cos \varphi} \right)^{n-2} \frac{dp d\varphi}{\cos^4 \varphi},$$

$$(55) \quad I_2 = \frac{4}{3} \frac{\binom{n}{2}}{a^4} \int_0^{\pi/4} \int_{p_1(\varphi)}^{p(\varphi)} \left(1 - \frac{(p(\varphi) - p)^2}{2 a^2 \sin \varphi \cos \varphi} \right)^{n-2} \frac{(p(\varphi) - p)^4 dp d\varphi}{\cos^4 \varphi \sin^4 \varphi},$$

$$(56) \quad J_1 = \frac{2}{3} \binom{n}{2} \int_0^{\pi/4} \int_0^{p_1(\varphi)} \left(\frac{1}{2} + \frac{p}{a \cos \varphi} \right)^{n-2} \frac{p dp d\varphi}{\cos^4 \varphi},$$

$$(57) \quad J_2 = \frac{2}{3} \frac{\binom{n}{2}}{a^4} \int_0^{\pi/4} \int_{p_1(\varphi)}^{p(\varphi)} \left(1 - \frac{(p(\varphi) - p)^2}{2 a^2 \sin \varphi \cos \varphi} \right)^{n-2} \frac{(p(\varphi) - p)^4 p dp d\varphi}{\cos^4 \varphi \sin^4 \varphi}.$$

Wir beginnen mit der Berechnung von I_1 . Durch die Substitution

$$(58) \quad p = x a \cos \varphi$$

ergibt sich

$$(59) \quad I_1 = \frac{2 n a}{3} \int_0^{\pi/4} \frac{(1 - \frac{1}{2} \operatorname{tg} \varphi)^{n-1}}{\cos^3 \varphi} d\varphi + 0(2^{-n}).$$

Substituieren wir nun

$$(60) \quad \operatorname{tg} \varphi = t$$

so erhalten wir I_1 in einer Form, die sich leicht abschätzen läßt. Es resultiert

$$(61) \quad I_1 = \frac{4 a}{3} + 0\left(\frac{1}{n^2}\right).$$

Nun berechnen wir I_2 . Durch die Substitution

$$(62) \quad \frac{(p(\varphi) - p)^2}{2 a^2 \sin \varphi \cos \varphi} = \frac{x}{n}$$

ergibt sich

$$(63) \quad I_2 = \frac{2^{5/2} \cdot a(n-1)}{3 n^{3/2}} \int_0^{\pi/4} (\cos \varphi \sin \varphi)^{-3/2} \left[\int_0^{(n \operatorname{tg} \varphi)/2} \left(1 - \frac{x}{n} \right)^{n-2} x^{3/2} dx \right] d\varphi.$$

Jetzt substituieren wir

$$(64) \quad n \operatorname{tg} \varphi = z$$

und erhalten

$$(65) \quad I_2 = \frac{2^{5/2} \cdot a(n-1)}{3 n} \int_0^n \left(\frac{1 + \frac{z^2}{n^2}}{z^3} \right)^{1/2} \int_0^{z/2} \left(1 - \frac{x}{n} \right)^{n-2} x^{3/2} dx dz.$$

Wir setzen

$$(66) \quad \left(1 + \frac{z^2}{n^2}\right)^{1/2} = \left[\left(1 + \frac{z^2}{n^2}\right)^{1/2} - 1\right] + 1$$

und zerlegen dadurch das Integral (65) in zwei Bestandteile. Durch die Ersetzung $z = n\tau$ ergibt sich für den ersten Bestandteil:

$$(67) \quad \frac{2^{5/2} \cdot a(n-1)}{3n} \int_0^n \frac{\sqrt{1 + \frac{z^2}{n^2}} - 1}{z^{3/2}} \int_0^{z/2} \left(1 - \frac{x}{n}\right)^{n-2} x^{3/2} dx dz = \sqrt{\frac{2\pi}{n}} a q + o\left(\frac{1}{n}\right)$$

wobei

$$(68) \quad q = \int_0^1 \frac{(\sqrt{1 + \tau^2} - 1)}{\tau^{3/2}} d\tau$$

ist. Für den zweiten Bestandteil erhalten wir nach einigen elementaren Umformungen

$$(69) \quad \frac{2^{5/2} \cdot a(n-1)}{3n} \int_0^n \left(\int_0^{z/2} \left(1 - \frac{x}{n}\right)^{n-2} x^{3/2} dx \right) \frac{dz}{z^{3/2}} = \frac{8a}{3} - 2 \sqrt{\frac{2\pi}{n}} \cdot a + o\left(\frac{1}{n}\right).$$

Aus (61), (67) und (69) ergibt sich für die mathematische Erwartung von L_n

$$(70) \quad E(L_n) = 4a - \frac{a(2-q)\sqrt{2\pi}}{\sqrt{n}} + o\left(\frac{1}{n}\right).$$

Zur Berechnung von J_1 führt man wieder die Transformationen (58) und danach (60) durch. Nach einigen elementaren Rechnungen erhält man

$$(71) \quad J_1 = \frac{1}{3} a^2 + o\left(\frac{1}{n}\right).$$

Schließlich müssen wir noch das Integral J_2 berechnen. Die Substitution (62) führt auf $J_2 = R_1 - R$ mit

$$(72a) \quad R_1 = \frac{4a^2(n-1)}{3n^{3/2}} \int_0^{\pi/4} \frac{\cos \varphi + \sin \varphi}{(\sin 2\varphi)^{3/2}} \left(\int_0^{(n \operatorname{tg} \varphi)/2} \left(1 - \frac{x}{n}\right)^{n-2} x^{3/2} dx \right) d\varphi,$$

$$(72b) \quad R = \frac{8a^2(n-1)}{3n^2} \int_0^{\pi/4} \left[\int_0^{(n \operatorname{tg} \varphi)/2} \left(1 - \frac{x}{n}\right)^{n-2} x^2 dx \right] \frac{d\varphi}{\sin 2\varphi}.$$

Die Berechnung von R_1 gelingt leicht durch die Substitution (64). Es ergibt sich

$$(73) \quad R_1 = \frac{2}{3} a^2 + o\left(\frac{1}{n}\right).$$

Für R erhalten wir durch die Substitution

$$(74) \quad \frac{n \operatorname{tg} \varphi}{2} = t$$

den Ausdruck

$$(75) \quad R = \frac{4a^2(n-1)}{3n^2} \int_0^{n/2} \left(\int_0^t \left(1 - \frac{x}{n}\right)^{n-2} x^2 dx \right) \frac{dt}{t}.$$

Integrieren wir über x , so ergibt sich

$$(76) \quad R = \frac{8a^2}{3(n+1)} \int_0^{n/2} \left[1 - \left(1 - \frac{t}{n}\right)^{n+1} \right] \frac{dt}{t} + O\left(\frac{1}{n}\right).$$

Für die Berechnung des in (76) auftretenden Integrals benutzen wir die Formel

$$(77) \quad \frac{1}{t} \left[1 - \left(1 - \frac{t}{n}\right)^{n+1} \right] = \frac{1}{n} \sum_{k=0}^n \left(1 - \frac{t}{n}\right)^k.$$

Es folgt

$$(78) \quad \int_0^{n/2} \left[1 - \left(1 - \frac{t}{n}\right)^{n+1} \right] \frac{dt}{t} = \ln n + C - \log 2 + O\left(\frac{1}{n}\right)$$

hierbei bedeutet C die Eulersche Konstante. Er ergibt sich

$$(79) \quad J_2 = R_1 - R = \frac{2a^2}{3} - \frac{8a^2 \ln n}{3n} + O\left(\frac{1}{n}\right).$$

Beachten wir die Formel (70) und $E(F_n) = J_1 + J_2$, so können wir die Ergebnisse dieses Paragraphen in dem folgenden Satz zusammenfassen:

Satz 2. In einem Quadrat K der Seitenlänge a bezeichne H_n die konvexe Hülle von n in K unabhängig und gleichverteilt gewählten Punkten. Für die mathematische Erwartung des Umfanges L_n von H_n gilt

$$(80) \quad E(L_n) = 4a - \frac{a(2-q)\sqrt{2\pi}}{\sqrt{n}} + O\left(\frac{1}{n}\right)$$

wobei die Konstante q durch (68) gegeben ist. Für die mathematische Erwartung des Flächeninhaltes F_n von H_n gilt

$$(81) \quad E(F_n) = a^2 - \frac{8a^2 \ln n}{3n} + O\left(\frac{1}{n}\right).$$

Literatur

- [1] RÉNYI, A., u. R. SULANKE: Über die konvexe Hülle von n zufällig gewählten Punkten, Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete **2** (1963) 75–84.
- [2] BLASCHKE, W.: Vorlesungen über Integralgeometrie, 3. Aufl., Berlin, VEB Deutscher Verlag der Wissenschaften, 1955.

ON AN EXTREMAL PROPERTY OF THE POISSON PROCESS

ALFRÉD RÉNYI

Some years ago (see [1], [2]) we defined the information-theoretical dimension $d=d(\xi)$ and the d -dimensional entropy $h_d(\xi)$ of a random s -dimensional vector ξ as follows. Let us divide each coordinate axis of the s -dimensional Euclidean space E_s into intervals of length $1/n$; let us denote by k the vector $(k_1, \dots, k_s)$ where $k_1, \dots, k_s$ are integers, and by C_k the s -dimensional cube of those points $x=(x_1, \dots, x_s)$ of E_s for which $\frac{k_i}{n} \leq x_i < \frac{k_i+1}{n}$ ($i=1, \dots, s$). Let us denote by $P_n(k)$ the probability that the endpoint of the vector ξ lies in the cube C_k , and put

$$(1) \quad H_n(\xi) = \sum_k P_n(k) \log_2 \frac{1}{P_n(k)}$$

where the summation is to be extended over all values of the vector k .

If $H_n(\xi)$ is finite and the limit

$$(2) \quad d(\xi) = \lim_{n \rightarrow +\infty} \frac{H_n(\xi)}{\log_2 n}$$

exists, we call $d(\xi)$ the (information-theoretical) dimension of ξ (resp. of the probability distribution of ξ). If further the limit

$$(3) \quad \lim_{n \rightarrow +\infty} (H_n(\xi) - d(\xi) \cdot \log_2 n) = h_d(\xi)$$

exists, we call $h_d(\xi)$ the d -dimensional entropy of ξ .

It is easy to see that if ξ is any random s -dimensional vector for which $H_n(\xi)$ is finite for $n \geq n_0$ and $d(\xi)$ exists then

$$(4) \quad d(\xi) \leq s,$$

while if the distribution of ξ is absolutely continuous with density function $f(x) = f(x_1, \dots, x_s)$ then $d(\xi) = s$ and

$$(5) \quad h_d(\xi) = \int f(x) \log_2 \frac{1}{f(x)} dx$$

(where the integration is to be extended over the whole E_s) provided that the integral on the right hand side of (5) exists. It has been proved by I. Csiszár [4] that in case the distribution of ξ is not absolutely continuous in the s -dimensional space one has

$$\lim_{n \rightarrow \infty} (H_n(\xi) - s \log_2 n) = -\infty.$$

The following lemma is well known.

LEMMA 1. *Among all absolutely continuous distributions which are concentrated in an open set G of the s -dimensional space, having finite s -dimensional volume $|G|$ (i.e. the density function of which vanishes outside G) the integral $J(f) = \int_G f(x) \log_2 \frac{1}{f(x)} dx$ is maximal if the distribution is uniform in G , in which case $J(f) = \log_2 |G|$.*

The proof of lemma 1 is trivial. As a matter of fact, using the inequality $\log(1+h) \leq h$ valid for all $h \geq -1$ we obtain

$$(6) \quad J(f) - \log_2 |G| = \frac{1}{\log 2} \int_G f(x) \log \left(1 + \frac{1/|G| - f(x)}{f(x)} \right) dx \leq 0.$$

An other lemma (see [1]) which will be needed here is as follows:

LEMMA 2. *If the distribution of the random vector ξ is the mixture with weights $w_1, w_2, \dots$ of the distributions of the random vectors $\xi_1, \xi_2, \dots$ whose distributions are orthogonal (i.e. $P(\xi = \xi_i) = w_i$ where $\sum w_i = 1$ further there exist sets A_i such that $P(\xi_i \in A_i) = 1$ for $i = 1, 2, \dots$ and $P(\xi_j \in A_i) = 0$ for $j \neq i$) and if the dimension $d_i = d(\xi_i)$ and the d_i -dimensional entropy $h_{d_i}(\xi_i)$ of ξ_i exists for $i = 1, 2, \dots$ then the dimension $d = d(\xi)$ of ξ and the d -dimensional entropy $h_d(\xi)$ of ξ exists, and one has*

$$(7) \quad d = d(\xi) = \sum_i w_i d_i$$

and

$$(8) \quad h_d(\xi) = \sum w_i h_{d_i}(\xi_i) + \sum w_i \log_2 \frac{1}{w_i}$$

provided that the series (8) is convergent.

Recently M. Rudemo [3] has developed further these ideas and applied them to the study of stochastic processes. His starting point can be summarized as follows. Let ξ_s be a random vector with random dimension v i.e. let v be a nonnegative integral valued random variable, $P(v=s) = w_s$ ($s=0, 1, 2, \dots; \sum_{s=0}^{\infty} w_s = 1$) and ξ_s an s -dimensional vector. Suppose that the distribution of ξ_s is absolutely continuous in s -space,

with density function $f_s(x_1, \dots, x_s)$ and further that the entropies

$$(9) \quad h_s(\xi_s) = \iint \dots \int f_s(x_1, \dots, x_s) \log_2 \frac{1}{f_s(x_1, \dots, x_s)} dx_1 \dots dx_s$$

exist.

In view of lemma 2 it is natural to define the dimension $d=d(\xi_v)$ of the random vector ξ_v by the formula

$$(10) \quad d(\xi_v) = \sum_{s=1}^{\infty} s w_s$$

and its (d -dimensional) entropy by

$$(11) \quad h_d(\xi_v) = \sum_{s=1}^{\infty} w_s h_s(\xi_s) + \sum_{s=1}^{\infty} w_s \log_2 \frac{1}{w_s}$$

provided the series (10) and (11) are convergent. Now let us be given a point process on the half-line $0 \leq t \leq +\infty$, defined by an infinite sequence $\eta = (\eta_1, \dots, \eta_s, \dots)$ of random variables, such that with probability 1 $0 < \eta_1 < \eta_2 < \dots < \eta_s < \dots$ and $\lim_{s \rightarrow +\infty} \eta_s = +\infty$. Let T be any positive number. Then the dimension $d(T)$ of the process $\eta = (\eta_1, \dots, \eta_s, \dots)$ and its $d(T)$ -dimensional entropy $h(T)$ in the interval $(0, T]$ are defined as follows. Let the random variable v denote the number of values of k such that $0 < \eta_k \leq T$, i.e. we define v by the inequality $\eta_v \leq T < \eta_{v+1}$. Let the random vector ξ_v be defined as the vector $\xi_v = (\eta_1, \dots, \eta_v)$. Let us put $w_s(T) = P(v=s)$ and

$$(12) \quad d(T) = \sum_{s=1}^{\infty} w_s(T) d(\xi_s)$$

(provided that the series converges) and call it *the dimension of the process η in the interval $(0, T)$* and put

$$(13) \quad h(T) = \sum_{s=1}^{\infty} w_s h_{d(\xi_s)}(\xi_s) + \sum_{s=1}^{\infty} w_s \log_2 \frac{1}{w_s}$$

(provided that these series converge) and call it *the entropy (of dimension $d(T)$) of the process η in the interval $(0, T]$* .*

In the present paper we shall investigate only homogeneous point processes, with finite density $\lambda > 0$, i.e. processes for which

$$(14) \quad \sum_{s=1}^{\infty} s w_s(T) = \lambda T$$

* Rudemo considered other processes too, but in this note we are concerned only with point processes.

for all $T > 0$. Taking into account that $d(\xi_s) \leq s$ the dimension $d(T)$ of such a process in the interval $(0, T)$ can not exceed λT .

We shall restrict ourselves to the study of processes, for which $d(\xi_s) = s$ for all s . For this it is sufficient by what has been said above that ξ_s should have an absolutely continuous distribution for all values of s . We shall call such processes *homogeneous point processes with maximal dimension*. We are now in the position to formulate the main result of this paper:

THEOREM. *For every $T > 0$ among all homogeneous point processes with given density $\lambda > 0$, the Poisson process has the greatest (λT -dimensional) entropy in the interval $(0, T)$.*

Remark. This theorem expresses in a precise form the intuitively clear fact, that the distribution of the points of a Poisson process is "more random" as of the points of any other homogeneous point process (having the same density).

PROOF. In view of the theorem of I. Csiszár mentioned above, we may restrict ourselves to processes, for which the distribution of ξ_s is absolutely continuous in the s -dimensional simplex $A_s(T)$ formed by the points $(x_1, \dots, x_s)$ for which $0 \leq x_1 \leq x_2 \leq \dots \leq x_s \leq T$, because otherwise $h_{\lambda T}(\xi_s) = -\infty$.

Now it is well known that for a Poisson process under condition $v = s$ the random vector ξ_s is uniformly distributed in the simplex $A_s(T)$, i.e. as the volume of $A_s(T)$ equals $\frac{T^s}{s!}$ in this case we have

$$(15) \quad h_s(\xi_s) = \log_2 \frac{T^s}{s!}.$$

Thus, in view of lemma 1 we have

$$(16) \quad h(T) \leq \sum_{s=1}^{\infty} w_s \log_2 \frac{T^s}{s!} + \sum_{s=0}^{\infty} w_s \log_2 \frac{1}{w_s}$$

and for the Poisson process we have equality in (16). However the property that ξ_s is uniformly distributed in $A_s(T)$ is valid not only for the Poisson process but is shared by all mixtures of Poisson processes. Thus we have to investigate the maximum of the expression

$$(17) \quad L = \sum_{s=1}^{\infty} w_s \log_2 \frac{T^s}{s!} + \sum_{s=0}^{\infty} w_s \log_2 \frac{1}{w_s}$$

under the condition (14) and the condition $\sum_{s=0}^{\infty} w_s = 1$. Putting

$$(18) \quad \pi_s = \frac{(\lambda T)^s e^{-\lambda T}}{s!}$$

we have

$$(19) \quad L = \sum_{s=0}^{\infty} w_s \log_2 \frac{\pi_s}{w_s} + \lambda T \log_2 \frac{e}{\lambda}.$$

Now it is well known that if $\{w_s\}$ and $\{\pi_s\}$ are arbitrary probability distributions, then

$$(20) \quad \sum_{s=0}^{\infty} w_s \log_2 \frac{\pi_s}{w_s} \leq 0,$$

with equality if and only if the distributions $\{w_s\}$ and $\{\pi_s\}$ are identical; it follows that

$$(21) \quad h(T) \leq \lambda T \log_2 \frac{e}{\lambda}$$

with equality standing in (21) if and only if

$$(22) \quad w_s = \pi_s$$

where π_s is defined by (18), i.e. if v has a Poisson distribution, that is if and only if η is a Poisson process. This proves our theorem.

It should be remarked that the value of $h(T)$ for a Poisson process has been computed already by M. Rudemo [3].

A generalization of the result for point processes in more than one dimension can be carried out without any difficulty.

REFERENCES

- [1] J. Balatoni and A. Rényi, "On the concept of entropy" (Hungarian), *Publ. Math. Inst. Hung. Acad. Sci.*, 1 (1956), 9-40. [A German translation, under the title: "Über den Begriff der Entropie" is published in *Arbeiten zur Informationstheorie*, Deutscher Verlag der Wissenschaften, Berlin, 1 (1957), 117-134].
- [2] A. Rényi, "On the dimension and entropy of probability distributions", *Acta Math. Acad. Sci. Hung.*, 10 (1959), 193-215.
- [3] M. Rudemo, "Dimension and entropy for a class of stochastic processes", *Publ. Math. Inst. Hung. Acad. Sci.*, 9 (1964) 73-87.
- [4] I. Csiszár, "Some remarks on the dimension and entropy of random variables", *Acta Math. Acad. Sci. Hung.*, 12 (1961), 399-408.

NOTE

The entropy maximum property of the Poisson process (No 228) is interpreted from the point of view of statistical physics by R. Holley [1]. The result is generalized in J. Fritz [3] in the following way. Consider point processes in a nonatomic separable measure space $(R, \mathfrak{A}, \mu)$; the expectation measure $\lambda = \lambda(G)$ denotes the average number of points in the set G . For $\lambda(R) < +\infty$ the $\lambda(R)$ -dimensional entropy of such point processes can be defined; in the construction the one-dimensional Lebesgue measure is replaced by μ . Then, among all point processes with given expectation measure, the Poisson process has maximal entropy, the value of which can be calculated, too. (J. F.)

REFERENCES

- [1] Holley, R.: The motion of a heavy particle in an infinite one dimensional gas of hard spheres. *Zeitschrift für Wahrscheinlichkeitstheorie*, **17** (3), (1971), 181—219.
- [2] Fritz, J.: Information theory and thermodynamics of gas systems. *Proc. Coll. Information Theory. Debrecen*, 1967, (1968), 167—176.
- [3] Fritz, J.: An approach to the entropy of point processes. *Periodica Math. Hung.*, **3** (1—2), (1973), 73—83.

Page 132, row 5, footnote:

The condition $H_n(\xi_s) < \infty$ is now automatically fulfilled since the range of ξ_s is bounded.

A GENERALIZATION OF A THEOREM OF E. VINCZE

by

R. G. LAHA¹, E. LUKACS¹ and A. RÉNYI

The functional equation $\varphi(x) = \varphi(ax)\varphi(bx)$ ($a, b > 0$, $a^2 + b^2 = 1$) was solved by E. VINCZE [1] under the assumption that $\varphi(x)$ is a complex valued function of the real variable x which can be differentiated twice at the origin. This equation occurs in certain problems in probability theory and was therefore studied by a number of authors under the restriction that $\varphi(x)$ is a positive definite function.

In the present note we prove the following generalization of VINCZE's result:

Theorem. Let $\varphi(x)$ be a complex valued function of the real variable x and let $\{a_j\}$ be a sequence of nonnegative real numbers such that $\sum_{j=1}^{\infty} a_j^2 = 1$ and $0 < a_1 < 1$. Suppose that there exist complex constants A and B such that

$$(1) \quad \lim_{x \rightarrow 0} \frac{\varphi(x) - \varphi(0) - Ax}{x^2} = B.$$

Assume further that $\varphi(x)$ satisfies for all real x the functional equation

$$(2) \quad \varphi(x) = \prod_{j=1}^{\infty} \varphi(a_j x)$$

where the infinite product converges.² Then $A = 0$ and $\varphi(x) = e^{Bx^2}$.

Proof. It follows from (1) that $\varphi(x)$ is continuous at $x = 0$. It follows further from the convergence of the infinite product (2) that $\lim_{j \rightarrow \infty} \varphi(a_j x) = 1$.

and as clearly $\lim_{j \rightarrow \infty} a_j = 0$ we obtain $\varphi(0) = 1$. Thus it follows from (1) that

$$(3) \quad \varphi(x) = 1 + Ax + O(x^2) \quad \text{for } x \rightarrow 0.$$

Thus we have

$$\prod_{j=1}^N \varphi(a_j x) = e^{A(\sum_{j=1}^N a_j)x + O(x^2)}.$$

¹ The Catholic University of America. The research of these authors was supported by the National Science Foundation through grant NSF-GP-96.

² As usually the convergence of an infinite product $\prod_{n=1}^{\infty} z_n$ is understood in the sense that only a finite number of factors may be equal to 0 and if $z_n \neq 0$ for $n \geq n_0$ then $\lim_{N \rightarrow \infty} \prod_{n=n_0}^N z_n$ exists and is different from 0.

As the product (2) is convergent, it follows that the series $\sum_{j=1}^{\infty} a_j$ is convergent too. Let us put

$$(4) \quad \sum_{j=1}^{\infty} a_j = C.$$

We have evidently $C > 1$. It follows that $\varphi(x) = e^{ACx + O(x^2)}$ and thus

$$(5) \quad \frac{\varphi(x) - 1 - Ax}{x^2} = \frac{A(C-1)}{x} + O(1) \quad \text{for } x \rightarrow 0.$$

Clearly (5) is compatible with (1) only if $A = 0$. Condition (1) now reduces to

$$(6) \quad \lim_{x \rightarrow 0} \frac{\varphi(x) - 1}{x^2} = B$$

which yields

$$(7) \quad \lim_{x \rightarrow 0} \frac{\log \varphi(x)}{x^2} = B.$$

Clearly (6) implies that there exist positive numbers d and D such that

$$(8) \quad |\varphi(x) - 1| < Dx^2 \quad \text{for } |x| \leq d.$$

As for $|z - 1| \leq \frac{1}{2}$ we have $|\arg z| \leq \frac{\pi}{3}|z - 1|$, it follows that for $|x| \leq \Delta = \min\left(d, \frac{1}{\sqrt{2D}}\right)$ we have

$$\sum_{j=1}^{\infty} |\arg \varphi(a_j x)| < \pi.$$

Thus we obtain from (2)

$$(9) \quad \log \varphi(x) = \sum_{j=1}^{\infty} \log \varphi(a_j x) \quad \text{for } |x| \leq D.$$

We obtain from (9) by iteration for any natural number k

$$(10) \quad \log \varphi(x) = \sum_{j_1=1}^{\infty} \dots \sum_{j_k=1}^{\infty} \log \varphi(a_{j_1} \dots a_{j_k} x).$$

Since $\max a_j = \alpha < 1$ we see that

$$(11) \quad \max a_{j_1} \dots a_{j_k} \leq \alpha^k.$$

In view of (11) and (7) for any $\varepsilon > 0$ we can choose the value of k so large that

$$(12) \quad |\log \varphi(a_{j_1} \dots a_{j_k} x) - Bx^2 a_{j_1}^2 \dots a_{j_k}^2| \leq \varepsilon a_{j_1}^2 \dots a_{j_k}^2$$

for all $|x| \leq \Delta$. It follows from (10) and (12) that

$$(13) \quad |\log \varphi(x) - Bx^2| \leq \varepsilon.$$

As ε can be chosen arbitrarily small we obtain that $\varphi(x) = e^{Bx^2}$ for $|x| \leq \Delta$.

Let us put $\psi(x) = \varphi(x) e^{-Bx^2}$. Then clearly $\psi(x)$ satisfies for all x the equation

$$(14) \quad \psi(x) = \prod_{j=1}^{\infty} \psi(a_j x)$$

further $\psi(x) = 1$ for $|x| \leq \Delta$. Let x_0 denote the upper bound of those positive numbers β for which $\psi(x) = 1$ for $|x| \leq \beta$. We have already shown that $x_0 \geq \Delta > 0$. Suppose that x_0 is finite; we shall prove that this leads to a contradiction. Clearly $\psi(\pm x_0) = 1$ because $\max a_j = \alpha < 1$. Let now η be an arbitrary real number such that $1 > \eta > \alpha$; then $\frac{a_j}{\eta} < \frac{a_j}{\alpha} \leq 1$ so that $\psi\left(\pm \frac{a_j}{\eta} x_0\right) = 1$. It follows that $\psi\left(\pm \frac{x_0}{\eta}\right) = 1$. This however contradicts the definition of x_0 . Thus $x_0 = +\infty$ and $\varphi(x) = e^{Bx^2}$ for all x .

We are indebted to P. Bártfai for a valuable remark, which we utilized in preparing the final version of this paper.

REFERENCE

- [1] VINCZE, E.: »Bemerkung zur charakterisierung des Gausschen Fehlergesetzes.« *Publications of the Mathematical Institute of the Hungarian Academy of Sciences* 7 (1962) 357—361.

ON TWO MATHEMATICAL MODELS OF THE TRAFFIC ON A DIVIDED HIGHWAY

A. RÉNYI, *Mathematical Institute of the Hungarian Academy of Sciences, Budapest*

Introduction

In the present paper we deal with two models of the traffic on a divided highway. In both models traffic is flowing in one direction only, in two lanes, of which one (the left hand lane) is used only for overtaking. We suppose that vehicles enter the highway at the same entrance so that the instants at which a vehicle enters the highway form a homogeneous Poisson process, with density λ . Thus λ is the rate at which vehicles enter the highway per unit time. We suppose that there are no junctions, or exits (i.e. the highway extends in one direction to infinity).

In the first model, discussed in Section 1, we suppose that each driver chooses a speed v , and drives constantly at this speed. We suppose in this model that if a vehicle B approaches a slower vehicle A ahead of it, B overtakes A without delay. This means that we neglect the case when a third, still faster car, C , has already begun overtaking B on the left hand lane, so that B has to slow down and wait until C passes, and only after this can itself go over to the left hand lane to pass A . In reality the cars lose some time because of overtaking, even on a divided highway. The second model, discussed in Section 2, differs from the first only in that this effect is taken into account, and the corresponding average decrease of speed is estimated. A more detailed analysis of the second model will be given elsewhere.

1. Discussion of the first model

We suppose that denoting by v_k the speed of the vehicle entering the highway at the moment τ_k , the random variables v_k ($k = 1, 2, \dots$) are independently and identically distributed with the cumulative distribution function $F(v) = P(v_k < v)$, and are also independent of the process $\{\tau_k\}$. Clearly we have to suppose $F(0) = 0$. Besides this, the only restriction necessary for $F(v)$ is that

$$(1.1) \quad \frac{1}{w} = \int_0^\infty \frac{dF(v)}{v} < +\infty,$$

i.e. that the mean value of $1/v_k$ should be finite; without this condition a traffic jam would arise and make all traffic flow impossible. Of course, in reality, there exists a positive lower limit to the velocities, i.e. a positive number a such that $F(a) = 0$; this ensures that condition (1.1) holds. (On many highways there is in fact a prescribed lower speed limit.) In Model 1 we suppose that overtaking a slower car takes place without delay; thus each car travels with constant velocity. (In the second model we shall drop this simplifying assumption.) In Model 1, if we consider the distribution of cars along the highway at a given instant of time, it can be easily seen that the spatial distribution of the vehicles along the highway is also a homogeneous Poisson process with density

$$(1.2) \quad \Lambda = \frac{\lambda}{w},$$

this shows why $1/w$ has to be finite).

The fact that the spatial process at any moment is again a Poisson process follows from a general theorem of Ryll-Nardzewski [1] (see also Prékopa [9]).

Recently Breiman [2], [3] considered¹ the problem of one-way traffic flow, starting from the spatial process. If one supposes that at a certain moment t_0 the spatial process is a Poisson process with density μ and the velocities of the vehicles are random variables with the identical distribution function $F(v)$, and are independent of each other and of the position of the vehicles at the moment t_0 , it follows from a more general result of Doob [5] that the process will have the same properties at any other moment t . Breiman has proved that the Poisson process is the only process having this time-invariance property.

Our main aim is to take into account (in Model 2 which will be discussed in Section 2) the delays in overtaking; for this reason we have found it more convenient to start from the process of entrance times of the vehicles rather than from the spatial process, as was done by Breiman.

We shall prove now some results concerning Model 1, which will be needed also in discussing Model 2. Let us imagine that we are sitting in a car travelling along the highway with velocity v_0 . Let τ_k^+ ($k=1, 2, \dots$) denote the instants when our car overtakes a car with a lower speed, and τ_k^- ($k=1, 2, \dots$) the instants when a faster car overtakes our car. The following theorem is valid.

Theorem 1. The instants $\{\tau_k^+\}$ and $\{\tau_k^-\}$ form two homogeneous Poisson processes, with densities

$$(1.3) \quad \lambda^{(+)}(v_0) = \lambda \int_0^{v_0} \frac{v_0 - v}{v} dF(v) \quad \text{and} \quad \lambda^{(-)}(v_0) = \lambda \int_{v_0}^{\infty} \left(\frac{v - v_0}{v} \right) dF(v),$$

¹ For further literature, we refer to the paper by Hammersley [4] where a bibliography up to 1961 is given. A complete bibliography of the scientific study of road traffic, containing more than 700 items, has been prepared by Frank A. Haight and will be issued by the International Statistical Institute in 1964.

Moreover these two processes are independent of each other.

The following corollary of Theorem 1 should be noted:

Corollary. We have $\lambda^{(+)}(v_0) = \lambda^{(-)}(v_0)$ if and only if

$$(1.4) \quad v_0 = \left(\int_0^\infty \frac{dF(v)}{v} \right)^{-1} = w.$$

In other words a car travelling with speed v_0 is as frequently overtaken by faster cars as it overtakes slower cars if its speed v_0 is equal to the harmonic mean w of the speeds of all the vehicles on the given highway.

If we make notes of the speeds of the cars which overtake us, and the speeds of the cars which we overtake, we naturally obtain a biased picture of the velocity distribution of the cars on the highway; however from this "apparent" velocity distribution, the real distribution can be easily determined. As a matter of fact, supposing for the sake of simplicity that the density function $f(v) = F'(v)$ of the velocity distribution exists, we obtain for the apparent density $f_a(v)$ the respective formulae

$$(1.5) \quad f_a(v) = \frac{\lambda f(v) \left(\frac{v_0}{v} - 1 \right)}{\lambda^{(+)}(v_0)} \quad \text{for } 0 < v \leq v_0$$

for the slower cars, and

$$(1.6) \quad f_a(v) = \frac{\lambda f(v) \left(1 - \frac{v_0}{v} \right)}{\lambda^{(-)}(v_0)} \quad \text{for } v_0 \leq v < +\infty$$

for the faster cars, and from these formulae, knowing $f_a(v)$, we can determine $f(v)$ easily.

It is possible to determine the velocity distribution also if we observe only one of the densities $\lambda^{(+)}(v_0)$ and $\lambda^{(-)}(v_0)$, but this must be done for every value of v_0 . As a matter of fact, if $\lambda^{+}(v_0)$ as a function of v_0 is given for all v_0 , we obtain from (1.3)

$$(1.7) \quad \lambda^{(+)}(v_0) = \lambda v_0 \int_0^{v_0} \frac{F(v) dv}{v^2}$$

and thus

$$(1.8) \quad F(x) = \frac{1}{\lambda} \left(\frac{x d\lambda^{(+)}(x)}{dx} - \lambda^{(+)}(x) \right).$$

[(1.7) shows that not only $\lambda^{+}(x)$ but also $\lambda^{+}(x)/x$ is an increasing function of x .]

Thus if we travel for sufficiently long periods with different velocities and count the number of cars we overtake (or which overtake us), we can estimate from these data the velocity distribution and the total flow of vehicles fairly accurately. We shall not go into the details of these estimation problems here.

The proof of Theorem 1 is based on the following two properties of Poisson processes:

(A) If $0 < \tau_1 < \tau_2 < \dots$ are the instants of time when an event occurs in a homogeneous Poisson process with density λ , and $\zeta_1, \zeta_2, \dots$ is a sequence of independent positive random variables, having the same distribution function $F(v)$, and independent of the process $\{\tau_k\}$, then the time instants $\tau_k \zeta_k$ ($k=1, 2, \dots$) also form a homogeneous Poisson process with density

$$(1.9) \quad \lambda^* = \lambda \int_0^\infty \frac{dF(v)}{v}$$

(B) If a subsequence $\{\tau_{v_k}\}$ of the instants τ_k , in which an event occurs in a Poisson process with density λ , is selected at random in such a way that for each j the probability of the event A_j that j should belong to the subsequence $\{v_k\}$ is equal to p ($0 < p < 1$) and the events A_j ($j=1, 2, \dots$) are independent, and if $\{\tau_{\mu_k}\}$ are the instants which are not selected, (i.e., j belongs to the sequence $\{\mu_k\}$ if and only if it does not belong to the sequence $\{v_k\}$), then both $\{\tau_{v_k}\}$ and $\{\tau_{\mu_k}\}$ are Poisson processes, with densities λp and λq , where $q = 1 - p$; moreover the two processes are independent.

Property (A) can be proved easily; it follows also from the mentioned theorem of Ryll-Nardzewski [1] or of Prékopa [9]. Property (B) is well known.

Let us mention that in a certain sense property (B) is characteristic of Poisson processes, as the following theorem shows.

Theorem 2. Let $\mathcal{P}_\lambda$ be a class of time-homogeneous point processes such that for each $\lambda > 0$ the process $\mathcal{P}_\lambda$ has density λ . Let us split at random the process $\mathcal{P}_\lambda$ into two processes $\mathcal{P}_\lambda^{(1)}$ and $\mathcal{P}_\lambda^{(2)}$ in such a way that for each point of $\mathcal{P}_\lambda$ the probability that it will belong to $\mathcal{P}_\lambda^{(1)}$ is equal to p , and the probability that it will belong to $\mathcal{P}_\lambda^{(2)}$ is equal to $q = 1 - p$, independently of what happens to the other points. Let us suppose that for every value of p the process $\mathcal{P}_\lambda^{(1)}$ will be governed by the same laws as the process $\mathcal{P}_{\lambda p}$, and $\mathcal{P}_\lambda^{(2)}$ by the same laws as $\mathcal{P}_{\lambda q}$. Further let the processes $\mathcal{P}_\lambda^{(1)}$ and $\mathcal{P}_\lambda^{(2)}$ be independent. Then for each λ , $\mathcal{P}_\lambda$ is a Poisson process with density λ .

Proof. Let $P_n(t, \lambda)$ denote the probability of the event that an interval of length t contains exactly n events of the process $\mathcal{P}_\lambda$. From the assumption that the probability distribution of the number of events in an interval in the process $\mathcal{P}_\lambda^{(1)}$ and the process $\mathcal{P}_{\lambda p}$ are identical, it follows that

$$(1.10) \quad P_k(t, \lambda p) = \sum_{n=k}^{\infty} \binom{n}{k} p^k q^{n-k} P_n(t, \lambda) \quad (k = 0, 1, \dots).$$

Putting

$$(1.11) \quad G(t, \lambda, u) = \sum_{n=0}^{\infty} P_n(t, \lambda) (1+u)^n,$$

where $G(t, \lambda, u)$ is certainly defined if $|1+u| \leq 1$, we obtain from (1.10) that the functional equation

$$(1.12) \quad G(t, \lambda p, u) = G(t, \lambda, pu)$$

holds. The identity (1.12) can be used for the analytic continuation of $G(t, \lambda, \mu)$ for all complex values of u such that $\operatorname{Re}(u) < 0$. It follows further from (1.12) that for $\operatorname{Re}(u) < 0$,

$$(1.13) \quad G(t, \lambda, u) = G(t, 1, \lambda u) = H(t, \lambda u).$$

Now from the assumption that the processes $\mathcal{P}_\lambda^{(1)}$ and $\mathcal{P}_\lambda^{(2)}$ are independent, it follows that

$$(1.14) \quad P_n(t, \lambda) = \sum_{k=0}^n P_k(t, \lambda p) P_{n-k}(t, \lambda q)$$

and thus that

$$(1.15) \quad H(t, \lambda u) = H(t, p\lambda u) \cdot H(t, q\lambda u).$$

As $H(t, v)$ is clearly analytic in v , we obtain

$$(1.16) \quad H(t, \lambda u) = e^{\lambda u K(t)}$$

and thus

$$(1.17) \quad \sum_{n=0}^{\infty} P_n(t, \lambda) z^n = e^{\lambda(z-1)K(t)}.$$

Let us now compute the mean value $M_\lambda(t)$ of the number of events in an interval of length t in the process $\mathcal{P}_\lambda$. We obtain from (1.17) that

$$(1.18) \quad M_\lambda(t) = \sum_{n=0}^{\infty} P_n(t, \lambda) \cdot n = \lambda K(t).$$

But as we suppose that the process $\mathcal{P}_\lambda$ is time-homogeneous and has density λ , we have $M_\lambda(t) = \lambda t$. Thus we obtain from (1.18) that $K(t) \equiv t$, and hence

$$(1.19) \quad \sum_{n=0}^{\infty} P_n(t, \lambda) z^n = e^{\lambda(z-1)t},$$

which implies that

$$(1.20) \quad P_n(t, \lambda) = \frac{(\lambda t)^n e^{-\lambda t}}{n!} \quad (n = 0, 1, \dots),$$

so that the process $\mathcal{P}_\lambda$ is a process with independent increments.

Thus $\mathcal{P}_\lambda$ is a Poisson process with density λ , and Theorem 2 is proved.

Let us mention that if we suppose only that $\mathcal{P}_\lambda^{(1)}$ and $\mathcal{P}_\lambda^{(2)}$ are governed by the same laws as $\mathcal{P}_{\lambda p}$ and $\mathcal{P}_{\lambda q}$ but do not assume the independence of the processes $\mathcal{P}_\lambda^{(1)}$ and $\mathcal{P}_\lambda^{(2)}$, there are other solutions too, e.g. the compound Poisson processes, for which

$$P_n(t, \lambda) = \int_0^\infty \frac{(\lambda t y)^n e^{-\lambda t y}}{n!} dL(y),$$

where $L(y)$ is a probability distribution function in $(0, \infty)$ with mean value 1.

Theorem 2 is related to investigations concerning the rarification of time-homogeneous point processes (see [6], [7] and [8]).

2. Discussion of the second model

Let us pass now to Model 2. In fact, if a car B in the right hand lane approaches a slower car A , it can overtake it only if the left hand lane behind it is free for a certain distance; that is if a still faster car C has not already begun to overtake the car B . If, however, a faster car C has started overtaking B , then B has to slow down to the velocity of the car A and travel with this velocity until C has passed. To make our model precise, we have to introduce quite strict rules on how overtaking has to be effected. First we suppose that if a car B with velocity v_2 approaches in the right hand lane from behind a slower car A , with velocity $v_1 < v_2$, it has to go over to the left hand lane at the instant when the distance between the two cars becomes equal to $T(v_2 - v_1)$ (provided that at this instant there is no third car behind it which has already started overtaking it) and remains there until it has passed A ; then it goes back immediately to the right hand lane. B does the same in the case when at the moment it starts overtaking A , A is in the left hand lane in the course of overtaking a third, still slower car; clearly this does not cause any difficulty, since the car A will spend a time less than T in the left hand lane, and thus A will go back to the right hand lane before B passes it, so that B can continue in the left hand lane without slowing down.

This rule is reasonable, as it corresponds to the practice of a cautious driver. Of course, one does not really return to the right hand lane immediately after passing another car, but only after passing it by a certain distance; in order to simplify the theory we neglect this second phase of overtaking. We did not incorporate into our model the fact that most drivers accelerate during overtaking;

these two neglected factors have opposite effects: the first means a lengthening, the second a shortening of the time spent on the left hand lane and their joint effect is practically negligible.

Our rule is convenient from a mathematical point of view because—as shown above—it ensures that no car has to slow down when it is in the left hand lane in the course of overtaking another car.

In our second model each vehicle (except the vehicles which travel either with the minimum or the maximum possible velocity) is from time to time forced to travel slower than its own chosen velocity v and thus its effective average velocity $\bar{v}$ is smaller than v . We want now to calculate $\bar{v}$ as a function of v . This problem is rather difficult. Therefore we deal here only with the case when all cars on the highway are travelling either with the velocity v_1 or with the velocity $v_3 > v_1$ except for the car in which we are sitting, which travels with an intermediate velocity v_2 , i.e. we have $v_1 < v_2 < v_3$.

More exactly we suppose that the process of arrival times of the cars at the entrance of the highway is a time-homogeneous Poisson process with density λ , and further that each car chooses at random the velocity v_1 or v_3 ($v_1 < v_3$) with the corresponding probabilities p and $q = 1 - p$. Let us call for the sake of brevity the cars with speed v_1 the slow cars, and those with speed v_3 the fast cars. Let us suppose further that we arrive at the entrance of the highway at time $t = 0$ and want to travel with the speed v_2 where $v_1 < v_2 < v_3$.

Clearly neither the slow nor the fast cars lose speed; the slow ones because they cannot overtake any other car, the fast ones because no vehicle overtakes them. Thus we have to compute only the velocity loss of our own car. As was shown in Section 2, so long as we maintain the velocity v_2 the time instants τ_k^+ when we overtake a car with velocity v_1 form a Poisson process $\mathcal{P}^+$ with density

$$(2.1) \quad \lambda^{(+)} = \lambda p \left(\frac{v_2 - v_1}{v_1} \right),$$

while the instants when a car with velocity v_3 overtakes us form a Poisson process $\mathcal{P}^-$ with density

$$(2.2) \quad \lambda^{(-)} = \lambda q \left(\frac{v_3 - v_2}{v_3} \right),$$

these two processes being independent.

Let us now compute the distribution of the random variable χ which is the length of the time interval from the moment we entered the highway until the moment when, for the first time, we should like to start overtaking a slow car in front of us, but cannot do this because a fast car has already started overtaking us. Clearly if τ_k^+ is the least instant $> T$ belonging to the process $\mathcal{P}^+$ such that there exists a τ_l^- belonging to $\mathcal{P}^-$ for which $\tau_l^- < \tau_k^+ < \tau_l^- + T$ then $\chi = \tau_k^+ - T$.

Now the time instants τ_k^+ of the process $\mathcal{P}^+$, for which there is such a τ_l^- in the process $\mathcal{P}^-$, themselves clearly form a Poisson process with density

$$(2.3) \quad D = \lambda^{(+)} \cdot (1 - e^{-\lambda^{(-)}T}).$$

Thus τ_k^+ has an exponential distribution with mean $1/D$. Now

$$P(\chi \geq x) = P(\tau_k^+ \geq x + T | \tau_k^+ \geq T) = P(\tau_k^+ \geq x),$$

and thus χ has also an exponential distribution with mean value $1/D$, i.e.

$$(2.4) \quad E(\chi) = \frac{1}{D} = \frac{1}{\lambda^{(+)}(1 - e^{-\lambda^{(-)}T})}.$$

If we are forced to slow down to the velocity v_1 because we cannot overtake the slow car in front of us until the fast car behind us, which has already started overtaking us, has passed, we have to continue to drive with velocity v_1 for at least a time interval of length

$$(2.5) \quad [T - (\tau_k^+ - \tau_l^-)] \frac{v_3 - v_2}{v_3 - v_1} = \delta_0.$$

However it may happen that we cannot start to overtake the slow car in front of us at the instant $\tau_k^+ - T + \delta_0$ because in the meantime another fast car has started to overtake us; in this case we have to wait until this fourth car has passed, and then look out to see whether there is a fifth car which has in the meantime already started overtaking us, and so on. Thus in computing the distribution of the length of the time interval in which we are forced to travel with the velocity v_1 of the slow car in front of us, we have to take into account these various possibilities. In dealing with this question we cannot work with the quantities $\tau_{l+1}^-, \tau_{l+2}^-, \dots$ because these do not give us the instants when a fast car overtakes us, because we have slowed down. Instead of this, we must work with the instants τ_j^* at which a fast car overtakes us now that we are travelling with the velocity v_1 . These instants τ_j^* form, according to what has been said in Section 1, a Poisson process with density

$$(2.6) \quad \lambda^* = \lambda q \left(\frac{v_3 - v_1}{v_3} \right).$$

As the first fast car passes us at the moment $\tau_k^+ - T + \delta_0$, we clearly have to let n fast cars pass before being able to pass the slow car in front of us if and only if

$$\tau_{j+1}^* - T < \tau_k^* - T + \delta_0 < \tau_{j+1}^* ,$$

$$\tau_{j+2}^* - T < \tau_{j+1}^* < \tau_{j+2}^* ,$$

and

$$\tau_{j+n-1}^* - T < \tau_{j+n-2}^* < \tau_{j+n-1}^* ,$$

$$\tau_{j+n}^* - T \geq \tau_{j+n-1}^* .$$

As the variables $\tau_j^* - (\tau_k^* - T + \delta_0), \tau_{j+1}^* - \tau_j^*, \dots$ are all independent and have an exponential distribution with the mean value $1/\lambda^*$, we have, if we denote by r the number of fast cars which we are forced to let pass us, that

$$(2.7) \quad P(r = n) = (1 - e^{-\lambda^* T})^{n-1} e^{-\lambda^* T}$$

and thus

$$(2.8) \quad E(r) = e^{\lambda^* T}$$

Let us now compute the mean value of the length of the time interval in which we have to drive slowly and wait for an opportunity for overtaking. Let us denote this time interval by η . Thus we have

$$(2.9) \quad \eta = \delta_0 + \delta_1 + \dots + \delta_{r-1} ,$$

where δ_0 is given by (2.5), $\delta_1 = \tau_{j+1}^* - (\tau_k^* - T + \delta_0)$ and $\delta_{i+1} = \tau_{j+i+1}^* - \tau_{j+i}^*$ for $i = 1, 2, \dots, r-2$. We have evidently

$$(2.10) \quad E(\delta_1 + \dots + \delta_{r-1}) = \sum_{n=2}^{\infty} P(r = n) E(\delta_1 + \dots + \delta_{n-1} | r = n) .$$

Now for $k < n$

$$(2.11) \quad E(\delta_k | r = n) = E(\delta_k | \delta_k \leq T) = \frac{1}{\lambda^*} - \frac{T}{e^{\lambda^* T} - 1} .$$

Thus we obtain

$$(2.12) \quad E(\delta_1 + \dots + \delta_{r-1}) = \frac{e^{\lambda^* T} - 1}{\lambda^*} - T .$$

Let us now compute $E(\delta_0)$. From (2.5) we obtain

$$E(\delta_0) = \left(\frac{v_3 - v_2}{v_3 - v_1} \right) \left(\frac{1}{\lambda^{(-)}} - \frac{T}{e^{\lambda^{(-)} T} - 1} \right)$$

and hence

$$(2.13) \quad E(\eta) = \left(\frac{v_3 - v_2}{v_3 - v_1} \right) \left(\frac{1}{\lambda^{(-)}} - \frac{T}{e^{\lambda^{(-)} T} - 1} \right) + \left(\frac{e^{\lambda^* T} - 1}{\lambda^*} - T \right) .$$

Now we are in a position to compute our average effective velocity. As we travel alternatively with velocities v_2 and v_1 , the mean values of the corresponding time intervals being $E(\chi)$ and $E(\eta)$ and the time intervals in question being independent, we obtain by the law of large numbers that in the long run our average velocity will be $\bar{v}_2$ where

$$(2.14) \quad \bar{v}_2 = \frac{v_2 \cdot E(\chi) + v_1 \cdot E(\eta)}{E(\chi) + E(\eta)},$$

where $E(\chi)$ and $E(\eta)$ are given by (2.4) and (2.13) respectively, and the quantities $\lambda^{(+)}, \lambda^{(-)}, \lambda^*$ figuring in these expressions are defined by (2.1), (2.2) and (2.6) respectively.

It is easy to see that a considerable loss in velocity is to be expected only if the traffic on the highway is heavy, more exactly, if both λ^*T and $\lambda^{(-)}T$ are large.

As regards the general case, one can get an approximate solution for the effective velocity $\bar{v}$ of a car which travels with velocity v when this is possible, by replacing the actual velocity distribution by a distribution in which there are only two velocities present, namely

$$v_1 = \frac{1}{F(v)} \int_0^v t dF(t)$$

and

$$v_3 = \frac{1}{1 - F(v)} \int_v^\infty t dF(t),$$

these having corresponding probabilities $p = F(v)$ and $q = 1 - F(v)$; in other words we replace the velocity of every car slower or faster than our car by the average velocity of such cars. However in the case when the traffic density is large, this approximation is rather crude. To make this clear, let us mention that in general, when we have to slow down behind a slow car to let a faster car (which has already started overtaking us) pass, we may then be overtaken by another car whose speed is less than our own original speed. This also happens quite often in heavy traffic, as everyone who has some experience of driving on divided highways knows. However the above approximation excludes this possibility, and so gives too high an estimate of the average speed (i.e. too optimistic a view on the loss of speed). We intend to return to the general problem in another paper.

References

- [1] RYLL-NARDZEWSKI, C. (1954) Remarks on the Poisson stochastic process (III). *Studia Math.* 14, 314-318.
- [2] BREIMAN, L. (1962) On some probability distributions occurring in traffic flow. *Bull. I.S.I. Paris* 33, 155-161.
- [3] BREIMAN, L. (1963) The Poisson tendency in traffic distribution. *Ann. Math. Statist.* 34, 308-311.
- [4] HAMMERSLEY, J. M. (1962) The mathematical analysis of traffic congestion. *Bull. I.S.I. Paris* 33, 89-108.
- [5] DOOB, J. L. (1953) *Stochastic Processes*. John Wiley, New York, 404-407.
- [6] RÉNYI, A. (1956) A characterisation of the Poisson process (in Hungarian). *Publ. Math. Inst. Hung. Acad. Sci.* 1, 519-527.
- [7] BELAEV, J. K. (1963) Limit theorems for rearing random flows (in Russian). *Teor. Veroyat. Primen.* 8, 175-184.
- [8] NAWROTZKI, K. (1962) Ein Grenzwertsatz für homogene zufällige Punktfolgen (Verallgemeinerung eines Satzes von A. Rényi). *Math. Nachr.* 24, 202-218.
- [9] PRÉKOPA, A. (1958) On secondary processes generated by a random point distribution of Poisson type. *Ann. Univ. Sci. Budapest. Sect. Math.* I, 153-170.

NOTE

Instead of asymptotic results exact formulas were obtained by Brown [4]. The case of inhomogeneous traffic flow was treated by Mine and Ohno [1]. The ideas of Rényi's paper were used to investigate a different model in Brill (1971).

The property of Poisson processes expressed by Theorem 2 was discussed in Brown [3] and Srivastava [2]. (D. Sz.)

REFERENCES

- [1] Mine, H.—Ohno, K.: Low density inhomogeneous traffic flow. J. Appl. Prob. 7 (1970), 573—598.
- [2] Srivastava, R. C. : On a characterization of the Poisson process. J. Appl. Prob. 8 (1971), 615—616.
- [3] Brown, M.: An invariance property of Poisson process. J. Appl. Prob. 6 (1969), 453—458.
- [4] Brown, M. Some results on a traffic model of Rényi. J. Appl. Prob. 6 (1969), 293—300.

ON THE AMOUNT OF INFORMATION CONCERNING AN UNKNOWN PARAMETER IN A SEQUENCE OF OBSERVATIONS

by

ALFRÉD RÉNYI

Introduction

Let $\xi_1, \xi_2, \dots, \xi_n, \dots$ be a sequence of identically distributed random variables. We suppose that the common distribution of the random variables ξ_n depends on a parameter θ , which itself is also a random variable. In the present paper we restrict ourselves to the case when θ is a discrete random variable; we shall denote the possible different values of θ by $t_1, t_2, \dots, t_r$. We shall suppose further that the random variables ξ_n ($n = 1, 2, \dots$) are independent and identically distributed under each of the conditions $\theta = t_j$ ($j = 1, 2, \dots, r$) and denoting by $F_j(x)$ the conditional distribution function of the variables ξ_n under the condition $\theta = t_j$, we suppose that $F_j(x)$ and $F_h(x)$ are not identical if $j \neq h$. Let $\mathbf{P}(\theta = t_j) = w_j$ ($j = 1, \dots, r$) denote the prior probability of θ taking on the value t_j . Without restricting the generality we may suppose $w_j > 0$ for $j = 1, 2, \dots, r$. We denote by $I_n = I_n((\xi_1, \dots, \xi_n), \theta)$ the amount of information concerning the (unknown) value of θ contained in the sequence of random variables $\xi_1, \xi_2, \dots, \xi_n$. As well known (see [1], [2], [3]) I_n is defined by

$$(1) \quad I_n = I_n((\xi_1, \dots, \xi_n), \theta) = \mathbf{H}(\theta) - \mathbf{M}(\mathbf{H}(\theta | \xi_1, \dots, \xi_n)).$$

Here and in what follows for any (discrete) random variable η we denote by $\mathbf{H}(\eta)$ the *entropy* of η , i.e. if $y_1, \dots, y_r$ are the values taken on by η and $\mathbf{P}(\eta = y_j) = p_j$ ($j = 1, 2, \dots, r$) we put

$$(2) \quad \mathbf{H}(\eta) = \sum_{j=1}^r p_j \log \frac{1}{p_j}.$$

(Here and in what follows $\mathbf{P}(A)$ denotes the probability of the event A and $\log$ denotes the logarithm with base 2.) If ζ is an other random variable we denote by $\mathbf{H}(\eta | \zeta)$ the *conditional entropy* of η given the value of ζ , i.e. we put

$$(3) \quad \mathbf{H}(\eta | \zeta) = \sum_{j=1}^r \mathbf{P}(\eta = y_j | \zeta) \log \frac{1}{\mathbf{P}(\eta = y_j | \zeta)}$$

where $\mathbf{P}(A | \zeta)$ denotes the conditional probability of the event A given the value of ζ . $\mathbf{H}(\eta | \zeta)$ is of course itself a random variable, as its value depends on the value taken on by ζ . We denote by $\mathbf{M}(\dots)$ the mean value of the random variable in the brackets. Thus $\mathbf{M}(\mathbf{H}(\theta | \xi_1, \dots, \xi_n))$ denotes the average

uncertainty which remains with respect to Θ after observing the values $\xi_1, \xi_2, \dots, \xi_n$.

The first author suggesting the use of the quantity I_n in statistical problems was — according to our knowledge — D. V. LINDLEY [4].

The aim of the present paper is to prove that for $n \rightarrow \infty$ I_n tends to $\mathbf{H}(\Theta)$ in such a way that there exist constants $A > 0$ and q ($0 < q < 1$) so that

$$(4) \quad 0 \leq \mathbf{H}(\Theta) - I_n \leq Aq^n$$

and to consider some consequences of this fact.

§ 1. Estimation of the amount of information obtained from observations

We shall restrict ourselves to the case when the random variables ξ_k have a finite discrete distribution. For the sake of the simplicity of notation we suppose that the possible values of the variables ξ_k are the integers $1, 2, \dots, s$. This is no essential restriction, because if the distribution of the variables ξ_k under condition $\Theta = t_j$ is different for each j , then one can find a Borel-measurable function $g(x)$ taking on only a finite number of different values, such that the conditional distribution of the variables $g(\xi_k) = \xi_k^*$ under condition $\Theta = t_j$ is different for each j and one has evidently

$$(1.1) \quad I_n((\xi_1, \dots, \xi_n), \Theta) \geq I_n((\xi_1^*, \dots, \xi_n^*), \Theta).$$

Thus if we prove that

$$(1.2) \quad 0 \leq \mathbf{H}(\Theta) - I_n((\xi_1^*, \dots, \xi_n^*), \Theta) \leq Aq^n$$

this implies

$$(1.3) \quad 0 \leq \mathbf{H}(\Theta) - I_n((\xi_1, \dots, \xi_n), \Theta) \leq Aq^n$$

Moreover one has

$$(1.4) \quad I_n((\xi_1, \dots, \xi_n), \Theta) = \sup_g I_n((\xi_1^*, \dots, \xi_n^*), \Theta),$$

where the supremum has to be taken over all possible choices of the function g . By the way, this remark shows, that if we observe the random variables ξ_n with the single aim of collecting information with respect to Θ , we may round off in an appropriate way the observed values ξ_n with no serious loss of information.

We shall need an elementary inequality, contained in the following

Lemma. *There exists a universal constant $C > 0$ such that for any sequence $p_1, \dots, p_N$ of positive numbers forming a probability distribution (i.e. for which $p_1 + p_2 + \dots + p_N = 1$) we have*

$$(1.5) \quad \sum_{k=1}^N p_k \log \frac{1}{p_k} \leq C \sum_{k=2}^N \sqrt{p_k}.$$

Proof of the lemma. Clearly both $\frac{x \log \frac{1}{x}}{\sqrt{x}}$ and $\frac{(1-x) \log \frac{1}{1-x}}{\sqrt{x}}$ are continuous in the closed interval $[0, 1]$. Putting

$$(1.6) \quad C_1 = \text{Max}_{0 \leq x \leq 1} \frac{x \log \frac{1}{x}}{\sqrt{x}}$$

and

$$(1.7) \quad C_2 = \text{Max} \frac{(1-x) \log \frac{1}{1-x}}{\sqrt{x}}$$

we have

$$(1.8) \quad \sum_{k=2}^N p_k \log \frac{1}{p_k} \leq C_1 \sum_{k=2}^N \sqrt{p_k}$$

and

$$(1.9) \quad p_1 \log \frac{1}{p_1} \leq C_2 \sqrt{\sum_{k=2}^N p_k} \leq C_2 \sum_{k=2}^N \sqrt{p_k}.$$

Thus (1.5) follows with $C = C_1 + C_2$.

Now we are in the position to prove (4). We have

$$(1.10) \quad \mathbf{H}(\Theta) - I_n = \sum_{h=1}^r w_h \mathbf{M}(\mathbf{H}(\Theta | \xi_1, \dots, \xi_n) | \Omega_h)$$

where Ω_h denotes the subset of the full probability space Ω on which $\Theta = t_h$ ($h = 1, 2, \dots, r$) and $\mathbf{M}(\eta | B)$ denotes conditional expectation with respect to B , i.e.

$$(1.11) \quad \mathbf{M}(\eta | B) = \frac{1}{\mathbf{P}(B)} \int_B \eta d\mathbf{P}.$$

On the other hand by supposition, putting

$$(1.12) \quad \mathbf{P}(\xi_m = x | \Theta = t_j) = P_j(x) \quad (x = 1, 2, \dots, s)$$

we have by BAYES theorem

$$(1.13) \quad \mathbf{P}(\Theta = t_j | \xi_1, \dots, \xi_n) = \frac{w_j \prod_{k=1}^n P_j(\xi_k)}{\sum_{l=1}^r w_l \prod_{k=1}^n P_l(\xi_k)} \leq \frac{w_j}{w_h} \prod_{k=1}^n \frac{P_j(\xi_k)}{P_h(\xi_k)}.$$

It follows by our lemma

$$(1.14) \quad \mathbf{H}(\Theta | \xi_j, \dots, \xi_n) \leq C \sum_{\substack{j=1 \\ j \neq h}}^r \sqrt{\frac{w_j}{w_h}} \cdot \prod_{k=1}^n \sqrt{\frac{P_j(\xi_k)}{P_h(\xi_k)}}$$

and thus in view of the conditional independence of the variables ξ_k on Ω_h

$$(1.15) \quad \mathbf{M}(\mathbf{H}(\Theta \mid \xi_1, \dots, \xi_n) \mid \Omega_h) \leq C \sum_{\substack{j=1 \\ j \neq h}}^r \sqrt{\frac{w_j}{w_h}} \left[\mathbf{M} \left(\sqrt{\frac{P_j(\xi_1)}{P_h(\xi_1)}} \mid \Omega_h \right) \right]^n.$$

Now clearly

$$(1.16) \quad \mathbf{M} \left(\sqrt{\frac{P_j(\xi_1)}{P_h(\xi_1)}} \mid \Omega_h \right) = \sum_{l=1}^s \sqrt{P_j(l) P_h(l)} = q_{jh}.$$

By Cauchy's inequality and in view of the supposition that the distributions $\{P_j(l)\}$ and $\{P_h(l)\}$ are different for $j \neq h$ we obtain $0 \leq q_{jh} < 1$. Thus putting

$$(1.17) \quad q = \max_{1 \leq j < h \leq r} q_{jh}$$

we have $q < 1$, and it follows from (1.10), (1.15), (1.16) and (1.17), further from (1.14) that

$$(1.18) \quad \mathbf{M}(\mathbf{H}(\Theta \mid \xi_1, \dots, \xi_n)) \leq Aq^n$$

with

$$(1.19) \quad A = C \sum_{j=1}^r \sum_{\substack{h=1 \\ h \neq j}}^r \sqrt{w_j w_h} \leq C(r-1).$$

Thus we have proved the following

Theorem 1. *Let Θ be a discrete random variable taking on r different values $t_1, t_2, \dots, t_r$ with positive probabilities $w_j = \mathbf{P}(\Theta = t_j)$ ($j = 1, 2, \dots, r$). Let us suppose that the discrete random variables $\xi_1, \xi_2, \dots, \xi_n, \dots$ are for each j ($1 \leq j \leq r$) independent and identically distributed under the condition that $\Theta = t_j$ and let us suppose that the conditional distribution of the variables ξ_n under condition $\Theta = t_j$ is different for each j . Then, denoting by I_n the amount of information on Θ obtained from observing the values of $\xi_1, \xi_2, \dots, \xi_n$, we have*

$$(1.20) \quad \lim_{n \rightarrow \infty} I_n = \mathbf{H}(\Theta) = \sum_{j=1}^r w_j \log \frac{1}{w_j};$$

moreover the rate of convergence in (1.20) is exponential, i.e. there exist positive constants A and $q < 1$ such that

$$0 \leq \mathbf{H}(\Theta) - I_n \leq Aq^n \quad (n = 1, 2, \dots).$$

As $\mathbf{H}(\Theta)$ is the full information missing on Θ [i.e. the total uncertainty concerning Θ before observing the values of ξ_k ($k = 1, 2, \dots$)] the result (1.20) expresses that the sequence of observations $\xi_1, \xi_2, \dots, \xi_n, \dots$ gives us — at least in the limit — total information on the unknown value of the parameter. This leads one to guess that there exists a decision function depending only on the observed values $\xi_1, \dots, \xi_n, \dots$ which leads *almost surely* to a correct decision concerning the value of Θ . This will be shown in the next §.

§ 2. Construction of an almost surely reliable decision function

If we have to decide after observing $\xi_1, \xi_2, \dots, \xi_n$ what is the most plausible value t_j of Θ , the most natural decision is to decide for that value t_j of Θ for which $P(\Theta = t_j | \xi_1, \dots, \xi_n)$ is maximal. Note that this is not quite the same as the decision suggested by the maximum likelihood principle which suggests to choose that value t_j of Θ for which $\prod_{k=1}^n P_j(\xi_k)$ is the largest, though for large values of n the two decisions coincide with probability near to 1. Let us put

$$(2.1) \quad \Delta_n = t_j \text{ if } \max_h P(\Theta = t_h | \xi_1, \dots, \xi_n) = P(\Theta = t_j | \xi_1, \dots, \xi_n).$$

(Of course the decision Δ_n is not necessarily unambiguous but as will be seen below it will be such with probability 1 if n is sufficiently large.) Thus if we take a sequence of observations $\xi_1, \xi_2, \dots, \xi_n, \dots$ we get a sequence of decisions $\Delta_1, \Delta_2, \dots, \Delta_n, \dots$. Clearly to each sequence of observations $\xi_1, \dots, \xi_n, \dots$ there corresponds a "true" value of Θ . Now we prove

Theorem 2. *With probability 1 all but a finite number of the decisions Δ_n are unambiguous and equal to the true value of the parameter Θ .*

Proof of Theorem 2. Evidently

$$(2.2) \quad P(\Delta_n \neq \Theta) \leq \sum_{h=1}^r \sum_{\substack{j=1 \\ j \neq h}}^r w_h P\left(\frac{P(\Theta = t_j | \xi_1, \dots, \xi_n)}{P(\Theta = t_h | \xi_1, \dots, \xi_n)} \geq 1 \mid \Omega_h\right).$$

By Markoff's inequality:

$$(2.3) \quad P(\eta \geq \lambda M(\eta)) \leq \frac{1}{\lambda}$$

valid for any nonnegative random variable η and any $\lambda > 1$, and in view of

$$(2.4) \quad \frac{P(\Theta = t_j | \xi_1, \dots, \xi_n)}{P(\Theta = t_h | \xi_1, \dots, \xi_n)} = \frac{w_j}{w_h} \prod_{k=1}^n \frac{P_j(\xi_k)}{P_h(\xi_k)}$$

and taking (1.16) into account, we obtain

$$(2.5) \quad P(\Delta_n \neq \Theta) \leq \sum_{h=1}^r w_h \sum_{\substack{j=1 \\ j \neq h}}^r \sqrt{\frac{w_j}{w_h}} q_{jh}^n \leq Bq^n$$

where

$$B = \sum_{h=1}^r \sum_{\substack{j=1 \\ j \neq h}}^r \sqrt{w_j w_h} = \left(\sum_{j=1}^r \sqrt{w_j} \right)^2 - 1 \leq r - 1$$

and q is defined by (1.17).

Thus it follows that the series

$$(2.6) \quad \sum_{n=1}^{\infty} P(\Delta_n \neq \Theta)$$

is convergent. Applying the BOREL—CANTELLI lemma it follows that with probability 1 $\Delta_n = \Theta$ for sufficiently large values of n . This proves Theorem 2.

Of course if ν denotes the least integer such that $\Delta_n = \Theta$ for $n \geq \nu$ then we get from Theorem 2 that the random variable ν is almost everywhere finite, but this does not mean that ν is bounded. However it is easy to prove that the expectation of ν is finite. As a matter of fact

$$(2.7) \quad \mathbf{P}(\nu \geq m) \leq \sum_{n=m}^{\infty} \mathbf{P}(\Delta_n \neq \Theta) \leq \frac{Bq^m}{1-q}$$

and thus the series

$$(2.8) \quad \mathbf{M}(\nu) = \sum_{m=1}^{\infty} \mathbf{P}(\nu \geq m)$$

is convergent; from (2.7) we even get the estimate

$$(2.9) \quad \mathbf{M}(\nu) \leq \frac{Bq}{(1-q)^2}.$$

Of course this does not mean that one can determine the true value of Θ from a finite number of observations with probability 1, because even if Δ_n is equal to the same value t_j , for $n \geq M$, if we stop observing the ξ_n -s with the observation ξ_{M+N} we can not be quite sure whether Δ_n would have remained equal to t_j if we would have continued the observations. Of course the probability of this event will be arbitrarily small if $M + N$ is sufficiently large.

For the discussion of the case when Θ has a continuous distribution other methods are needed. We intend to return to this problem in an other paper.

§ 3. Some further remarks

In the present paper we have taken the Bayesian point of view, which — as has been pointed out already by LINDLEY (see [4]) — is the natural point of view if one wants to compute the amount of information on a parameter furnished by some observations, this quantity being dependent on the prior distribution of this parameter. In this connection we want to emphasize that as the inequalities

$$0 \leq \mathbf{H}(\Theta) - I_n \leq C(r-1)q^n$$

and

$$\mathbf{P}(\Delta_n \neq \Theta) \leq (r-1)q^n$$

hold *uniformly* for all possible prior distributions $\{w_j\}$, our results are meaningful even in the case when nothing is known about the prior distribution.

It should be added finally that the random variables $\xi_1, \xi_2, \dots, \xi_n, \dots$ considered in this paper, while being independent on each subspace Ω_h of the total probability space Ω , are dependent on Ω , but in a particularly simple way: they are equivalent (symmetrically dependent); as a matter of fact if $n_1 < n_2 < \dots < n_k$ we have

$$\mathbf{P}(\xi_{n_1} = x_1, \xi_{n_2} = x_2, \dots, \xi_{n_k} = x_k) = \sum_{h=1}^r w_h \prod_{l=1}^k P_h(x_l)$$

and thus this probability does not depend on the choice of the indices $n_1, n_2, \dots, n_k$.

Thus the values $\xi_1, \dots, \xi_n, \dots$ may be considered as a sequence of signals emitted by a stationary source of a particularly simple type which may be called a *source with equivalent signals*. We shall return to the corresponding problem for an arbitrary stationary source in an other paper.

Finally we want to call attention to the information-theoretical meaning of the quantities q_{jh} defined by (1.16). Some years ago we have introduced (see [5], [6], [7]) the notion of the entropy of order α ($0 < \alpha < +\infty$) of a probability distribution $\mathcal{S} = (p_1, \dots, p_r)$ which is defined for $\alpha \neq 1$ by the formula

$$(3.1) \quad H_\alpha(\mathcal{S}) = \frac{1}{1-\alpha} \log \left(\sum_{k=1}^r p_k^\alpha \right).$$

We define $H_1(\mathcal{S})$ by passing to the limit in (3.1), i.e. we put

$$(3.2) \quad H_1(\mathcal{S}) = \lim_{\alpha \rightarrow 1} H_\alpha(\mathcal{S}) = \sum_{k=1}^r p_k \log \frac{1}{p_k}.$$

Thus $H_1(\mathcal{S})$ is equal to SHANNON's entropy of the distribution $\mathcal{S}$.

Similarly we have introduced the notion of "information gain" of order α obtained if the prior distribution $\mathcal{S} = (p_1, \dots, p_r)$ is replaced by the posterior distribution $\mathcal{Q} = (q_1, \dots, q_r)$ defined for $\alpha \neq 1$ by the formula

$$(3.3) \quad I_\alpha(Q \parallel \mathcal{S}) = \frac{1}{\alpha-1} \log \left(\sum_{k=1}^r q_k^\alpha p_k^{1-\alpha} \right).$$

If we define $I_1(Q \parallel \mathcal{S})$ again by passing to the limit in (3.3), we obtain

$$(3.4) \quad I_1(Q \parallel \mathcal{S}) = \lim_{\alpha \rightarrow 1} I_\alpha(Q \parallel \mathcal{S}) = \sum_{k=1}^r q_k \log \frac{q_k}{p_k}$$

i.e. $I_1(Q \parallel \mathcal{S})$ is given by the familiar formula for information-gain.

Now clearly

$$q_{jk}^2 = 2^{-I_{1/2}(P_k \parallel P_j)}$$

where $P_l = \{P_l(1), \dots, P_l(s)\}$ is the conditional distribution of the variables ξ_n under the condition $\Theta = t_l$ ($l = 1, 2, \dots, r$).

Similarly the constant B figuring in (2.5) can be expressed by the formula

$$B = 2^{H_{1/2}(W)} - 1$$

where $W = (w_1, \dots, w_r)$ is the prior distribution of the random variable Θ .

Let us mention that the quantity $I_{1/2}(Q \parallel \mathcal{S})$ as a measure of the discrepancy between the distributions Q and $\mathcal{S}$ has been considered earlier by A. BHATTACHARYYA [8] and H. JEFFREYS [9].

Thus the situation can be characterized as follows: though we accepted as a measure of the amount of information in the sample $(\xi_1, \dots, \xi_n)$ SHANNON's usual measure (of order $\alpha = 1$) nevertheless in course of the proof the

measure of order $\alpha = \frac{1}{2}$ of information gain and of entropy resp. entered our considerations for purely technical reasons. (See also [10], [11] and [12].)

Note that instead of $\alpha = 1/2$ any value of α such that $0 < \alpha < 1$ could have been used. The value of α which leads to the least value of q depends in general on the conditional distributions P_l ($l = 1, 2, \dots, r$). However, in the present paper we did not aim at finding the least possible value of q only to prove that such a value less than 1 exists, therefore for the sake of simplicity we have chosen $\alpha = \frac{1}{2}$.

REFERENCES

- [1] KOLMOGOROFF, A. N.: "Theorie der Nachrichtenübermittlung." *Arbeiten zur Informationstheorie* I. 91–114. Deutscher Verlag der Wissenschaften, Berlin, 1957.
- [2] GELFAND, I. M.—JAGLOM, A. M.—KOLMOGOROFF, A. N.: "Zur allgemeinen Definition der Information." *Arbeiten zur Informationstheorie* II. 57–60. Deutscher Verlag der Wissenschaften, Berlin, 1958.
- [3] CHIANG TSE-PEI: "Eine Bemerkung zur Definition der Information." *Arbeiten zur Informationstheorie* II. 61–64. Deutscher Verlag der Wissenschaften, Berlin, 1958.
- [4] LINDLEY, D. V.: "On a measure of the information provided by an experiment." *Annals of Math. Stat.* **27** (1956), 986–1005.
- [5] RÉNYI, A.: "Az információelmélet néhány alapvető kérdése." *MTA III. Oszt. Közl.* **10** (1960) 251–282.
- [6] RÉNYI, A.: "Dimension, entropy and information." *Transactions of the 2nd Prague Conference on Information theory* (1960) 545–556.
- [7] RÉNYI, A.: "On measures of entropy and information." *Proceedings of the 4th Berkeley Symposium on Math. Stat. and Prob.* (1960) 547–561.
- [8] BHATTACHARYYA, A.: "On some analogues of the amount of information and their use in statistical estimation." *Sankhya* **8** (1946) 1–14.
- [9] JEFFREYS, H.: *Theory of probability* (2nd edition). Oxford, Clarendon Press, 1948.
- [10] KULLBACK, S.: *Information theory and statistics*. Wiley, 1959.
- [11] CHERNOFF, H.: "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations." *Bull. Amer. Math. Soc.* **23** (1952) 493–507.
- [12] RÉNYI, A.: "Az információ-akkumuláció statisztikus törvényszerűségeiről." *MTA III. o. Közl.* **12** (1962) 15–33.

236, 265, 266, 267, 285, 288, 305, 328

ON THE AMOUNT OF INFORMATION IN A FREQUENCY-COUNT

ALFRÉD RÉNYI

*Mathematical Institute of the Hungarian Academy of Sciences
Budapest, Hungary*

Let us consider the following basic problem of statistics. Let $\xi_1, \xi_2, \dots, \xi_n, \dots$ be a sequence of identically distributed random variables the common distribution of which depends on a parameter θ , which may take on a finite number of different values $t_1, t_2, \dots, t_r$. Let us suppose that the variables ξ_n ($n = 1, 2, \dots$) are independent and identically distributed under the condition $\theta = t_j$ for $j = 1, 2, \dots, r$ and that the conditional distribution of the variables ξ_n under the condition $\theta = t_j$ is different for different values of j . It is natural to ask how much information is contained in the sample $(\xi_1, \xi_2, \dots, \xi_n) = h_n$ concerning the parameter θ ?

This question admits a definite answer only if θ is considered as a random variable, and the answer depends also on the prior distribution of θ . Thus in order that one should be able to evaluate the accumulation of information during sampling in the sense of information theory one has to take the Bayesian point of view.

Let us therefore suppose that θ is a discrete random variable having the prior distribution $P(\theta = t_j) = W_j$ ($j = 1, 2, \dots, r$).

In this case, denoting by $I_n = I(h_n, \theta)$ the amount of information on θ contained in the sample $h_n = (\xi_1, \xi_2, \dots, \xi_n)$, one has [1]

$$I_n = H(\theta) - E(H(\theta | h_n)) \quad (1)$$

where $H(\theta)$ is the entropy of θ , i.e.

$$H(\theta) = \sum_{j=1}^r W_j \log \frac{1}{W_j}. \quad (2)$$

(here and in what follows $\log$ always denotes logarithm with base 2) and $H(\theta | h_n)$ is the entropy of the conditional distribution of θ given h_n , i.e.

$$H(\theta | h_n) = \sum_{j=1}^r P(\theta = t_j | h_n) \log \frac{1}{P(\theta = t_j | h_n)} \quad (3)$$

and $E(\dots)$ denotes the expectation of the random variable in the brackets.

Clearly if there exists a sufficient statistic $\eta_n = \psi_n(\xi_1, \dots, \xi_n)$ for θ then $H(\theta | h_n) = H(\theta | \eta_n)$ because

$$P(\theta = t_j | h_n) = P(\theta = t_j | \eta_n) \quad \text{for } j = 1, 2, \dots, r,$$

and thus

$$I(h_n, \theta) = I(\eta_n, \theta)$$

Recently (see [2]) I have proved that

$$\lim_{n \rightarrow \infty} I_n = H(\theta) \quad (4)$$

moreover that there exist constants A and λ with $A > 0$ and $0 < \lambda < 1$ such that

$$0 \leq H(\theta) - I_n \leq A\lambda^n \quad (n = 1, 2, \dots) \quad (5)$$

The problem presents itself to find the lower bound of those values of λ for which (5) holds. In the present paper we shall solve this problem for the special case when the parameter θ has only two possible values θ_1 and θ_2 and the random variables ξ_n take on only the values 0 and 1, i.e. when we consider a frequency count.

In what follows we suppose that θ takes on only the values t_1 and t_2 and

$$P(\xi_n = 1 | \theta = t_j) = p_j, \quad P(\xi_n = 0 | \theta = t_j) = q_j = 1 - p_j \quad (j = 1, 2) \quad (6)$$

and that the numbers P_1 and P_2 are different. For this special case it follows from our general result proved in [2] that (5) holds with

$$\lambda = \sqrt{p_1 p_2} + \sqrt{q_1 q_2}. \quad (7)$$

In what follows we shall find the best possible value of λ for the special case considered.

In our special case the frequency $\eta_n = \xi_1 + \xi_2 + \dots + \xi_n$ is clearly a sufficient statistic for the parameter θ and one has

$$P(\theta = t_i | \eta_n = k) = \frac{p_i^k q_i^{n-k} W_i}{p_1^k q_1^{n-k} W_1 + p_2^k q_2^{n-k} W_2} \quad (i = 1, 2) \quad (8)$$

and thus

$$E(H(\theta | \eta_n)) = A_n + B_n \quad (9)$$

where

$$A_n = W_1 \sum_{k=0}^n \binom{n}{k} p_1^k q_1^{n-k} \log \left(1 + \left(\frac{p_2}{p_1} \right)^k \left(\frac{q_2}{q_1} \right)^{n-k} \frac{W_2}{W_1} \right) \quad (9')$$

and

$$B_n = W_2 \sum_{k=0}^n \binom{n}{k} p_2^k q_2^{n-k} \log \left(1 + \left(\frac{p_1}{p_2} \right)^k \left(\frac{q_1}{q_2} \right)^{n-k} \frac{W_1}{W_2} \right) \quad (9'')$$

The second sum B_n on the right of (9) can be obtained from the first sum A_n by interchanging p_1 with p_2 , q_1 with q_2 and W_1 with W_2 . Thus in estimating $E(H(\theta | \eta_n))$ we may restrict ourselves to the first sum A_n on the right of (9).

Let us suppose first that $p_1 < p_2$; this of course implies $q_1 > q_2$.

We introduce the following notation

$$\Delta(x, y) = x \log \frac{x}{y} + (1 - x) \log \frac{1 - x}{1 - y} \quad (10)$$

for

$$0 \leq x \leq 1, 0 \leq y \leq 1.$$

Clearly $\Delta(x, y) \geq 0$ with equality if and only if $x = y$

Let us denote by ρ the unique solution of the equation

$$\Delta(\rho, p_1) = \Delta(\rho, p_2) \quad (11)$$

Evidently (11) can be written in the form

$$\rho \log \frac{1}{p_1} + (1 - \rho) \log \frac{1}{q_1} = \rho \log \frac{1}{p_2} + (1 - \rho) \log \frac{1}{q_2} \quad (11')$$

and is a linear equation in ρ , the solution of which is given by

$$\rho = \frac{\log \frac{q_1}{q_2}}{\log \frac{p_2 q_1}{p_1 q_2}} \quad (12)$$

It follows

$$0 \leq p_1 < \rho < p_2 \leq 1 \quad (13)$$

Let us denote further by $d(p_1, p_2)$ the common value of $\Delta(\rho, p_1)$ and $\Delta(\rho, p_2)$. Thus we put

$$d(p_1, p_2) = \Delta(\rho, p_1) = \Delta(\rho, p_2) \quad (14)$$

with ρ given by (12).

Using for $\frac{k}{n} \leq \rho$ the inequality $\log(1+x) \leq x$ valid for $0 \leq x \leq 1$ and for $\frac{k}{n} > \rho$ the inequality

$$\log(1+x) \leq \log x + 1 \quad (x \geq 1)$$

it follows, taking into account that the series

$$\sum_{l=-\infty}^{+\infty} b^l \log(1 + ca^l)$$

is convergent if $|b| > 1$ and $|ab| < 1$, that

$$A_n = O\left(\frac{1}{\sqrt{n}} \cdot 2^{-d(p_1, p_2)n}\right) \quad (15)$$

On the other hand, putting $k_0 = [n\rho] + 1$, the term of index $k = k_0$ of A_n has the same order of magnitude as that given by the right-hand side of (15). It follows that putting

$$\lambda = 2^{-d(p_1, p_2)} \quad (16)$$

one has

$$H(\theta) - I_n = O(\lambda^n) \quad (17)$$

and λ given by (16) is the least number for which (17) holds.

$$\lambda = \min_{0 < t < 1} (p_1^t p_2^{1-t} + q_1^t q_2^{1-t})$$

Clearly for the second sum B_n of (9) we obtain the same estimates as for A_n because the estimate obtained for A_n is symmetrical in p_1 and p_2 .

Thus we have proved the following

Theorem. The least value of λ for which (17) holds is the number λ defined by (16) with

$$d(p_1, p_2) = \Delta(\rho, p_1) = \Delta(\rho_1 p_2)$$

where ρ is given by (12).

Remark 1. It is easy to show that $d(p_1, p_2)$ increases from 0 to $\log \frac{1}{p_1}$, i.e. λ decreases from 1 to p_1 if p_2 increases from p_1 to 1. It follows from (7) that

$$2^{-d(p_1, p_2)} \leq \sqrt{p_1 p_2} + \sqrt{q_1 q_2} \quad (18)$$

Remark 2. For the special case when $p_1 = q_2 = p$, $q_1 = p_2 = q = 1 - p$ with $p \neq \frac{1}{2}$ one has $\rho = \frac{1}{2}$ and $d(p, 1 - p) = \log \frac{1}{2 \sqrt{p q}}$ i.e. $\lambda = 2 \sqrt{p q}$. Thus in this case we have equality in (18).

Thus the result of this paper shows that there exist cases in which the inequality given in [2] is best possible as regards the value of λ .

REFERENCES

1. D. V. Lindley. *On a measure of the information provided by an experiment.* Annals of Math. Stat. 27/1956/986—1005.
2. A. Rényi. *On the amount of information in a sample concerning a parameter.* Publications of the Mathematical Institute of the Hungarian Academy of Sciences 9(1964)617-624.

DISCUSSION

YU. V. LINNIK. A question on the optimal values of the parameter λ .

A. RÉNYI. The best value of λ is given by formula (16) in my paper.

231, 265, 266, 267, 285, 288, 305, 328

Sur les espaces simples des Probabilités conditionnelles

par

Alfred RÉNYI
(Budapest).

Avertissement

par Maurice FRÉCHET
(Paris).

Il y a quelques années, M. Rényi avait fait à Paris un exposé qui m'avait vivement frappé. Je lui avais dit que ses très remarquables contributions à divers chapitres du Calcul des Probabilités viendraient se placer à côté d'autres importantes contributions dues à divers auteurs, tandis que sa conception entièrement nouvelle ⁽¹⁾ de ce que j'appellerai ses « probabilités généralisées » apporte un aspect fondamentalement distinct aux fondements du Calcul des Probabilités. Depuis lors, M. Rényi a donné des exposés très complets de sa théorie en différentes langues.

Je l'ai plusieurs fois invité à donner un article en français donnant une idée simple de sa théorie.

M. Rényi a bien voulu y consentir et se limite dans ce Mémoire à l'étude de ce qu'il appelle (p. 7) un espace *simple* de probabilités conditionnelles.

Avant de lui donner la parole, je voudrais prévenir le lecteur contre un malentendu possible. A lire le texte qui suit, on pourrait penser qu'il y a

⁽¹⁾ Toutefois, M. Rényi a appris, assez récemment, que M. Kolmogoroff a émis des idées analogues dans une conférence qui n'a pas été publiée.

dans ce texte deux innovations : 1° on renoncerait aux probabilités absolues pour se limiter aux probabilités *conditionnelles*; 2° une probabilité généralisée de l'événement A sous la condition B est de la forme

$$(I.13) \quad P(A | B) = \frac{\mu(AB)}{\mu(B)},$$

où $\mu(B)$ n'est pas borné quand B varie.

Or si l'on parle souvent, pour abrégé, de la probabilité $P(A)$ d'un événement A, comme s'il s'agissait d'une probabilité absolue, en réalité, l'expression n'a pas de sens par elle-même. Que l'auteur le précise ou non, les probabilités dont il parle sont toujours relatives à ce que j'ai appelé dans toutes mes publications « Une certaine catégorie d'épreuves » B ou ce que d'autres auteurs ont explicité d'une autre façon.

De sorte que l'innovation essentielle de M. Rényi réside dans l'hypothèse que dans la formule (I.13) (de la p. 12), la mesure $\mu(B)$ n'est pas bornée.

M. Rényi a bien voulu m'écrire : « Vous avez parfaitement raison en disant que la théorie des champs de probabilités conditionnelles ne fournit au fond de résultat nouveau que si la mesure μ [dans la formule (I.13)] n'est pas bornée ».

Pour voir comment cette hypothèse permet de donner un sens à des probabilités qui n'en avaient pas, je crois que le lecteur ferait bien, avant de lire en détail le texte qui suit, de voir les deux excellents exemples donnés pages 16-17, par M. Rényi.

Exposé d'Alfred RÉNYI

RÉSUMÉ. — Il y a quelques années, l'auteur a proposé une théorie axiomatique des espaces des probabilités conditionnelles (voir [2] à [6], qui est une généralisation naturelle de la théorie axiomatique des probabilités due à M. Kolmogoroff [1]. Dans le présent Mémoire, le cas spécial le plus simple des espaces des probabilités conditionnelles ayant une seule mesure génératrice, non bornée est élaboré d'une façon détaillée.

SUMMARY. — Some years ago the author (see [2]-[6]) proposed an axiomatic theory of conditional probability spaces, which is a natural generalization of the axiomatic theory of probability due to A. N. Kolmogoroff [1]. In the present note the most simple special case of conditional probability spaces generated by a single unbounded measure is worked out in detail.

Introduction. — Il y a quelques années j'ai élaboré une théorie axiomatique des espaces des probabilités conditionnelles ⁽¹⁾, qui est une généralisation naturelle de la théorie axiomatique des probabilités aujourd'hui généralement acceptée, due à M. Kolmogoroff ⁽²⁾ [1]. Cette théorie générale est basée, comme celle de M. Kolmogoroff, sur la théorie des ensembles et de la mesure; les événements aléatoires sont représentés de la même façon par les sous-ensembles mesurables d'un espace abstrait. Une différence principale consiste en ce que les probabilités conditionnelles sont exprimées dans ma théorie par l'intermédiaire d'une mesure qui peut être non bornée; tandis que, dans la théorie classique, seulement les mesures bornées sont admises. Il y a aussi une autre différence qui est plutôt d'ordre didactique. Ceci correspond au fait qu'en réalité chaque probabilité est conditionnelle. La question : quelle est la valeur de la probabilité d'un événement aléatoire ? n'a de sens exact que si l'on précise les conditions sous lesquelles cet événement est observé. Comme M. M. Fréchet l'a formulé (*voir* [7], p. 5-10), la probabilité d'un événement n'a un sens que « dans une certaine catégorie d'épreuves ». Par exemple, si l'on parle de la probabilité de tirer une carte donnée d'un paquet de cartes, il est sous-entendu que ce paquet est bien mêlé et contient une de toutes les cartes possibles. Mais cela s'entend sans dire, et les probabilités calculées sous cette condition ne sont pas appelées probabilités conditionnelles, bien qu'elles le soient. Le fait que toute probabilité est conditionnelle est contenu seulement d'une manière implicite dans la théorie classique, mais il est exprimé d'une façon explicite dans la mienne.

En général, en appliquant la théorie de M. Kolmogoroff à une situation réelle, on choisit toujours quelques conditions (circonstances) données comme fondamentales et les probabilités calculées sous ces conditions sont appelées les probabilités ordinaires (ou absolues) sans faire allusion aux conditions fixées. C'est seulement si à ces conditions il s'ajoute une nouvelle condition complémentaire, qu'on parle des probabilités conditionnelles; mais, malgré cet emploi des mots usuels, en principe chaque probabilité est conditionnelle. Ce fait a été souligné du point de vue philosophique par plusieurs auteurs, comme par exemple MM. Reichenbach [8], Popper [9], Keynes [10], Koopman [11], Copeland [12], Barnard [13], Good [14], mais

⁽¹⁾ Voir mes travaux ([2] à [6]).

⁽²⁾ Après avoir élaboré cette théorie, j'ai appris par M. B. V. Gnedenko que M. Kolmogoroff lui-même avait déjà indiqué dans une conférence, quelques années auparavant, la possibilité d'une telle généralisation de sa théorie, mais il n'avait rien publié sur ce sujet.

ces auteurs n'ont pas suivi cette idée jusqu'à la construction d'une théorie mathématique — comme celle de M. Kolmogoroff — fondée sur la théorie des ensembles et de la mesure. D'autres auteurs sont arrivés aux mêmes conclusions en partant des applications concrètes de la notion des probabilités. Il y a des situations réelles dans lesquelles il n'existe pas de condition susceptible d'être considérée comme naturelle ; chaque condition qu'on peut prendre comme fondamentale étant également arbitraire. Tel est le cas, par exemple, dans la psychologie des choix. La probabilité de choisir quelque chose dépend essentiellement de l'ensemble des alternatives possibles. Autrement dit, choisir cela signifie toujours, choisir un ensemble donné. Demander, par exemple, quelle est la probabilité qu'un consommateur choisisse un plat déterminé, n'a de sens que si l'ensemble des plats sur la carte est donné. Ces considérations ont conduit, par exemple, M. R. Luce [15], un peu plus tard, mais indépendamment de l'auteur de cette Note, à la notion d'espaces des probabilités conditionnelles spéciales.

Pour caractériser le point de départ d'un autre groupe de chercheurs, nous devons mentionner d'abord l'avantage le plus important, d'un point de vue strictement mathématique, de la théorie des probabilités conditionnelles. Comme il est bien connu, dans la théorie de Kolmogoroff, la probabilité conditionnelle $P(A | B)$ d'un événement A sous la condition que l'événement B a lieu (en bref : sous la condition B) est exprimé par la formule

$$(1) \quad P(A | B) = \frac{P(AB)}{P(B)},$$

où $P(B)$ est la probabilité de l'événement B , et $P(AB)$ celle de la réalisation conjointe des événements A et B . Étant donné que, dans la théorie de M. Kolmogoroff, les événements sont représentés par les sous-ensembles mesurables d'un espace abstrait, et la probabilité des événements est une mesure définie sur ces ensembles (en dénotant l'ensemble représentant un événement par la même lettre que cet événement, et en désignant l'intersection des deux ensembles par leur produit), on peut dire que la probabilité conditionnelle s'exprime dans la théorie de M. Kolmogoroff sous la forme

$$(2) \quad P(A | B) = \frac{\mu(AB)}{\mu(B)},$$

où A et B sont les sous-ensembles d'un espace Ω , AB désigne leur intersection et μ est une mesure. Cependant, dans la théorie de M. Kolmogoroff μ est toujours une mesure bornée, notamment une mesure normée par la condition $\mu(\Omega) = 1$. Par contre, notre théorie admet des cas où la pro-

babilité conditionnelle de l'événement A sous la condition B est exprimée par la formule (2), où μ est une mesure non bornée. Or, des cas où l'emploi d'une mesure qui n'est pas bornée semble être naturel se présentent justement dans des domaines différents, tels que la physique quantique, la statistique mathématique (en connexion avec la formule de Bayes), la géométrie intégrale et en connexion avec l'application des méthodes probabilistes dans la théorie des nombres. Dans ces cas, il est clair, pour des raisons purement mathématiques, que seulement des probabilités conditionnelles ont un sens et que les probabilités absolues ne peuvent pas être définies. Plusieurs auteurs, comme par exemple M. Jeffreys [16], M. Dumas ([17], [18]) et M. Baticle ([19], [20]) sont arrivés à la notion des espaces des probabilités conditionnelles dans des cas concrets. Mais ces auteurs n'ont pas essayé d'élaborer une théorie généralisée des probabilités où l'emploi de la formule (1) avec une mesure μ non bornée est admissible, ils ont utilisé de telles mesures d'une manière heuristique, étant satisfaits par le fait que ce mode de raisonnement conduit souvent à des résultats finaux raisonnables.

Jusqu'ici seulement les fondements de la théorie des espaces des probabilités conditionnelles sont élaborés. L'auteur a été encouragé à écrire ce travail par M. le Professeur Maurice Fréchet qui pensait que la publication en français d'un compte rendu de cette théorie (qui ne suppose pas la connaissance de mes travaux antérieurs sur ce sujet) peut être utile pour le développement ultérieur de cette théorie. En essayant de répondre à l'invitation obligeante de M. Fréchet qui me fait beaucoup d'honneur, j'ai pensé à élaborer d'une façon plus détaillée que dans mes publications précédentes, le cas spécial le plus simple et en même temps le plus important des espaces de probabilités conditionnelles, notamment celui des espaces des probabilités conditionnelles ayant une seule mesure génératrice, c'est-à-dire dans laquelle la probabilité conditionnelle $P(A | B)$ est pour chaque A et B donnée par la formule (2), où la mesure μ est toujours la même, et ne dépend pas de B , comme dans le cas général. Nous appellerons dans ce qui suit un tel espace un espace simple des probabilités conditionnelles.

En ce qui concerne quelques généralisations des théorèmes fondamentaux de la théorie des probabilités aux espaces des probabilités conditionnelles et quelques applications de la théorie de ces espaces (par exemple la théorie cinétique des gaz), le lecteur est renvoyé aux travaux de l'auteur déjà mentionnés; ici nous ne discutons que les notions fondamentales de cette théorie.

Dans le paragraphe 1 nous traitons un système d'axiomes pour les espaces simples des probabilités conditionnelles, et quelques questions de nature générale. Dans le paragraphe 2 nous nous occupons des cas spéciaux les plus intéressants. Dans le paragraphe 3 nous examinons le produit des

espaces simples des probabilités conditionnelles et l'indépendance conditionnelle des événements, et enfin dans le paragraphe 4 nous étudions les variables aléatoires sur un espace des probabilités conditionnelles et leurs fonctions de répartition et leurs densités de probabilité. Je remercie M. le Professeur Fréchet pour ses conseils concernant la rédaction de mon travail.

1. Un système d'axiomes de la théorie des espaces simples des probabilités conditionnelles. — Soit Ω un ensemble quelconque non vide; soit $\mathcal{A}$ une σ -algèbre des sous-ensembles de Ω , c'est-à-dire un système des sous-ensembles de Ω ayant les propriétés suivantes :

A 1. Si $A_1 \in \mathcal{A}$ et $A_2 \in \mathcal{A}$, alors $A_2 - A_1 \in \mathcal{A}$, où $A_2 - A_1$ désigne l'ensemble des éléments de Ω appartenant à A_2 , mais n'appartenant pas à A_1 .

A 2. Si $A_k \in \mathcal{A}$ ($k = 1, 2, \dots$) et $A = \sum_{k=1}^{\infty} A_k$ (où la somme des ensembles désigne leur union), alors $A \in \mathcal{A}$.

A 3. $\Omega \in \mathcal{A}$.

Il est clair que l'ensemble vide $\emptyset$ appartient à $\mathcal{A}$.

Soit $\mathcal{B}$ un sous-ensemble de $\mathcal{A}$ ayant les propriétés suivantes :

B 1. Si $B_1 \in \mathcal{B}$ et $B_2 \in \mathcal{B}$, alors $B_1 + B_2 \in \mathcal{B}$.

B 2. Il existe une suite B_n ($n = 1, 2, \dots$) d'ensembles tels que $B_n \in \mathcal{B}$ ($n = 1, 2, \dots$) et $\sum_{n=1}^{\infty} B_n = \Omega$.

B 3. L'ensemble vide n'appartient pas à $\mathcal{B}$.

Nous appellerons les systèmes d'ensembles avec les propriétés B 1, B 2 et B 3, des *bouquets* d'ensembles.

Supposons maintenant que $P(A | B)$ soit une fonction à valeurs réelles à deux variables définie pour $A \in \mathcal{A}$ et $B \in \mathcal{B}$, où $\mathcal{A}$ est une σ -algèbre des sous-ensembles de l'ensemble Ω et $\mathcal{B}$ est un sous-ensemble de $\mathcal{A}$ qui est un bouquet des ensembles, et supposons que $P(A | B)$ satisfait aux axiomes suivants :

P 1. $P(A | B)$ est comme fonction de A , une mesure ⁽³⁾ sur $\mathcal{A}$ pour chaque $B \in \mathcal{B}$ fixé.

P 2. $P(B | B) = 1$.

⁽³⁾ C'est-à-dire une fonction d'ensemble non négative et σ -additive.

P 3. Si $B \in \mathcal{B}$, $C \in \mathcal{B}$ et (*) $B \subset C$, on a

$$P(B | C) > 0,$$

et pour chaque $A \in \mathcal{A}$, on a

$$(1.1) \quad P(A | B) = \frac{P(AB | C)}{P(B | C)}.$$

Nous appellerons un tel système $[\Omega, \mathcal{A}, \mathcal{B}, P(A | B)]$ un *espace simple des probabilités conditionnelles*.

L'interprétation probabiliste d'un tel système est donnée par la terminologie suivante :

Nous appellerons les éléments ω de Ω des événements élémentaires, les ensembles A appartenant à $\mathcal{A}$ des événements aléatoires, Ω lui-même l'événement sûr et $\emptyset$ l'événement impossible, les ensembles B appartenant à $\mathcal{B}$ des conditions. Par conséquent, toute condition est un événement, mais il y a des événements qui ne sont pas des conditions; par exemple, l'événement impossible $\emptyset$ n'est pas une condition. Enfin, nous appellerons le nombre $P(A | B)$ la probabilité conditionnelle de l'événement A sous la condition B .

Ajoutons que la notion d'un espace simple des probabilités conditionnelles est plus restreinte que la notion d'un espace à probabilités conditionnelles, définie dans nos travaux ([2] à [6]). La différence entre ces deux notions consiste en ce qu'un espace de probabilités conditionnelles générales est un système $[\Omega, \mathcal{A}, \mathcal{B}, P(A | B)]$, où $\mathcal{B}$ est un sous-ensemble arbitraire non vide de $\mathcal{A}$ et l'on ne suppose pas qu'on ait $P(B | C) > 0$ pour $B \in \mathcal{B}$, $C \in \mathcal{B}$ et $B \subset C$, et la validité de la formule (1.1) est postulée seulement dans le cas où les deux membres ont un sens, c'est-à-dire si $P(B | C) > 0$. Deux conditions B_1 et B_2 telles que $P(B_1 | B_1 + B_2) \cdot P(B_2 | B_1 + B_2) > 0$ sont appelées *commensurables*. Dès lors, un espace simple des probabilités conditionnelles est un espace des probabilités conditionnelles dans lequel le système des conditions est un bouquet d'ensembles et où toutes les conditions sont commensurables.

En effet, si B_1 et B_2 sont des conditions quelconques, alors, d'après B 1 $B_1 + B_2$ est aussi une condition, et comme

$$B_1 \subset B_1 + B_2 \quad \text{et} \quad B_2 \subset B_1 + B_2,$$

ainsi d'après P 3, on a

$$P(B_1 | B_1 + B_2) > 0 \quad \text{et} \quad P(B_2 | B_1 + B_2) > 0.$$

(*) $B \subset C$ désigne que B est un sous-ensemble de C .

Dans ce travail, nous nous occupons seulement avec les espaces simples des probabilités conditionnelles.

Notons quelques conséquences simples des axiomes. En premier lieu, en prenant dans P 3, $B = C$, on obtient, d'après P 2,

$$(I.2) \quad P(A | B) = P(AB | B).$$

Étant donné que $P(A | B)$ est une mesure, c'est-à-dire une fonction d'ensemble A , non négative et σ -additive, on a

$$P(AB | B) \leq P(B | B) = 1.$$

Il s'ensuit que

$$0 \leq P(A | B) \leq 1 \quad \text{pour chaque } A \in \mathcal{A} \text{ et } B \in \mathcal{B}.$$

Fixons une condition $B \in \mathcal{B}$. Dans ce cas, $\mathcal{E}_B = [\Omega, \mathcal{A}, P(A | B)]$ est évidemment un espace des probabilités ordinaires au sens de Kolmogoroff. On en tire qu'un espace simple des probabilités conditionnelles est un système des différentes mesures de probabilités définies sur la même σ -algèbre $\mathcal{A}$ des sous-ensembles d'un espace Ω , liées entre elles par l'axiome P 3. D'ailleurs, P 3 est une condition de compatibilité dans le sens suivant. Soit B et C deux conditions, et $B \subset C$. Alors dans l'espace des probabilités de Kolmogoroff,

$$\mathcal{E}_C = [\Omega, \mathcal{A}, P(A | C)]$$

la probabilité conditionnelle $P(A | B)$ est définie précisément par la formule (I.1). Mais dans l'espace $[\Omega, \mathcal{A}, \mathcal{B}, P(A | B)]$ la probabilité conditionnelle $P(A | B)$ est supposée donnée auparavant. Donc P 3 exprime que les deux valeurs de $P(A | B)$ (l'une supposée donnée auparavant et l'autre après la définition des probabilités conditionnelles dans l'espace de Kolmogoroff $\mathcal{E}_C$) sont égales.

Nous démontrons maintenant le théorème suivant ⁽⁵⁾ :

THÉORÈME 1. — *Si $[\Omega, \mathcal{A}, \mathcal{B}, P(A | B)]$ est un espace simple des probabilités conditionnelles, alors il existe une mesure μ σ -finie sur $\mathcal{A}$ telle que pour chaque $B \in \mathcal{B}$, on a*

$$0 < \mu(B) < +\infty,$$

et pour chaque $A \in \mathcal{A}$ et $B \in \mathcal{B}$, on a

$$(I.3) \quad P(A | B) = \frac{\mu(AB)}{\mu(B)}.$$

La mesure μ est déterminée à un facteur constant près.

⁽⁵⁾ Pour un résultat plus général de ce type, voir le travail de M. A. Cszaszar [22].

Démonstration. — Soit $B_0 \in \mathcal{B}$ une condition arbitraire mais fixée. Posons pour chaque $B \in \mathcal{B}$

$$(I.4) \quad \mu(B) = \frac{P(B | B + B_0)}{P(B_0 | B + B_0)},$$

$\mu(B)$ est positive par hypothèse et finie pour tous les $B \in \mathcal{B}$.

Si $A \in \mathcal{A}$ est un ensemble, tel qu'il existe un $B \in \mathcal{B}$ tel que $A \subset B$, nous posons

$$(I.5) \quad \mu(A) = P(A | B) \mu(B).$$

Nous démontrons maintenant que la définition de $\mu(A)$ par (I.5) ne dépend pas du choix de B . Soit $A \subset B_i \in \mathcal{B}$ pour $i = 1, 2$. Ainsi il faut démontrer que

$$(I.6) \quad P(A | B_1) \mu(B_1) = P(A | B_2) \mu(B_2).$$

Soit $B_3 = B_1 + B_2$. Pour démontrer (I.6), il suffit de vérifier que

$$(I.7) \quad P(A | B_1) \mu(B_1) = P(A | B_3) \mu(B_3).$$

En effet, si (I.7) est valable, on a aussi par symétrie

$$(I.8) \quad P(A | B_2) \mu(B_2) = P(A | B_3) \mu(B_3)$$

et (I.7) et (I.8) entraînent (I.6).

Pour vérifier (I.7), nous utilisons l'axiome P 3. En vertu de cet axiome, nous avons

$$(I.9) \quad P(A | B_1) = \frac{P(A | B_3)}{P(B_1 | B_3)}$$

et, par conséquent, il ne reste à vérifier que

$$(I.10) \quad \mu(B_1) = P(B_1 | B_3) \mu(B_3).$$

Pour obtenir (I.10) nous appliquons l'axiome P 3 aux probabilités $P(B_1 | B_1 + B_0)$ et $P(B_0 | B_1 + B_0)$ et obtenons, d'après (I.4),

$$(I.11) \quad \mu(B_1) = \frac{P(B_1 | B_3 + B_0)}{P(B_3 | B_3 + B_0)} \mu(B_3).$$

Mais il suit aussi de l'axiome P 3 que

$$(I.12) \quad \frac{P(B_1 | B_3 + B_0)}{P(B_3 | B_3 + B_0)} = P(B_1 | B_3)$$

et nous obtenons ainsi (I.10). Ainsi (I.6) est aussi démontré. Nous obtenons comme cas particulier que (I.4) et (I.5) sont en accord, car si $A \in \mathcal{B}$, nous pouvons prendre $B = A$.

Soit $\mathcal{A}^*$ l'ensemble de tous les ensembles $A \in \mathcal{A}$ pour lesquelles il existe un $B \in \mathcal{B}$, tel que $A \subset B$.

$\mathcal{A}^*$ est évidemment un anneau des ensembles. En effet, si $A_1 \in \mathcal{A}^*$ et $A_2 \in \mathcal{A}^*$, alors $A_1 \subset B_1$ et $A_2 \subset B_2$ avec $B_i \in \mathcal{B}$ ($i = 1, 2$) il s'ensuit que $A_1 + A_2 \subset B_1 + B_2$ et comme, d'après B 1, $B_1 + B_2 \in \mathcal{B}$, donc $A_1 + A_2 \in \mathcal{A}^*$; si $A_1 \in \mathcal{A}^*$, $A_2 \in \mathcal{A}^*$ et si, de plus, $A_1 \subset B_1 \in \mathcal{B}$, on a aussi $A_1 - A_2 \subset B_1$ et, par conséquent, $A_1 - A_2 \in \mathcal{A}^*$. Nous démontrons maintenant que $\mu(A)$ est une mesure sur $\mathcal{A}^*$. $\mu(A)$ est évidemment non négatif.

Si $A_i \in \mathcal{A}^*$ ($i = 1, 2, \dots$) et $A_i A_j = \emptyset$ pour $i \neq j$ et $\sum_{i=1}^{\infty} A_i \in \mathcal{A}^*$, alors nous

pouvons trouver toujours par définition un $B \in \mathcal{B}$ tel que $\sum_{i=1}^{\infty} A_i \subset B$.

Puisqu'on a $A_i \subset B$ pour $i = 1, 2, \dots$, il s'ensuit de la σ -additivité de $P(A | B)$, considérée comme une fonction d'ensemble A que

$$\mu\left(\sum_{i=1}^{\infty} A_i\right) = P\left(\sum_{i=1}^{\infty} A_i | B\right) \mu(B) = \sum_{i=1}^{\infty} P(A_i | B) \mu(B) = \sum_{i=1}^{\infty} \mu(A_i).$$

$\mu(A)$ est donc vraiment une mesure sur $\mathcal{A}^*$. Soit maintenant $\sigma(\mathcal{A}^*)$ la plus petite σ -algèbre contenant $\mathcal{A}^*$. Dès lors (voir [21]), la définition de μ peut être étendue à $\sigma(\mathcal{A}^*)$ de telle façon que μ soit une mesure sur $\sigma(\mathcal{A}^*)$. Mais $\sigma(\mathcal{A}^*)$ est manifestement l'ensemble de tous les ensembles $A \in \mathcal{A}$ qui sont contenus dans l'union d'une suite dénombrable des ensembles $B_n \in \mathcal{B}$. Or, d'après notre axiome B 2, Ω même et, par conséquent, tous les $A \in \mathcal{A}$ sont contenus dans l'union d'une infinité dénombrable des ensembles $B_n \in \mathcal{B}$. $\mathcal{A}$ étant une σ -algèbre, $\sigma(\mathcal{A}^*) = \mathcal{A}$ et ainsi μ est une mesure σ -finie sur $\mathcal{A}$. Naturellement, $\mu(A)$ peut être égale à $+\infty$ pour certains ensembles $A \in \mathcal{A}$. D'autre part, comme pour chaque $A \in \mathcal{A}$ et $B \in \mathcal{B}$ on a $AB \subset B$ et ainsi $AB \in \mathcal{A}^*$, il s'ensuit de (1.2) et de (1.5) qu'on a pour chaque $A \in \mathcal{A}$ et $B \in \mathcal{B}$

$$(1.13) \quad P(A | B) = \frac{\mu(AB)}{\mu(B)},$$

où μ est une mesure σ -finie sur $\mathcal{A}$.

Il reste à montrer que la mesure μ est déterminée à un facteur positif constant près. Si ν est une autre mesure sur $\mathcal{A}$ et

$$\frac{\mu(AB)}{\mu(B)} = \frac{\nu(AB)}{\nu(B)}$$

pour chaque $A \in \mathcal{A}$ et $B \in \mathcal{B}$, alors en fixant B , il s'ensuit qu'on a

$$\nu(A) = C_B \mu(A) \quad \text{pour } A \in \mathcal{A}, A \subset B, \quad \text{où } C_B = \frac{\nu(B)}{\mu(B)}.$$

Considérons maintenant une suite B_n ($n = 1, 2, \dots$) telle que

$$B_n \in \mathcal{B} \quad \text{et} \quad \sum_{n=1}^{\infty} B_n = \Omega;$$

d'après B 3, une telle suite existe. Prenons maintenant pour B l'ensemble

$$\sum_{k=1}^n B_k, \text{ nous avons}$$

$$\nu(A) = C_n \mu(A) \quad \text{pour } A \in \mathcal{A}, A \subset \sum_{k=1}^n B_k,$$

où C_n est une constante positive. Comme $\sum_{k=1}^n B_k \subset \sum_{k=1}^{n+1} B_k$, il s'ensuit que les constantes C_n sont toutes égales, et par conséquent

$$(1.14) \quad \nu(A) = C \mu(A)$$

pour l'anneau des ensembles A pour lesquelles il existe un nombre tel que

$$A \subset \sum_{k=1}^n B_k. (1.14) \text{ est donc aussi valable pour tous les ensembles } A \text{ qui}$$

appartiennent à la plus petite σ -algèbre contenant cet anneau, c'est-à-dire (1.41) est valable pour tous les $A \in \mathcal{A}$. Notre théorème est ainsi démontré.

Deux cas essentiellement différents sont évidemment possibles : $\mu(\Omega)$ est ou bien fini, ou bien $\mu(\Omega) = +\infty$. Dans le premier cas, on peut supposer sans restreindre la généralité, que $\mu(\Omega) = 1$. Dans ce cas, notre système $[\Omega, \mathcal{A}, \mathcal{B}, P(A|B)]$ est essentiellement équivalent avec l'espace des probabilités de Kolmogoroff $[\Omega, \mathcal{A}, P]$, où $P(A) = \mu(A)$ pour tous les $A \in \mathcal{A}$. D'ailleurs, si $[\Omega, \mathcal{A}, P]$ [où $\mathcal{A}$ est une σ -algèbre des sous-ensembles de l'ensemble Ω , et P est une mesure sur $\mathcal{A}$ telle que $P(\Omega) = 1$] est un espace de probabilité de Kolmogoroff, et si $\mathcal{B}$ désigne l'ensemble de tous les ensembles $B \in \mathcal{A}$ tels que $P(B) > 0$, en posant

$$P(A|B) = \frac{P(AB)}{P(B)},$$

on obtient un espace simple des probabilités conditionnelles.

Dans l'autre cas, si $\mu(\Omega) = +\infty$, nous obtenons un espace des probabilités conditionnelles qui ne peut être déduit d'un espace des probabilités de Kolmogoroff.

Étant donné un espace simple des probabilités conditionnelles $[\Omega, \mathcal{A}, \mathcal{B}, P(A | B)]$, où $P(A | B)$ peut être exprimé à l'aide de la mesure μ σ -finie sous la forme (I.3), on peut facilement étendre la définition de $P(A | B)$ sur tous les ensembles $B \in \mathcal{B}$ pour lesquels (I.3) a un sens, c'est-à-dire pour tous les $B \in \mathcal{A}$ pour lesquels $0 < \mu(B) < +\infty$. En effet, il est clair que tous les axiomes restent valables, l'ensemble $\mathcal{B}^*$ de tous les ensembles $B \in \mathcal{A}$, avec $0 < \mu(B) < +\infty$, étant un bouquet et l'axiome P 3 ayant lieu parce que, en vertu de $BC = B$ (si $B \subset C$), on a

$$\frac{\mu(AB)}{\mu(B)} = \frac{\frac{\mu(ABC)}{\mu(C)}}{\frac{\mu(BC)}{(\mu C)}}.$$

Nous appellerons l'espace des probabilités conditionnelles que nous obtenons ainsi, un espace simple et *complet* des probabilités conditionnelles. En d'autres mots, un espace simple des probabilités conditionnelles $[\Omega, \mathcal{A}, \mathcal{B}, P(A | B)]$, avec

$$P(A | B) = \frac{\mu(AB)}{\mu(B)}$$

est dit complet si $\mathcal{B}$ contient tous les ensembles $B \in \mathcal{A}$ pour lesquels $\mu(B)$ est positive et finie.

Il est évident d'ailleurs que si Ω est un ensemble non vide arbitraire, $\mathcal{A}$ une σ -algèbre des sous-ensembles de $\mathcal{A}$, μ une mesure σ -finie sur $\mathcal{A}$, et si $\mathcal{B}$ désigne l'ensemble de tous les ensembles $B \in \mathcal{A}$ pour lesquels $\mu(B)$ est positive et finie, alors $\mathcal{B}$ est un bouquet d'ensembles, et si $P(A | B)$ est définie par (I.3), alors $P(A | B)$ satisfait aux axiomes P 1, P 2 et P 3, c'est-à-dire $[\Omega, \mathcal{A}, \mathcal{B}, P(A | B)]$ est un espace simple et complet des probabilités conditionnelles.

Il se présente la question intéressante suivante : *Si $\mathcal{B}$ est un bouquet d'ensembles appartenant à la σ -algèbre $\mathcal{A}$, sous quelles conditions supplémentaires existe-t-il une mesure σ -finie μ sur $\mathcal{A}$ telle que $\mathcal{B}$ soit identique avec le système de tous les ensembles B pour lesquels $\mu(B)$ est positive et finie ?* En d'autres mots, comment peut-on caractériser par des conditions nécessaires et suffisantes les systèmes d'ensembles $\mathcal{B}$ pour lesquels il existe une mesure σ -finie μ telle que $\mu(B)$ soit positive et finie si et seulement si B appartient à $\mathcal{B}$?

Nous ne connaissons pas la réponse à cette question. Il est facile de donner des conditions supplémentaires nécessaires autres que B 1, B 2 et B 3 (qui sont évidemment nécessaires), notamment les conditions suivantes :

B 4. Si $A_n \in \mathcal{A}$ ($n = 1, 2, \dots$) et $\sum_{n=1}^{\infty} A_n \in \mathcal{B}$, alors au moins un des ensembles A_n appartient à $\mathcal{B}$.

B 5. Si $B_1 \subset B_2 \subset B_3$, où $B_1 \in \mathcal{B}$ et $B_3 \in \mathcal{B}$, alors $B_2 \in \mathcal{B}$.

On peut distinguer deux types d'ensembles n'appartenant pas à $\mathcal{B}$. Nous disons que l'ensemble $A \in \mathcal{A}$ n'appartenant à $\mathcal{B}$ est de la première espèce s'il existe un $B \in \mathcal{B}$ tel que $B \subset A$, et qu'il est de la seconde espèce s'il n'existe pas un tel ensemble [Il est clair que les ensembles A de la première espèce sont les ensembles pour lesquels $\mu(A) = +\infty$, et que sont de la seconde espèce ceux pour lesquels $\mu(A) = 0$].

Ceci posé, nous pouvons donner encore quelques conditions nécessaires : Soit $\mathcal{D}$ l'ensemble de tous les ensembles $A \in \mathcal{A}$, $A \notin \mathcal{B}$ de la première espèce, et l'ensemble de tous les ensembles $A \in \mathcal{A}$, $A \notin \mathcal{B}$ de la seconde espèce.

B 6. Si $A \in \mathcal{D}$, il existe deux ensembles disjoints $A_1 \in \mathcal{D}$ et $A_2 \in \mathcal{D}$ tels que $A = A_1 + A_2$.

B 7. Si $A_n \in \mathcal{D}$ ($n = 1, 2, \dots$), il existe des ensembles $B_n \in \mathcal{B}$ tels que

$$B_n \subset A_n \quad \text{et} \quad \sum_{n=1}^{\infty} B_n \in \mathcal{D}.$$

B 8. $\mathcal{N}$ est un σ -idéal dans $\mathcal{A}$, c'est-à-dire si

$$A_n \in \mathcal{N} \quad (n = 1, 2, \dots), \quad \text{alors} \quad \sum_{n=1}^{\infty} A_n \in \mathcal{N}$$

et si

$$A \in \mathcal{N} \quad \text{et} \quad C \in \mathcal{A}, \quad \text{alors} \quad AC \in \mathcal{N}.$$

La question de caractériser les systèmes des sous-ensembles d'un ensemble Ω sur lesquels une mesure σ -finie prend des valeurs positives et finies, est ouverte aussi dans le cas spécial où Ω est un ensemble dénombrablement infini. Dans ce cas, la question peut se réduire à la question suivante : caractériser les classes $\mathcal{C}$ des suites $\{n_i\}$ des nombres naturels tels qu'il existe une série divergente à termes positifs $\sum p_n$ telle que $\sum p_{n_i}$ soit convergente si et seulement si $\{n_i\}$ appartient à $\mathcal{C}$. Cette question fut posée — comme M. P. Erdős a bien voulu m'en informer — par MM. Kakutani

et Smithies, et fut discutée par MM. Erdős et de Bruijn en 1953 en détail; ils ont trouvé quelques résultats partiels intéressants, qui ne sont pas encore publiés. Mais un système de conditions nécessaires et suffisantes manque jusqu'à aujourd'hui (Il est aisé de voir que les huit conditions mentionnées plus haut ne sont pas suffisantes).

2. Quelques exemples. — Nous donnons maintenant quelques exemples d'espaces simples des probabilités conditionnelles.

Exemple 1. — Soit $\Omega = \{1, 2, \dots\}$ l'ensemble de tous les entiers positifs, p_n ($n = 1, 2, \dots$) une suite de nombres non négatifs tels que la série $\sum_{n=1}^{\infty} p_n$ soit divergente. Soit $\mathcal{A}$ l'ensemble de tous les sous-ensembles de Ω , et $\mathcal{B}$ l'ensemble des sous-ensembles B de Ω pour lesquels $\sum_{n \in B} p_n = \mu(B)$ est positive et finie, et posons

$$P(A | B) = \frac{\mu(AB)}{\mu(B)}$$

pour chaque $A \in \mathcal{A}$ et $B \in \mathcal{B}$. Alors $[\Omega, \mathcal{A}, \mathcal{B}, P(A | B)]$ est un espace simple et complet des probabilités conditionnelles.

Spécialement si $p_n = 1$ pour $n = 1, 2, \dots$, on a

$$P(A | B) = \frac{N(AB)}{N(B)},$$

où $N(C)$ désigne le nombre des éléments de l'ensemble C . Ce cas spécial peut servir pour donner un sens précis à l'expression « choisir un entier positif au hasard d'une telle façon que tous les nombres entiers aient la même chance d'être choisis ».

Le sens exact de cet énoncé paradoxal est naturellement le suivant : sous la condition que l'entier positif choisi au hasard appartienne à l'ensemble fini et non vide arbitraire B , tous les éléments de B ont la même probabilité conditionnelle d'être choisis.

Exemple 2. — Soit l'ensemble de tous les nombres réels x soit $\mathcal{A}$ l'ensemble des sous-ensembles de Borel de Ω , et soit μ une mesure σ -finie sur $\mathcal{A}$. Soit enfin $\mathcal{B}$ l'ensemble de tous les sous-ensembles $B \in \mathcal{A}$ pour lesquels $\mu(B)$ est finie et positive et $P(A | B)$ soit défini par (1.3). Alors $[\Omega, \mathcal{A}, \mathcal{B}, P(A | B)]$ est un espace simple et complet des probabilités conditionnelles. On peut, par exemple, choisir une mesure μ -donnée par la formule

$$\mu(A) = \int_A f(x) dx,$$

où $f(x)$ est une fonction non négative et mesurable telle que $\int_I f(x)dx$ est fini pour chaque intervalle fini I , mais

$$\int_{-\infty}^{+\infty} f(x)dx = +\infty.$$

En particulier, si $f(x) = 1$, $\mu(A)$ est identique avec la mesure de Lebesgue de A . Ce cas particulier peut servir pour donner un sens précis à l'expression « choisir un nombre réel avec une répartition uniforme sur tout l'axe réel ». Le sens exact de cet énoncé paradoxal est le suivant : sous la condition qu'un nombre choisi au hasard appartienne à un intervalle fini mais arbitraire I , il est réparti uniformément sur cet intervalle.

3. Produit des espaces simples et complets des probabilités conditionnelles, indépendance conditionnelle des événements. — Soit

$$\mathcal{E}_1 = [\Omega_1, \mathcal{A}_1, \mathcal{B}_1, P_1(A | B)] \quad \text{et} \quad \mathcal{E}_2 = [\Omega_2, \mathcal{A}_2, \mathcal{B}_2, P_2(A | B)]$$

des espaces simples et complets des probabilités conditionnelles. Le produit $\mathcal{E}_1 * \mathcal{E}_2$ de ces espaces est aussi un espace simple et complet des probabilités conditionnelles $[\Omega_3, \mathcal{A}_3, \mathcal{B}_3, P_3(A | B)]$ qui est définie comme suit. Soient μ_1 et μ_2 des mesures σ -finies sur $\mathcal{A}_1$ et $\mathcal{A}_2$ telles que

$$P_1(A | B) = \frac{\mu_1(AB)}{\mu_1(B)} \quad \text{et} \quad P_2(A | B) = \frac{\mu_2(AB)}{\mu_2(B)}.$$

Soit Ω_3 l'ensemble de tous les couples d'éléments (ω_1, ω_2) où $\omega_1 \in \Omega_1$ et $\omega_2 \in \Omega_2$. Soit $\mathcal{A}_3$ la plus petite σ -algèbre des sous-ensembles de Ω_3 qui contienne tous les ensembles $A_3 = A_1 * A_2$ tels que $A_1 \in \mathcal{A}_1$ et $A_2 \in \mathcal{A}_2$, c'est-à-dire des ensembles A_3 de couples (ω_1, ω_2) , où

$$\omega_1 \in A_1, \quad \omega_2 \in A_2 \quad \text{et} \quad A_1 \in \mathcal{A}_1, \quad A_2 \in \mathcal{A}_2.$$

Soit μ_3 le produit des mesures μ_1 et μ_2 défini en posant

$$\mu_3(A_1 * A_2) = \mu_1(A_1) \mu_2(A_2) \quad \text{pour} \quad A_1 \in \mathcal{A}_1, \quad A_2 \in \mathcal{A}_2$$

et en étendant la définition de μ_3 sur $\mathcal{A}_3$ d'une façon habituelle (voir [21]).

Soit $\mathcal{B}_3$ l'ensemble de tous les sous-ensembles B de Ω_3 appartenant à $\mathcal{A}_3$ tels que $\mu_3(B)$ possède une valeur finie et positive. Posons enfin

$$P_3(A | B) = \frac{\mu_3(AB)}{\mu_3(B)} \quad \text{pour} \quad A \in \mathcal{A}_3 \quad \text{et} \quad B \in \mathcal{B}_3.$$

Alors $[\Omega_3, \mathcal{A}_3, \mathcal{B}_3, P_3(A | B)] = \mathcal{E}_3$ est manifestement un espace simple et complet des probabilités conditionnelles. Il est clair que $\mathcal{E}_3$ ne dépend pas du choix de μ_1 et μ_2 .

Ajoutons quelques mots sur la notion d'indépendance. Nous appellerons deux événements A' et A'' d'un espace des probabilités conditionnelles $[\Omega, \mathcal{A}, \mathcal{B}, P(A | B)]$ *indépendants par rapport à une condition* $B \in \mathcal{B}$, si

$$(3.1) \quad P(A'A'' | B) = P(A' | B) = P(A'' | B).$$

Il est évident que deux événements peuvent être indépendants simultanément par rapport à plusieurs conditions. Leur indépendance est d'autant plus forte, que l'ensemble des conditions par rapport auxquelles l'indépendance ait lieu est plus étendu. Dans ce sens la notion d'indépendance dans un espace des probabilités conditionnelles est plus riche que dans le cas d'un espace des probabilités ordinaires. Pour en donner un exemple, revenons au produit $\mathcal{E}_3 = \mathcal{E}_1 * \mathcal{E}_2$ des espaces $\mathcal{E}_1$ et $\mathcal{E}_2$. Soit

$$A' = A_1 * \Omega_2 \quad \text{et} \quad A'' = \Omega_1 * A_2,$$

où $A_1 \in \mathcal{A}_1$ et $A_2 \in \mathcal{A}_2$. Alors A' et A'' sont indépendants par rapport à chaque condition B de la forme

$$B = B_1 * B_2, \quad \text{avec} \quad B_1 \in \mathcal{B}_1 \quad \text{et} \quad B_2 \in \mathcal{B}_2.$$

4. Les variables aléatoires et leurs répartitions. — Soit $[\Omega, \mathcal{A}, \mathcal{B}, P(A | B)]$ un espace simple et complet des probabilités conditionnelles. Soit $X(\omega)$ une fonction définie pour tout $\omega \in \Omega$ et mesurable par rapport à $\mathcal{A}$, c'est-à-dire telle que l'image inverse de tout intervalle I de l'axe réel $X^{-1}(I)$ [où $X^{-1}(I)$ désigne ici l'ensemble des $\omega \in \Omega$ tels que $X(\omega) \in I$] appartienne à $\mathcal{A}$. Soit m la mesure sur l'axe réel $\mathcal{R}$ définie en posant pour chaque intervalle I de $\mathcal{R}$

$$(4.1) \quad m(I) = \mu(X^{-1}(I)).$$

Nous appellerons la mesure m la *répartition de la variable aléatoire* X (La répartition m est définie évidemment à un facteur positif près). S'il existe un intervalle ouvert I^* (fini ou infini) de l'axe réel tel que pour chaque sous-intervalle I de I^* fermé à gauche et ouvert à droite, $m(I)$ a une valeur finie et s'il existe un sous-intervalle I_0 de I^* tel que $m(I_0) > 0$, nous disons que la répartition de X est finie dans I^* . Dans ce cas, nous pouvons définir la fonction de répartition de X dans I^* comme suit : Soit $I^* = (a^*, b^*)$; choisissons un point arbitraire dans $I^*(a^* < X_0 < b^*)$ et posons

$$F(X) = m(I_{X_0, X}) \quad \text{pour} \quad X_0 < X < b^*$$

et

$$F(X) = -m(I_{x, x_0}) \quad \text{pour } a^* < X \leq X_0,$$

où $I_{a,b}$ est l'intervalle $a \leq X$ (fermé à gauche et ouvert à droite). $F(X)$ est évidemment une fonction non décroissante et continue à droite, avec $F(X_0) = 0$.

Si $a^* < a_0 < a < b < b_0 < b^*$ et $I_0 = [a, b]$ est tel que $m(I_0) > 0$, et si nous posons $I = [a, b]$, nous avons

$$(4.2) \quad P(X \in I \mid X \in I_0) = \frac{F(b) - F(a)}{F(b_0) - F(a_0)}.$$

Il est clair qu'une variable aléatoire possède plusieurs fonctions de répartition dans le même intervalle, mais si $F(x)$ et $G(x)$ sont deux fonctions de répartition de la variable aléatoire X dans le même intervalle, alors il existe des constantes $c > 0$ et d telles que

$$G(x) = c F(x) + d.$$

Si une fonction de répartition $F(x)$ de la variable aléatoire X dans un intervalle I^* est absolument continue et $F'(x) = f(x)$, nous appellerons $f(x)$ la fonction de densité de probabilité de X dans I^* . Dans ce cas, on a, au lieu de (4.2) sous les mêmes conditions,

$$(4.3) \quad P(X \in I \mid X \in I_0) = \frac{\int_a^b f(x) dx}{\int_{a_0}^{b_0} f(x) dx},$$

$f(x)$ est définie évidemment à un facteur positif constant près.

Par exemple, si $\mathcal{E}$ est l'espace des probabilités conditionnelles de l'exemple 2 du paragraphe 2, où μ est la mesure de Lebesgue et si $X(\omega) = e^\omega$ pour $-\infty < \omega < +\infty$, alors la densité de probabilité de X dans l'intervalle $(0 < x < +\infty)$ est égale à $\frac{1}{x}$. Notons que, dans ce cas, les variables aléatoires X^α , où α est un nombre réel différent de 0, mais d'ailleurs arbitraire, ont toutes la même densité de probabilité.

Voyons un autre exemple. Soit X une variable aléatoire définie sur le même espace des probabilités conditionnelles comme dans le dernier exemple, par $X(\omega) = \frac{1}{\omega}$. Alors $F(x) = -\frac{1}{x}$ est une fonction de répartition et $f(x) = \frac{1}{x^2}$ une fonction de densité de probabilité de X dans l'intervalle $(0, +\infty)$ et aussi dans l'intervalle $(-\infty, 0)$.

Il est clair que si $X_1, X_2, \dots, X_n$ sont des variables aléatoires définies sur un espace des probabilités conditionnelles $\mathcal{E}$ et $g(X_1, X_2, \dots, X_n)$ est une fonction mesurable Borel à n variables, alors $Y = g(X_1, X_2, \dots, X_n)$ est aussi une variable aléatoire sur $\mathcal{E}$. Voyons un exemple de la composition des répartitions.

Soit $\mathcal{E}_1 = [\Omega_1, \mathcal{A}_1, \mathcal{B}_1, P_1(A | B)]$ l'espace des probabilités conditionnelles définies comme suit : soit Ω l'intervalle $0 < \omega_1 < +\infty$, $\mathcal{A}_1$ l'ensemble de tous les sous-ensembles mesurables de Ω , $\mathcal{B}_1$ l'ensemble de tous les ensembles mesurables de Ω_1 dont chacun a une mesure de Lebesgue positive et finie. Soit

$$P(A | B) = \frac{\mu_1(AB)}{\mu_1(B)},$$

où μ_1 est la mesure de Lebesgue. Soit

$$\mathcal{E}_2 = \mathcal{E}_1 \quad \text{et} \quad \mathcal{E}_3 = \mathcal{E}_1 * \mathcal{E}_2$$

au sens du paragraphe 2 et supposons que les variables aléatoires X_1 et X_2 soient définies sur $\mathcal{E}_3$ par les relations

$$X_1(\omega_1, \omega_2) = \omega_1 \quad \text{et} \quad X_2(\omega_1, \omega_2) = \omega_2.$$

Alors la répartition de X_1 et celle de X_2 est telle que chaque intervalle du demi-axe positif a une mesure infinie; mais la répartition de $X_1 + X_2$ en est tout à fait différente : sa densité de probabilité est $f(x) = x$ pour $0 < x < +\infty$.

Remarquons que

$$(4.4) \quad f(x) = \int_0^\infty f_1(u) f_1(x-u) du,$$

où $f_1(x)$ est la densité de probabilité de la variable aléatoire X_1 définie sur $\mathcal{E}_1$ par $X_1(\omega_1) = \omega_1$, c'est-à-dire

$$f_1(x) = \begin{cases} 1 & \text{pour } 0 < x < +\infty, \\ 0 & \text{pour } x < 0. \end{cases}$$

Donc la répartition de $X_1 + X_2$ avec la densité x pour $x > 0$ est le produit de composition de la répartition uniforme sur le demi-axe positif avec lui-même.

Notons enfin que, quand il s'agit de composition de répartitions avec des mesures non bornées, on ne peut pas appliquer la méthode usuelle des fonctions caractéristiques, parce qu'elle n'existe pas au sens ordinaire. Mais il existe comme des distributions au sens de L. Schwartz [23], et ainsi cette méthode peut néanmoins être appliquée dans un sens généralisé (voir [6]).

BIBLIOGRAPHIE

- [1] A. N. KOLMOGOROFF, *Grundbegriffe der Wahrscheinlichkeitsrechnung*, Springer, Berlin, 1933.
- [2] A. RÉNYI, *On a new axiomatic theory of probability* (*Acta Math. Acad. Sc. Hungar.*, t. 6, 1955, p. 285-335).
- [3] A. RÉNYI, *Axiomatischer Aufbau der Wahrscheinlichkeitsrechnung. Bericht über die Tagung Wahrscheinlichkeitsrechnung und Mathematische Statistik*, V. E. B. Deutscher Verlag der Wissenschaften, Berlin, 1954, p. 7-15.
- [4] A. RÉNYI, *On conditional probability spaces generated by a dimensionnally ordered set of measures* (*Teor. Veroiatn. prim.*, t. 1, 1956, p. 61-71).
- [5] A. RÉNYI, *A new deduction of Maxwell's law of velocity distribution* (*Isw. Mat. Inst. Sofia*, t. 2, 1957, p. 45-53).
- [6] A. RÉNYI, *Wahrscheinlichkeitsrechnung, mit einem Anhang über Informationstheorie*, V. E. B. Deutscher Verlag der Wissenschaften, Berlin, 1962, p. 1-547.
- [7] M. FRÉCHET, *Généralités sur les probabilités (Traité du calcul des probabilités et ses applications*, par É. BOREL, t. I, 2^e éd., Gauthier-Villars, Paris, 1950).
- [8] H. REICHENBACH, *Wahrscheinlichkeitslehre*, Sijthoff, Leiden, 1935.
- [9] K. POPPER, *Philosophy of science : A personal report*, *British Philosophy in the Mid-Century*, ed. by C. A. Mace, 1956, p. 191.
- [10] M. I. KEYNES, *A treatise on probability theory*, MacMillan, London, 1952, p. 1-460.
- [11] B. O. KOOPMAN, *The axioms and algebra of intuitive probability* (*Ann. Math.*, t. 41, 1940, p. 269-292).
- [12] A. H. COPELAND, *Postulates for the theory of probability* (*Amer. J. Math.*, t. 63, 1941, p. 741-762).
- [13] G. A. BARNARD, *Statistical inference* (*J. Roy. Stat. Soc.*, série B, t. 11, 1949, p. 115-139).
- [14] F. I. GOOD, *Probability and weighing of evidence*, London, 1950.
- [15] R. D. LUCE, *Individual choice behaviour. A theoretical analysis*, Wiley, New York 1959.
- [16] H. JEFFREYS, *Theory of probability*, 2^e éd., Clarendon Press, Oxford, 1948.
- [17] M. DUMAS, *Sur les lois de probabilités divergentes et la formule de Fisher* (*Interméd. Rech. Math.*, t. 9, 1947, Suppl., p. 127-130).
- [18] M. DUMAS, *Interprétation de résultats de tirages exhaustifs* (*C. R. Acad. Sc.*, t. 288, 1949, p. 904-906).
- [19] E. BATICLE, *Sur une loi de probabilité a priori des paramètres d'une loi laplacienne* (*C. R. Acad. Sc.*, t. 226, 1948, p. 55-57).
- [20] E. BATICLE, *Sur une loi de probabilité a priori pour l'interprétation des résultats de tirages dans une urne* (*C. R. Acad. Sc.*, t. 228, 1949, p. 902-904).
- [21] P. R. HALMOS, *Measure theory*, Van Nostrand. New York, 1949.
- [22] A. CSASZAR, *Sur la structure des espaces de probabilités conditionnelles* (*Acta Math. Acad. Sc. Hungar.*, t. 6, 1955, p. 337-361).
- [23] L. SCHWARTZ, *Théorie des distributions*, t. I-II, Paris, 1950-1951.

110, 120, 179, 242, 242

NOTE

The axiomatic definition of the conditional probability spaces is one of the most famous works of A. Rényi. Nevertheless, there are few papers applying or developing it.

There are two fundamental problems in connection with the conditional probability spaces. One of them is the existence of distribution function, the other is the existence of marginal distributions. The first problem is closely connected with the quotient representation of the conditional probability. Császár [1] found the sufficient and necessary conditions for the quotient representation by one measure or by a dimensionally ordered set of measures. These conditions concerned only the conditional probability. Later Rényi No. 120 and No. 179 (for the latter see also [7]) has perceived that some natural structural restrictions on the set of conditions imply these representations. Rényi's result is extended to Boole algebras by Krauss [4].

The other problem is mostly unsolved. The projection of conditional probability distribution is defined by Pergel [5] only in the cases, when the conditions are Cartesian products. Using this definition he proved the generalized version of the fundamental theorem of Kolmogorov.

A continual aim of Rényi was to develop the probability theory on conditional probability spaces. A list of topics to be worked out is as follows:

- convergence of conditional probability on measures: [7], Sec. 2.5;
- general notion of conditional probability: [6], Sec. 5.3;
- laws of large numbers: this work § 4; [6], Sec. 7.15;
- characteristic function: [6], Sec. 6.9;
- central limit theorems: No. 96, § 3;
- information theory: [6], Sec. 9.10.

The problem of definition of the convergence to the uniform distribution has already arisen in the probability spaces of Kolmogorov-type, too. This theory offers a new type of convergence, the so-called Rényi's type or relative convergence. The theorem on the limiting uniform distribution of sums (Sec. 3.4) is proved under weaker conditions in [6] p. 361. The concept of conditional ergodicity of Markov chains (introduced by Rényi in Sec. 3.7) is based upon this notion of convergence, too. Dyson and Chung [2] have showed that not every Markov chain is ergodic. This notion of convergence is applied in some number theoretical works of Rényi as well.

Ingarden and Urbanik [3] defined the entropy without probability, here the probability appears as a secondary concept, but this entropy can be realized in fact only on a conditional probability space (see also No. 242). (P. B.)

REFERENCES

- [1] Császár, Á.: Sur la structure des espaces de probabilité conditionnelle. *Acta Math. Acad. Sci. Hung.*, **6** (1955), 337–361.
- [2] Dyson, F. J. and Chung, K. L.: *Math. Reviews*, **18** (1957), 339–340.
- [3] Ingarden, R. S. and Urbanik, K.: Information without probability. *Coll. Math.*, **9** (1962), 131–162.
- [4] Krauss, P. H.: Representation of conditional probability measures on Boole algebras. *Acta Math. Acad. Sci. Hung.*, **19** (1968), 229–241.
- [5] Pergel, J.: An extension of Kolmogorov's fundamental theorem to conditional probability spaces. *MTA Mat. Kut. Int. Közl.*, **6** (1961), 61–65.
- [6] Rényi, A.: *Probability theory*. Akadémiai Kiadó, Budapest, 1970.
- [7] Rényi, A.: *Foundations of probability*. Holden-Day, San Francisco, 1970.

ON THE FOUNDATIONS OF INFORMATION THEORY¹

by

A. Rényi

Mathematical Institute of the Hungarian Academy of Sciences, Budapest

1. INTRODUCTION

In the present paper we shall give a review of certain investigations on the foundations of information theory. We shall deal exclusively with one question, which is however fundamental in information theory: *how should the amount of information be measured?* By other words we shall give a review of results concerning the *definition of information*.

This question can be approached from two essential different points of view. The first is the *axiomatic* (or postulational) *approach*; starting from the intuitive notion of information one formulates certain properties which a reasonable measure of information has to satisfy; after this the purely mathematical question has to be solved to find all the expressions which possess the postulated properties. The first to adopt this point of view was *C. Shannon* who in his fundamental paper [1] deduced from certain postulates his formula

$$(1.1) \quad H(P) = - \sum_{k=1}^a p_k \log_2 \frac{1}{p_k}$$

for the entropy² of a probability distribution $P = (p_1, p_2, \dots, p_a)$ i.e. the amount of information contained in a single observation of a random variable ξ which takes on a different values $x_1, x_2, \dots, x_a$ with the probabilities $p_k = P(\xi = x_k)$ ($k = 1, 2, \dots, a$).

The second point of view may be characterized as the *pragmatic approach*; this approach starts from certain particular problems of information theory and accepts as measures of the amount of information the quantities which present themselves in the solution. According to this point of view the real justification of some measure of information is that it does work. This second point of view has been recently emphasized by *J. Wolfowitz* in his book [2], who however points out that the view that the main reason for introducing the quantity (1) is its role in coding theory, was expressed already by *Shannon*.

These two points of view are according to the opinion of the author of this paper not as opposed to each other as they seem to be; they are compatible and even complement each other and therefore both deserve attention. Both of the mentioned approaches may and should be used as a control to the other. As a matter of fact, if certain quantities are deduced from some natural postulates (from "first principles") these certainly need for their final justification the control whether they can be effectively used in solving concrete problems. On the other hand if one encounters a

¹ A review paper prepared for the 34th Session of the International Statistical Institute, Ottawa, Canada, August 1963.

² The quantity $H(P)$ defined by (1) is interpreted either as a measure of entropy (i.e. of uncertainty) or as a measure of information. Both interpretations are justified. As a matter of fact the difference between these two interpretations consists only in that whether we imagine ourselves in a moment *before* carrying out an experiment whose a possible results have the probabilities $p_1, p_2, \dots, p_a$ (in which case $H(P)$ measures our uncertainty concerning the result of the experiment) or we imagine ourselves in a moment *after* the experiment has been carried out (in which case $H(P)$ measures the amount of information we got from the experiment).

certain quantity in course of the solution of a particular problem, this in itself does not prove that the quantity in question is of general importance; only the fact that one encounters the same quantity in solving a large number of rather different problems (as is the case e.g. with *Shannon's* measure of information) convinces us that it is a fundamental notion. In this case however it is quite natural to try to find out the reason why the same quantity occurs in different contexts, i.e. to find which are its properties which make it so useful; and exactly this is the aim of the axiomatic approach.

In §§ 2-5 we shall deal with the pragmatic approach and in §§ 6-9 with the axiomatic approach, while in § 10 we add some further remarks.

2. A PRAGMATIC APPROACH

The entropy $H(P)$ of a finite discrete probability distribution $P = (p_1, p_2, \dots, p_a)$ presents itself in the solution of the following simple coding problem. Let us consider a sequence of independent identically distributed random variables $\xi_1, \xi_2, \dots, \xi_n$ each of which takes on the different values $x_1, x_2, \dots, x_a$ with the corresponding probabilities $p_1, p_2, \dots, p_a$ i.e.

$$(2.1) \quad P(\xi_j = x_k) = p_k \quad (1 \leq k \leq a; 1 \leq j \leq n)$$

where $p_k \geq 0$ ($1 \leq k \leq a$) and $\sum_{k=1}^a p_k = 1$. The sequence $\xi_1, \xi_2, \dots, \xi_n$ may be interpreted as produced by an information source emitting stationary and independent signals. Let Ω_n be the set of all ordered sequences of length n of the symbols $x_1, x_2, \dots, x_a$. Let be given a fixed number ϵ ($0 < \epsilon < 1$) and let us consider those subsets E of Ω_n for which $P_n(E) \geq 1 - \epsilon$ where $P_n(E)$ is the probability that the observed sequence $\xi_1, \xi_2, \dots, \xi_n$ belongs to the set E . Let $b(n, \epsilon)$ denote the minimum of the number of elements of such sets E ; by other words if $N(E)$ denotes the number of elements of a set E , we put

$$(2.2) \quad b(n, \epsilon) = \min_{P_n(E) \geq 1 - \epsilon} N(E).$$

Now it is easy to show that the limit

$$(2.3) \quad \lim_{n \rightarrow +\infty} \frac{\log_2 b(n, \epsilon)}{n} = H(P)$$

exists, it is independent of ϵ , and it depends only on the distribution P , namely one has

$$(2.4) \quad H(P) = - \sum_{k=1}^a p_k \log_2 \frac{1}{p_k}.$$

Still more is known; it has been shown recently by *W. Strassen* [3] (improving a previous result by *Jushkewich* [4]) that - if the numbers p_k are not all equal³ one has

$$(2.5) \quad \log_2 b(n, \epsilon) = nH(P) + \sqrt{n} \cdot \lambda D - \frac{\log n}{2 \log 2} + O(1)$$

where

$$D = \left[\sum_{k=1}^a \left(\log_2 \frac{1}{p_k} - H(P) \right)^2 p_k \right]^{\frac{1}{2}}$$

³ If $p_1 = p_2 = \dots = p_a = \frac{1}{a}$ then clearly $b(n, \epsilon)$ is equal to the least integer $\geq a^n(1 - \epsilon)$ and thus, as in this case $H(P) = \log_2 a$, we have $\log_2 b(n, \epsilon) = nH(P) + O(1)$.

and λ is defined by $\Phi(\lambda) = 1 - \varepsilon$, where $\Phi(x)$ denotes the standard normal distribution function $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-u^2/2} du$; in (2.3) $O(1)$ denotes a remainder term⁴ which remains bounded for $n \rightarrow +\infty$.

Thus we may consider (1.3) as a definition of the entropy $H(P)$. The result can be interpreted as follows: if we want to express (code) the sequence of signals $\xi_1, \xi_2, \dots, \xi_n$ by a sequence of 0-s and 1-s so that the correspondence should be one to one, except for certain rather improbable sequences which we are ready to neglect if the total probability of occurrence of these neglected sequences does not exceed ε , then this can be accomplished by using sequences of 0-s and 1-s of length $n H(P) + O(\sqrt{n})$.

Thus if we accept as the unity of the amount of information the maximal amount of information which a signal capable of only two values (e.g. 0 and 1) can carry, then $H(P)$ can be interpreted as the amount of information per signal produced by a stationary source of independent signals, if the probability distribution of the possible values of the signals is $P = (p_1, p_2, \dots, p_a)$.

As it is easy to see

$$(2.6) \quad H(P) \leq \log_2 a$$

with equality standing in (2.6) if and only if $p_1 = p_2 = \dots = p_a = \frac{1}{a}$.

An important point in favour of accepting (2.3) as the definition of the entropy $H(P)$ is that the amount of information per signal furnished by a more general source (e.g. a stationary Markovian source, see Jushkevich [4]) further the definition of the capacity of a channel can be defined in a quite analogous way; as regards the latter question we refer to the coding theorem and its strong converse (see [2], [3]). Here and in what follows we restrict ourselves to discuss the entropy of a stationary source of independent signals.

3. ANOTHER PRAGMATIC APPROACH

While the simple coding problem discussed in § 1, the solution of which leads us to Shannon's entropy $H(P)$, is certainly of fundamental importance, nevertheless there are other problems which are equally of fundamental character and which may also be used as an alternative for introducing in a pragmatic manner the entropy $H(P)$. In this § we shall discuss another problem of this kind, which may be called the *problem of random search* (see [5], [6], [7], [8]).

Let us consider the following situation: we want to find an unknown element x of a set S_n having n elements. The information available is of the following nature: we can carry out independent experiments, each experiment consisting in dividing at random the set S_n into a classes $C_1, C_2, \dots, C_a$ so that for any element of S_n the probability that it will belong to the class C_k is equal to p_k ($k = 1, 2, \dots, a$) independently from what happens to the other elements. By other words we suppose further that if the elements of S_n are $x_1, x_2, \dots, x_n$ and λ_j denotes the index of the class into which x_j belongs, then the random variables $\lambda_1, \lambda_2, \dots, \lambda_n$ are independent and $P(\lambda_j = k) = p_k$ ($1 \leq j \leq n; 1 \leq k \leq a$). The result of the experiment consists in that we are informed which one of the classes $C_1, C_2, \dots, C_a$ contains the unknown element x . Let be given a number ε ($0 < \varepsilon < 1$) and let $d(n, \varepsilon)$ denote the

⁴ Strassen has analyzed this term further, but we do not go into these details here.

least such value of m that the probability that the unknown element can be uniquely determined from m experiments of the above mentioned type, exceeds $1 - \varepsilon$. It is easy to see that $d(n, \varepsilon)$ is the least number m such that

$$(3.1) \quad \sum_{\substack{a \\ \sum_{i=1}^a m_i = m}} \frac{m!}{m_1! m_2! \dots m_a!} p_1^{m_1} p_2^{m_2} \dots p_a^{m_a} (1 - p_1^{m_1} p_2^{m_2} \dots p_a^{m_a})^{n-1} \geq 1 - \varepsilon.$$

It follows by an easy calculation that putting

$$(3.2) \quad D = \left[\sum_{k=1}^a p_k \left(\log_2 \frac{1}{p_k} - H(P) \right)^2 \right]^{1/2}$$

we have in case $D > 0$

$$(3.3) \quad d(n, \varepsilon) = \frac{\log_2 n}{H(P)} + \frac{D \lambda \sqrt{\log_2 n}}{H(P)^{1/4}} + O(\sqrt{\log_2 n})$$

where λ is determined by the equation $\Phi(\lambda) = 1 - \varepsilon$.

Thus we have

$$(3.4) \quad H(P) = \lim_{n \rightarrow +\infty} \frac{\log_2 n}{d(n, \varepsilon)}.$$

In case $D = 0$, i.e. if $p_1 = p_2 = \dots = p_a = \frac{1}{a}$ we have for $0 < \varepsilon < 1 - \frac{1}{e}$

$$(3.5) \quad d(n, \varepsilon) = \left\lceil \frac{\log_2 n + \log_2 \frac{1}{\log \frac{1}{1-\varepsilon}}}{H(P)} \right\rceil$$

where $\{x\}$ denotes the least integer $\geq x$ (and of course $H(P) = \log_2 a$).

The result obtained can be interpreted as follows: to determine an unknown element of a set S_n , having n elements, one needs $\log_2 n$ bits of information. If S_n is divided at random into a classes having approximately $p_1 n, p_2 n, \dots, p_a n$ elements, and we are informed which of these classes contains the unknown element which we try to find, then each such experiment gives us in the average $H(P)$ bits of information, and thus approximately $\frac{\log_2 n}{H(P)}$ such experiments have to be carried out in order to get a sufficient amount of information. (The reason why slightly more than $\frac{\log_2 n}{H(P)}$ experiments are needed if we want to determine the unknown x with a probability $\geq 1 - \varepsilon$, is that there is some overlapping between the partial informations obtained.)

The number $d(n, \varepsilon)$ can be interpreted also in the following alternative way: Let us consider again a stationary information source producing independent signals, with values $x_1, x_2, \dots, x_a$ having the corresponding probabilities $p_1, p_2, \dots, p_a$. Suppose that the source produces n sequences of signals, each sequence consisting of m signals; let us denote these sequences by

$$s_1 = \{\xi_{11}, \dots, \xi_{1m}\}, s_2 = \{\xi_{21}, \dots, \xi_{2m}\}, \dots, s_n = \{\xi_{n1}, \dots, \xi_{nm}\}.$$

Then $d(n, \varepsilon)$ is the least value of m such that the probability that the sequences $s_2, s_3, \dots, s_n$ are all different from the sequence s_1 , exceeds $1 - \varepsilon$.

4. AN OTHER MEASURE OF INFORMATION

We shall deal now with a modification of the problem considered in § 3 (see [7]) which leads to a measure of information, different from that of *Shannon*. The problem discussed in § 3 can be characterized as follows: we divide a finite set S_n into a classes at random several times, and we are interested in the number m of such subdivisions which is necessary in order that the m divisions together should separate a fixed (but unknown) element x of S_n from all other elements of S_n with a prescribed probability. (We shall say that a subdivision of S_n into $a \geq 2$ classes separates two elements x and y of S_n if x and y belong to different classes of the subdivision.) Now we modify the problem as follows: how many independent subdivisions of the same type are needed in order that these subdivisions should separate any two element of S_n from each other, with a prescribed probability.

We suppose again that the subdivisions in question are independent from each other and are such that each element of S_n will belong to the k -th class with probability p_k independently of what happens to the other elements (i.e. if $x_1, \dots, x_n$ are the elements of S_n and λ_j denotes the index of the class into which x_j belongs, then the random variables $\lambda_1, \dots, \lambda_n$ are independent and $P(\lambda_j = k) = p_k$ for $1 \leq j \leq n$, $1 \leq k \leq a$). Let P_{nm} denote the probability that m such subdivisions separate any two elements of S_n . P_{nm} can be expressed as follows. Let us consider all possible ordered products consisting of m factors, each of which is one of the numbers $p_1, p_2, \dots, p_a$, i.e. the products of the form $p_{i_1} p_{i_2} \dots p_{i_m}$. There are clearly a^m such products (two products containing the same factors but in a different order are considered as different). Let us label these products in any order by the numbers $1, 2, \dots, a^m$ and denote them by $w_1, w_2, \dots, w_{a^m}$. Then we have

$$(4.1) \quad P_{nm} = \sum' w_{j_1} w_{j_2} \dots w_{j_n}$$

where the summation is to be extended over all positive ordered n -tuples $j_1, j_2, \dots, j_n$ which consist of different numbers chosen among the numbers $1, 2, \dots, a^m$; thus the sum on the right contains $\binom{a^m}{n} n!$ terms. It can be proved that if $e_2(n, \epsilon)$ denotes the least integer m such that $P_{nm} \geq 1 - \epsilon$ then

$$(4.2) \quad e_2(n, \epsilon) = \left\lceil \frac{2 \log_2 n + \log_2 \frac{1}{\log \frac{1}{1-\epsilon}}}{I_2(P)} \right\rceil$$

where

$$(4.3) \quad I_2(P) = \log_2 \frac{1}{\left(\sum_{k=1}^a p_k^2 \right)}.$$

The quantity $I_2(P)$ which in formula (4.2) plays the same role as the entropy $H(P)$ in formula (3.3), can also be considered as a measure of the amount of information contained in the value of a discrete random variable ξ which has the distribution $P = (p_1, \dots, p_a)$.

The relation between $H(P)$ and $I_2(P)$ can be characterized as follows. Let $P = (p_1, \dots, p_a)$ be any finite probability distribution; let λ be a random variable which takes on the values $1, 2, \dots, a$ with the corresponding probabilities $p_1, p_2, \dots, p_a$ and let π be the random variable defined by $\pi = p_\lambda$; by other words π is always equal to the probability of that value of λ which λ takes on. Thus we have

$$(4.4) \quad P(\pi = p_k) = p_k \quad (k = 1, 2, \dots, a).$$

Now let us put

$$(4.5) \quad L(x) = \log_2 \frac{1}{x}$$

and let us denote by $E(\eta)$ the expectation of the random variable η . With these notations we have

$$(4.6a) \quad H(P) = E(L(\pi))$$

and

$$(4.6b) \quad I_2(P) = L(E(\pi)).$$

Thus $H(P)$ is obtained by transforming π by the function L and then calculating the expectation of this random variable, while $I_2(P)$ is obtained by carrying out the same operations in the reversed order.

$I_2(P)$ has certain properties in common with $H(P)$. For instance both are additive with respect to taking the direct product of probability distributions; more exactly if $P = (p_1, \dots, p_a)$ and $Q = (q_1, \dots, q_b)$ are two arbitrary probability distributions, and if we denote by $P \times Q$ the distribution consisting of the terms $P_i q_j$ ($1 \leq i \leq a$; $1 \leq j \leq b$) then

$$(4.7) \quad H(P \times Q) = H(P) + H(Q)$$

and similarly

$$(4.8) \quad I_2(P \times Q) = I_2(P) + I_2(Q)$$

It follows from Jensen's inequality and the convexity of the function $\log_2 \frac{1}{x}$ that the values of $H(P)$ and $I_2(P)$ are equal if and only if $p_1 = p_2 = \dots = p_a = \frac{1}{a}$; in every other case one has $I_2(P) < H(P)$.

5. A CLASS OF MEASURES OF INFORMATION

Both $H(P)$ and $I_2(P)$ considered in the previous §-s belong to the same class of measures of information, defined as follows (see [9] and [10]): Let α be any fixed positive number, $\alpha \neq 1$; we shall call the quantity

$$(5.1) \quad I_\alpha(P) = \frac{1}{1-\alpha} \log_2 \left(\sum_{k=1}^a p_k^\alpha \right)$$

the *measure of order α of the amount of information contained* in a value of a random variable having the finite discrete probability distribution $P = (p_1, \dots, p_a)$. For $\alpha = 1$ we define $I_1(P)$ as the limit of $I_\alpha(P)$ for α tending to 1; we have evidently

$$(5.2) \quad I_1(P) = \lim_{\alpha \rightarrow 1} I_\alpha(P) = H(P)$$

Clearly for $\alpha = 2$ we get the same quantity $I_2(P)$ which we encountered in (3.2).

The problem considered in the previous § can be generalized so that we encounter instead of $I_2(P)$ the measure $I_r(P)$ of (integral) order r of information. As a matter of fact, let us consider again m independent random subdivisions $\Delta_1, \dots, \Delta_m$ of the finite set S_n having n elements, so that each subdivision splits the set S_n into a classes, so that each element of S_n should be contained in the k -th class of any of the subdivisions with probability p_k ($k = 1, 2, \dots, a$) independently of what happens to the other elements. The m subdivisions together define a subdivision Δ of the set S_n which

may be called the product of the subdivisions Δ_j ($j = 1, \dots, m$) and denoted by $\Delta = \Delta_1 \cdot \Delta_2 \dots \Delta_m$. The subdivision Δ is defined as follows: two elements of S_n belong to the same class of Δ if and only if they belong to the same class with respect to each subdivision $\Delta_1, \Delta_2, \dots, \Delta_m$. Now let $e_r(n, \epsilon)$ ($r \geq 2, 0 < \epsilon < 1$) denote the least value of m such that with probability $\geq 1 - \epsilon$ each class of $\Delta = \Delta_1 \cdot \Delta_2 \dots \Delta_m$ contains less than r elements. Clearly $e_r(n, \epsilon)$ is for $r = 2$ equal to $e_2(n, \epsilon)$ defined in the previous §. Now it can be proved (though the proof is rather complicated) that for $r = 2, 3, \dots$ we have

$$(5.3) \quad \lim_{n \rightarrow \infty} \frac{\log_2 n}{e_r(n, \epsilon)} = (1 - \frac{1}{r}) I_r(P) = \frac{1}{r} \log_2 \frac{1}{\sum_{k=1}^a p_k^r}.$$

As it is easy to see the right hand side of (5.3) is an increasing function of r .

Another closely related relation containing $I_r(P)$ which however is easy to prove, is as follows: let $f_r(n)$ denote the least value of m such that the expected number of such r -tuples of elements of S_n which belong to the same class of Δ does not exceed 1; then we have

$$(5.4) \quad f_r(n) = \frac{\log_2 n}{(1 - \frac{1}{r}) I_r(P)} + O(1)$$

As a matter of fact, if $v_r(m, n)$ denotes the number of r tuples of elements of S_n which belong to the same class of $\Delta = \Delta_1 \dots \Delta_m$, then we have evidently

$$(5.5) \quad E(v_r(m, n)) = \binom{n}{r} \left(\sum_{k=1}^a p_k^r \right)^m$$

and (5.5) clearly implies (5.4).

The quantity $I_\alpha(P)$ has the same additivity property as $H(P)$ for each positive value of α ; that is for any two probability distribution P and Q we have

$$(5.6) \quad I_\alpha(P \times Q) = I_\alpha(P) + I_\alpha(Q)$$

If $p_1 = p_2 = \dots = p_a = \frac{1}{a}$ then $I_\alpha(P) = \log_2 a$ for each $\alpha > 0$. For other distributions $I_\alpha(P)$ is a decreasing function of α .

As regards other properties of $I_\alpha(P)$ these will be discussed in connection with the axiomatic characterization of measures of information.

6. AXIOMATIC CHARACTERIZATION OF SHANNON'S MEASURE OF INFORMATION

Different sets of postulates have been found which characterize *Shannon's* entropy $H(P)$ (defined by (1.1) uniquely). The original set of postulates given by *Shannon* [1] himself was later somewhat simplified by *Chintschin* and *Faddeew* [11], [12]. In this last form these postulates are as follows: Let Π denote the set of all finite, discrete probability distributions $P = (p_1, \dots, p_a)$ ($p_k \geq 0$ ($k = 1, \dots, a$) and $\sum_{k=1}^a p_k = 1$).

Let us suppose that a function $I(P) = I[p_1, \dots, p_a]$ is defined for all $P \in \Pi$ which satisfies the following conditions:

- A) $I[p, 1-p]$ is continuous for $0 \leq p \leq 1$ and $I[\frac{1}{2}, \frac{1}{2}] = 1$.
- B) $I[p_1, \dots, p_a]$ is a symmetrical function of its variables.
- C) If $0 \leq \vartheta < 1$, we have

$$I[p_1, \dots, p_{a-1}, \vartheta p_a, (1 - \vartheta)p_a] = I[p_1, p_2, \dots, p_a] + p_a I[\vartheta, 1 - \vartheta]$$

Then $I(P) = H(P)$ where $H(P)$ is the entropy of the distribution P defined by (1.1). (For a simple proof see [12]).

The proof depends mainly on the following number theoretical lemma due to P. Erdős [13]: If $f(n)$ is an additive number theoretical function (i.e. $f(nm) = f(n) + f(m)$) further if $\lim_{n \rightarrow +\infty} (f(n+1) - f(n)) = 0$ then $f(n) = c \log n$ where c is a constant. (For simple proofs see [14] and [15]).

Note that postulate C) implies that $I(P)$ has the additivity property

$$(6.1) \quad I(P \times Q) = I(P) + I(Q)$$

but C) is not implied by (6.1). As a matter of fact C) is not valid for $I_\alpha(P)$ with $\alpha \neq 1$. However C) can be replaced by (6.1) and by some other supplementary condition. For instance Chaundy and McLeod [16] have remarked that if we suppose that $I(P)$ is of the form $I(P) = \sum_{k=1}^a F(p_k)$ where $F(x)$ is continuous in the interval $[0, 1]$ and $F(\frac{1}{2}) = \frac{1}{2}$ and if $I(P)$ satisfies (6.1) then $F(p) = p \log_2 \frac{1}{p}$ and thus $I(P) = H(P)$ (see also [17] where it is shown that it is sufficient to suppose the validity of (6.1) for the case when P and Q have an equal number of terms).

Another such condition has been given in [9], for functions $I(P)$ defined for the wider class of *generalized probability distributions*, including also incomplete distributions.

Let Π^* denote the set of all finite sequences $P = (p_1, \dots, p_a)$ of nonnegative numbers such that $0 < w(P) = \sum_{k=1}^a p_k \leq 1$. We shall call every $P \in \Pi^*$ a *generalized distribution* and $w(P) = \sum_{k=1}^a p_k$ the *weight* of the generalized distribution P . A distribution $P \in \Pi^*$ will be called a *complete probability distribution* if $w(P) = 1$ and an *incomplete probability distribution* if $w(P) < 1$. The natural extension of Shannon's formula for $P \in \Pi^*$ is

$$(6.2) \quad H(P) = \frac{\sum_{k=1}^a p_k \log_2 \frac{1}{p_k}}{\sum_{k=1}^a p_k}$$

The direct product $P \times Q$ is defined in the same way for generalized probability distribution as for ordinary (complete) probability distributions. If $P \in \Pi^*$ and $Q \in \Pi^*$ where $P = (p_1, \dots, p_a)$, $Q = (q_1, \dots, q_b)$ and $w(P) + w(Q) \leq 1$ we put $P \cup Q = (p_1, \dots, p_a, q_1, \dots, q_b)$. (If $w(P) + w(Q) > 1$ then $P \cup Q$ is not defined.)

Now we have shown that if $I(P) = I[p_1, \dots, p_a]$ is defined for $P \in \Pi^*$ such that

A*) $I[p]$ is continuous for $0 < p \leq 1$, and $I[\frac{1}{2}] = 1$

B*) $I[p_1, \dots, p_a]$ is a symmetric function of its variables,

C₁*) $I(P \times Q) = I(P) + I(Q)$, further

C₂*) if $w(P) + w(Q) \leq 1$ then

$$I(P \cup Q) = \frac{w(P) I(P) + w(Q) I(Q)}{w(P) + w(Q)}$$

then $I(P) = H(P)$ where $H(P)$ is defined by (6.2).

An incomplete probability distribution P can be interpreted as the probability distribution of a random variable whose value can not be observed always only with probability $w(P)$.

Note that the extension of the notion of information (entropy) to incomplete distributions has among others the advantage that it has a sense to speak about the entropy of a single event with probability p , this being equal to $\log_2 \frac{1}{p}$.

Thus introducing this extension of the notion of entropy one can say that the entropy of a probability distribution is equal to the weighted mean of the entropies of its terms, the weights being the probabilities themselves.

7. AXIOMATIC CHARACTERIZATION OF MEASURES OF INFORMATION OF ORDER α

By weakening to some extent the axiom C) one can obtain a characterization of the measures of information of order α . These investigations show that in a certain sense there are no other measures of information besides those of order $\alpha \neq 1$ which have similar properties as Shannon's measure of information. This was conjectured by the author in [9], and his conjecture was proved by *J. Aczél* and *Z. Daróczy* in [17]. Their result has been recently sharpened by *Z. Daróczy* [18].

We reproduce here only this last result which is as follows: If $I(P)$ is defined for $P \in \Pi$, satisfies the condition (6.1) further there exists a function $f(x)$ such that

$$(7.1) \quad I(P) = \log_2 \frac{1}{M(P)}$$

with

$$(7.2) \quad M(P) = f^{-1} \left(\sum_{k=1}^a p_k f(p_k) \right)$$

where $f(x)$ is a strictly monotonic function, $\lim_{x \rightarrow 0} x f(x) = 0$ and $f(x)$ is continuous for $0 < x \leq 1$, then $f(x)$ is either a linear function or a linear function of an exponential function and correspondingly either $I(P) = H(P) = I_1(P)$ or $I(P) = I_\alpha(P)$ with $\alpha \neq 1$, $\alpha > 0$.

Note that the continuity of $I(P)$ follows from the continuity of $x f(x)$ while the symmetry of $I(p_1, \dots, p_n)$ from the symmetric form of $M(P)$.

The expression $M(P)$ is called by *J. Aczél* and *Z. Daróczy* a mean value of the probability distribution P .

The mentioned theorem can be stated also in the following form: a mean value $M(P)$ of the distribution $P = (p_1, \dots, p_a)$ which is of the form (7.2) where $f(x)$ is strictly monotonic and $x f(x)$ continuous for $0 \leq x \leq 1$ and which has the multiplicative property

$$(7.3) \quad M(P \times Q) = M(P) \cdot M(Q)$$

is necessarily either of the form

$$(7.4) \quad M(P) = \prod_{k=1}^a p_k^{p_k}$$

or of the form

$$(7.5) \quad M(P) = \left(\sum_{k=1}^a p_k^\alpha \right)^{\frac{1}{\alpha-1}} \text{ with } \alpha > 0, \alpha \neq 1$$

Shannon's entropy can be uniquely characterized as follows: Let $R = \{r_{jk}\}$ ($1 \leq j \leq a; 1 \leq k \leq b$) be any distribution whose projections are the distribution $P = \{p_1, \dots, p_a\}$ and $Q = \{q_1, \dots, q_b\}$, i.e.

$$\sum_{k=1}^b r_{jk} = p_j \quad (1 \leq j \leq a) \quad \text{and} \quad \sum_{j=1}^a r_{jk} = q_k \quad (1 \leq k \leq b).$$

We shall write $R = [P, Q]$

If $r_{jk} = p_j \cdot q_k$, i.e. if $R = P \times Q$ then one has for every

$$I_\alpha(R) = I_\alpha(P) + I_\alpha(Q).$$

However the inequality

$$(7.6) \quad I_\alpha(R) \leq I_\alpha(P) + I_\alpha(Q)$$

holds for any $R = [P, Q]$, if and only if $\alpha = 1$.

8. CHARACTERIZATION OF THE MEASURES OF INFORMATION OF ORDER α OF GENERALIZED PROBABILITY DISTRIBUTIONS

In analogy with (6.2) the measure of information $I_\alpha(P)$ of order α ($\alpha > 0, \alpha \neq 1$) of a generalized distribution $P \in \Pi^*$ ($P = \{p_1, \dots, p_a\}$) is defined by

$$(8.1) \quad I_\alpha(P) = \frac{1}{1-\alpha} \log_2 \frac{\sum_{k=1}^a p_k^\alpha}{\sum_{k=1}^a p_k}.$$

Note that if $P \in \Pi^*$ consists of a single term i.e. $P = \{p\}$ we have for each value of α

$$(8.2) \quad I_\alpha(\{p\}) = \log_2 \frac{1}{p}$$

Z. Daróczy [19] has shown that the quantities (6.2) and (8.1) can be characterized as follows: Let $I(P) = I[p_1, \dots, p_a]$ be defined for $P \in \Pi^*$ and suppose that $I(P)$ satisfies the following postulates:

A*) $I[p]$ is a continuous function of p in the interval $0 < p \leq 1$, and $I[\frac{1}{2}] = 1$

C₁*) $I(P * Q) = I(P) + I(Q)$

C₃*) There exists a strictly monotonic and continuous function $g(x)$ such that if $P \in \Pi^*, Q \in \Pi^*$ further $w(P) + w(Q) \leq 1$ then

$$I(P \cup Q) = g^{-1} \left[\frac{w(P) g(I(P)) + w(Q) g(I(Q))}{w(P) + w(Q)} \right]$$

Then $g(x)$ is either a linear function or a linear function of an exponential function and correspondingly either $I(P) = H(P)$ or $I(P) = I_\alpha(P)$ with some real $\alpha \neq 1$. J. Aczél [20] has simplified the proof of this theorem. He remarked also that the undesirable functions $I_\alpha(P)$ with $\alpha < 0$ can be excluded by the additional postulate:

D*) $\lim_{q \rightarrow 0} I[p, q] = I[p].$

9. AXIOMATIC CHARACTERIZATION OF INFORMATION WITHOUT USING PROBABILITIES

An interesting attempt has been made recently by R. S. Ingarden and K. Urbanik (see [21], [22]). They gave an axiomatic characterization of Shannon's measure of infor-

mation, which does not presuppose the notion of probability. Information is defined as a real valued function on a set X of finite Boolean rings. Each ring $R \in X$ is interpreted as an experiment, the elements of the ring as events. As regards X it is supposed that if R_1 is a ring belonging to X and R_2 a nontrivial subring of R_1 then R_2 belongs to X also, further if $R_1 \in X$ there exists another ring $R_2 \in X$ such that R_1 is a proper subring of R_2 . With respect to any real valued function F defined on X a distance function $\rho_F(R_1, R_2)$ is defined as follows: $\rho_F(R_1, R_2) = 1$ if R_1 and R_2 are non-isomorphic, while $\rho_F(R_1, R_2) = \delta_F(R_1, R_2) / (1 + \delta_F(R_1, R_2))$ if R_1 and R_2 are isomorphic, where $\delta_F(R_1, R_2) = \min_{\varphi} \max_R |F(R) - F(\varphi(R))|$ where R runs over all subrings of R_1 and φ over all isomorphisms of R_1 onto R_2 . X is a pseudometric space with respect to ρ_F . A ring $R \in X$ is called F -homogeneous if for every automorphism ψ of R and for every subring R_1 of R we have $F(R_1) = F(\psi(R_1))$. Let X_F denote the class of all F -homogeneous rings from X and their subrings. The function F is called regular if X_F is dense in X with respect to the metric ρ_F . Let as usual $\cup$ resp. $\cap$ denote union (joint) resp. intersection (meet) and $-$ difference of elements of a Boolean ring. For any $A \in R$ let us put $\bar{A} = 1(R) - A$ where $1(R)$ is the unity element of R .

If R is a ring and $A \in R$ let $A|R$ denote the subring of R consisting of all $B \in R$ which can be written in the form $B = A \cap C$ with $C \in R$. If $R \in X$ and $A \in R$ let $R|A$ denote the least Boolean ring containing A and all elements of $\bar{A}R$ where $\bar{A} = 1(R) - A$. ($R|A$ can be interpreted as the experiment which differs from the experiment R only in that the outcomes belonging to A are "pooled".)

A real valued function $H = H(R)$ defined for $R \in X$ is called an information if it satisfies five axioms of which the first is as follows:

$$I) (H(R) - H(\bar{R}_3)) H(R_1) H(R_2) = (H(R) - H(\bar{R}_1)) H(R_2) H(R_3) + (H(R) - H(\bar{R}_2)) H(R_1) H(R_3)$$

Here R is any element of X , $R_1 = A|R$, $R_2 = B|R$ where A and B are any disjoint elements $\neq 0$ of R , $R_3 = (A \cup B)|R$, $\bar{R}_1 = R|A$, $\bar{R}_2 = R|B$, $\bar{R}_3 = R|A \cup B$.

The second axiom can be formulated as follows:

$$II) \text{ If } R_1 \in X, R_2 \in X, A \in R_1, B \in R_2 \text{ further if } \rho_H(A|R_1, B|R_2) = 0 \text{ and } \rho_H(R_1|\bar{A}, R_2|\bar{B}) = 0 \text{ (here of course } \bar{B} \text{ stands for } 1(R_2) - B) \text{ then}$$

$$H(R_1) - H(R_1|A) = H(R_2) - H(R_2|B).$$

The next two axioms postulate the monotonicity of information $H(R_2) < H(R_1)$ if R_2 is a proper subring of R_1 , further that isomorphic H -homogeneous rings have ρ_H distance 0. The last axiom normalizes information by postulating that if R is an H -homogeneous ring having two atoms then $H(R) = 1$.

Ingarden and Urbanik proved the following theorem:

If H is an information on X then for every $R \in X$ there exists a unique strictly positive probability measure $P(A|R)$ defined for $A \in R$ such that for every subring

$$R_1 \text{ of } R \text{ and for every } B \in R_1 \text{ one has } P(B|R_1) = \frac{P(B|R)}{P(1(R_1)|R)} \text{ where } 1(R_1) \text{ is the unity element of } R_1, \text{ and } H(R) = \sum P(A|R) \log_2 \frac{1}{P(A|R)} \text{ where the base of the logarithm is 2 and } A \text{ runs over all atoms of } R.$$

By other words the information as defined by the axioms of the authors (which do

not presuppose the notion of probability) can be expressed by *Shannon's* well known formula by means of a uniquely defined (conditional) probability measure, the existence of which follows from the existence of information. Thus the axiomatic approach of the authors shows that though the usual logical order, according to which information is defined by means of probability can be reversed, and one can introduce information first, without using probabilities, probabilities come in however inevitably at a later stage.

It seems to us that the fact that a theory which starts with the aim to define information without probability leads to the proof of the existence of (conditional) probabilities, supports the view that the notion of information can not be separated from that of probability. The situation becomes particularly clear if we adopt the point of view of § 8, i.e. we consider also the information corresponding to an incomplete distribution (i.e. to an experiment whose result is not always observable.)

In this case to each event A there correspond two numbers: its probability $P(A)$ and its information content $I(A)$, which are connected by the formulae

$$(9.1) \quad I(A) = \log_2 \frac{1}{P(A)}, \quad P(A) = 2^{-I(A)}$$

Thus it does not matter which of $P(A)$ or $I(A)$ is taken as fundamental, the other can be expressed by it.

An interesting feature of the result is that the probabilities whose existence is deduced from that of information are not ordinary but conditional probabilities in the sense of the author's paper [23].

Let us add some remarks concerning the meaning of the axioms of *Ingarden* and *Urbanik*.

Clearly the axiom C) of *Faddeew* can be expressed with the present notations as follows:

$$(9.2) \quad H(R) = H(R|A) + P(A) H(A R)$$

Thus if $H(A R) > 0$, we have

$$(9.3) \quad P(A) = \frac{H(R) - H(R|A)}{H(A R)}$$

Now in the light of the formula (9.3) the meaning of the axioms becomes clear. As a matter of fact if we define the probability $P(A)$ by (9.3) then evidently the first axiom expresses the additivity of probability. As regards the second axiom it expresses the fact, that while in the definition (9.3) of $P(A)$ there occurs the ring R which can be chosen arbitrarily with the single restriction that it should contain the event A , nevertheless the value of $P(A)$ does not depend on the choice of R . Thus axioms I) and II) together imply axiom C). In view of this it is now clear why the axioms of *Ingarden* and *Urbanik* characterize *Shannon's* measure of information.

The axioms of *Ingarden* and *Urbanik* can be formulated also in term of finite algebras of sets instead of Boolean rings. We do not go into the details here.

10. CONCLUDING REMARKS

In addition to what has been said in the previous § about the relation of the notions of probability and information, one remark has to be added. While when speaking about a simple event A , both its probability $P(A)$ and its information content $I(A)$

are positive numbers⁶, connected by formula (9.1) further in this case the measures of information of order α have all the same value, the situation changes when we are dealing with a system of (disjoint) events $(A_1, A_2, \dots, A_a)$. In this case we have a corresponding probability distribution $P = (P(A_1), P(A_2), \dots, P(A_a))$ being a set of numbers (or to put it otherwise, the probability distribution is vector-valued).

On the other hand we have different measures of information $I_\alpha(P)$ corresponding to the distribution P , all of which are *number-valued*. All these measures of information are obtained from the *information-distribution* $J = (I(A_1), I(A_2), \dots, I(A_a))$ corresponding to the events $A_1, A_2, \dots, A_a$ by some method of averaging, i.e. they are all mean values. This explains why different measures of information are possible: the situation is the same as taking different (arithmetic, geometric, harmonic etc.) mean values of a set of numbers. Shannon's measure of information is clearly the simplest among them, and plays a role analogous to that of the ordinary (linear) mean value. Nevertheless in certain situations the other non-linear mean values of information (i.e. the informations of order $\alpha > 0, \alpha \neq 1$) may also be useful.

REFERENCES

- [1] Shannon, C. (1948). A mathematical theory of communication. *Bell System Technical Journal*, 27, 379-423, 623-653.
- [2] Wolfowitz, J. (1961). Coding theorems of information theory. *Ergebnisse der Mathematik und ihre Grenzgebiete*, Springer, Berlin-Göttingen-Heidelberg, 1-125.
- [3] Strassen, W. (1962). Asymptotic expansions in information theory. *Colloquium on combinatorial methods in probability theory*, Aarhus, 74-77.
- [4] Jushkewich, A. (1958). On a limit theorem connected with the notion of the entropy of a Markov chain. *Uspechi Mat. Nauk*, 8, p. 5 (in Russian).
- [5] Rényi, A. (1961). On random generating elements of a finite Boolean algebra. *Acta Scientiarum Mathematica Szeged*, 22, 75-81.
- [6] Rényi, A. (1961). Statistical laws of accumulation of information. *Bulletin de l'Institut International de Statistique, 33rd Session*, Paris, 1-7.
- [7] Rényi, A. (1962). On statistical laws of the accumulation of information. *Magyar Tudományos Akadémia III. Osztályának Közleményei*, 12, 15-33.
- [8] Rényi, A. (1961). On a problem of information theory. *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, 6, 505-516. (in Hungarian with English and Russian summaries)
- [9] Rényi, A. (1961). On measures of entropy and information. *Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability*. University of California Press, Vol. I, 547-561.
- [10] Rényi, A. (1962). Wahrscheinlichkeitsrechnung, mit einem Anhang über Informationstheorie. *Deutscher Verlag der Wissenschaften*, Berlin, 435-498.
- [11] Chintschin, A. J. (1957). Der Begriff der Entropie in der Wahrscheinlichkeitsrechnung. *Arbeiten zur Informationstheorie, I*. Deutscher Verlag der Wissenschaften, Berlin, 7-25.
- [12] Faddeev, D. K. (1957). Zum Begriff der Entropie eines endlichen Wahrscheinlichkeitsschemas, *Arbeiten zur Informationstheorie*. Deutscher Verlag der Wissenschaften, Berlin, 88-90.
- [13] Erdős, P. (1946). On the distribution function of additive functions. *Annals of Mathematics*, 47, 1-20.
- [14] Rényi, A. (1960). On a theorem of P. Erdős and its application in information theory. *Mathematica*, 1, 341-344.
- [15] Besicovitch, A. S. (1962). On additive functions of a positive integer. *Studies in Mathematical Analysis and related topics*, Stanford University Press, Stanford, 38-41.
- [16] Chaundy, T. W. and McLeod, J. B. (1960). On a functional equation. *Edinburgh Mathematical Notes*, 43, 7-8.
- [17] Aczél, J. and Daróczy, Z. (1963). Charakterisierung der Entropien positiver Ordnung und der Shannonschen Entropie. *Acta Mathematica Academiae Scientiarum Hungaricae*, 14, 95-121.

⁶ We exclude here for the sake of simplicity both impossible and sure events.

- [18] Daróczy, Z. (1964). Über Mittelwerte und Entropien vollständiger Wahrscheinlichkeitsverteilungen. *Acta Mathematica Academiae Scientiarum Hungaricae*, 15, 203–210.
- [19] Daróczy, Z. (1963). Über die gemeinsame Charakterisierung der zu den nicht vollständigen Verteilungen gehörigen Entropien von Shannon und von Rényi. *Zeitschrift für Wahrscheinlichkeitstheorie*, 1, 381–388.
- [20] Aczél, J. Zur gemeinsamen Charakterisierung der Entropien α -ter Ordnung und der Shannonschen Entropie nicht unbedingt vollständiger Verteilungen. *Zeitschrift für Wahrscheinlichkeitstheorie* (in print).
- [21] Ingarden, R. S. and Urbanik, K. (1961). Information as a fundamental notion of statistical physics. *Bulletin de L'Académie des Sciences Polonaise, Ser. sci. math.*, 9, 313–316.
- [22] Ingarden, R. S. and Urbanik, K. (1962). Information without probability. *Colloquium Mathematicum*, 9, 131–150.
- [23] Rényi, A. (1955). A new axiomatic theory of probability. *Acta Mathematica Academiae Scientiarum Hungaricae*, 6, 285–335.

DISCUSSION

C. R. RAO: Is there any special advantage in choosing $\alpha = 1/2$ in the measure of information?

$$P_{\alpha}(p) = \frac{1}{1-\alpha} \log_2 \sum_{i=1}^k p_i^{\alpha}.$$

It was found useful in theory of statistical inference as a measure of distance between $(p_1, \dots, p_k)$ and the uniform distribution $(\frac{1}{k}, \dots, \frac{1}{k})$.

A. RÉNYI: In answer to the question of Professor Rao, I should like to mention that in a previous paper I made reference to the work of Indian mathematicians concerning the case $\alpha = 1/2$ in connection with the information – theoretical distance of two probability distributions. In the present paper, however, I dealt only with the amount of information connected with a single distribution, and it seems to me that in this case the information of order $1/2$ does not play the same exceptional role.

D. G. KENDALL: In § 6 of his paper Prof. Rényi recalls the theorem of Fadeev, that Shannon's function is uniquely characterised by the conditions A, B, and C. The assumption that $h(t) = I(t, 1-t)$ is continuous for $0 < t < 1$ is very natural, but the more severe assumption (used by Fadeev) that $h(\cdot)$ is continuous for $0 \leq t \leq 1$ is not so natural; it excludes the possibility of solutions for which $h(t) \rightarrow -\infty$ when $t \downarrow 0$. A different argument (due to H. Tverberg) replaced the continuity assumption of Fadeev by the requirement that $h \in L(0, 1)$, but this is not at all natural, and is still undesirably restrictive. I have shown that Shannon's function is uniquely characterised by B and C, the condition that $h(1/2) = 1$, and the condition that $h(\cdot)$ is to be non-decreasing for $0 < t \leq 1/2$. In a sequel to this work Mr. P. M. Lee has shown that Shannon's function is uniquely characterised by B and C, the condition that $h(1/2) = 1$, and the condition that $h(\cdot)$ is to be Lebesgue measurable on $(0, 1)$. It seems likely that Lee's theorem is incapable of further improvement, in the sense that there may exist non-measurable solutions to the functional equations, but attempts to construct such non-measurable entropies have so far proved unsuccessful. It is not, of course, suggested that the question of their existence has any practical relevance.

110, 120, 174, 180, 237

NOTE

This is a very clear and persuasive exposition of Rényi's views on the fundamental question of how to measure the information. Taking for granted that information is essentially connected with probability and using the criterion that a measure of information needs both operational (pragmatic) and postulational (axiomatic) justification, he arrives at the family of entropies of order $\alpha > 0$; of course, the case $\alpha = 1$ (i.e. Shannon's entropy) plays a distinguished role. In addition to the mentioned search problems leading to entropies of order $\alpha \neq 1$, now such coding problem is also known, see Campbell [1]. On the further developments of the theory of postulational characterizations of information measures see e.g. Aczél [5], Aczél and Daróczy [6]. It should be noted that an operationally useful generalization of Shannon's entropy may be obtained also in another way, see the comments to No. 174.

The idea of information without probability has been revived by Kampé de Fériet and Forte [2]; their approach appears more natural than that of Ingarden and Urbanik, but it still needs a "pragmatic" justification. For further developments of this theory, see e.g. Kampé de Fériet [3] and Forte [4]. [I. Cs.]

(Reference [14] of this paper is not included in this volume since it is fully reproduced in Rényi No. 175; see also the comments there.)

REFERENCES

- [1] Campbell, L. L.: A coding theorem and Rényi's entropy. *Information and Control*, 8 (1965), 423—429.
- [2] Kampé de Fériet, J. and Forte, B.: Information et probabilité. *Comptes Rendus*, 265A (1967), 110—114.
- [3] Kampé de Fériet, J.: Mesure de l'information fournie par un événement. Les Probabilités sur les structures Algébriques. *Colloques Internationaux du CNRS*, (1970), 191—221.
- [4] Forte, B.: Generalized measures of information and uncertainty. *Proc. Meeting on Information Measures*, Kitchener-Waterloo, (1970), I.17—I.31.
- [5] Aczél, J.: On measures of information and their characterizations. *Proc. Meeting on Information Measures*, Kitchener-Waterloo, (1970), I.1—I.17.
- [6] Aczél, J. and Daróczy, Z.: *On information measures and their characterizations*. Academic Press, New York, (1973).

PROBABILISTIC METHODS IN GROUP THEORY

By

P. ERDÖS AND A. RÉNYI
in Budapest, Hungary

Introduction

The application of probabilistic methods to another chapter of mathematics (number theory, different branches of analysis, graph theory etc.) has in the last 30 years often led to interesting results, which could not be obtained by the usual methods of the chapters in question. These results are in most cases of the following character: it is shown that in some sense “most” elements of a set of mathematical objects possess a certain property. Thus these results deal with typical properties of elements of a certain set, neglecting elements which behave in a different way, provided that their number is in some sense negligibly small. If the number of elements of the set considered is infinite a certain natural measure has to be introduced and relations are studied which are valid for “almost all” elements of the set considered, i.e. with the exception of subset of measure zero according to the chosen measure. If finite systems are studied, then the most natural measure is the number of elements of the sets considered. In such cases the point of view usually adopted is as follows: if $S_n (n = 1, 2, \dots)$ is a sequence of finite sets, the number of elements of S_n being equal to $N(n)$ where $\lim_{n \rightarrow +\infty} N(n) = +\infty$, and if $A(n)$ denotes the number of elements of S_n having the property A , and if $\lim_{n \rightarrow +\infty} \frac{A(n)}{N(n)} = 1$, we say that in the limit for $n \rightarrow +\infty$ “almost all” elements of S possess the property A .

In proving such assertions, probabilistic methods are usually the natural tool, in spite of the fact that the problem considered has nothing to do with chance.

It often happens that the easiest (or the only available) way to prove that S contains at least one element having the property A for sufficiently large

values of n , is to prove that $\liminf_{n \rightarrow +\infty} \frac{A(n)}{N(n)} > 0$; in this way the existence of elements of S_n having property A can be proved while the actual construction of an element of S_n having the property A cannot be carried out. Thus probabilistic considerations lead often to proofs of existence concerning finite systems. While investigations of the above described type have been frequently made in number theory (see for instance [1], where further references are given) and graph theory (we mention here for instance our papers [2], [3], [4]; [5]), up to now such methods were only exceptionally (see [6]) applied to the study of finite algebraic systems.

In the present paper we shall give an example of applying probabilistic methods to the study of finite groups.

Let G_n be a finite Abelian group of order n . (We use the additive notation for the group operation). Let us choose k arbitrary elements of G_n , and denote them by $a_1, a_2, \dots, a_k$. Let us consider all possible 2^k sums $\varepsilon_1 a_1 + \varepsilon_2 a_2 + \dots + \varepsilon_k a_k$ where $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k$ are equal either to 0 or to 1. In other words we consider the set of all possible sums $a_{i_1} + a_{i_2} + \dots + a_{i_r}$ where $1 \leq i_1 < i_2 < \dots < i_r \leq k$ and $0 \leq r \leq k$. The question is now, whether all elements b of G_n can be represented in the form $b = \sum_{i=1}^k \varepsilon_i a_i$?

Of course this is possible only if $2^k \geq n$, i.e. if $k \geq \frac{\log n}{\log 2}$. We shall prove in §2 (see Theorem 2) that if we choose the elements $a_1, \dots, a_k$ of G_n at random and if $k \geq \frac{\log n + \log \log n + \omega_n}{\log 2}$ where ω_n tends to $+\infty$ for $n \rightarrow +\infty$ arbitrarily slowly, then every $b \in G_n$ can be represented in the form

$$(1) \quad b = \sum_{i=1}^k \varepsilon_i a_i$$

with probability tending to 1 for $n \rightarrow +\infty$. It is natural to ask also, how much larger the value of k has to be chosen that each $b \in G_n$ should have approximately the same number of representations in the form (1). We shall prove in §1 that if $k \geq \frac{2 \log n + c}{\log 2}$ where c is a sufficiently large positive number then every

$b \in G_n$ has approximately the same number of representations in the form (1) with probability near to 1 (see Theorem 1). More exactly, if

$$k \geq \frac{2 \log n + 2 \log \frac{1}{\varepsilon} + \log \frac{1}{\delta}}{\log 2}$$

then with probability $\geq 1 - \delta$ the number of representations of b in the form (1) is contained between $(1 - \varepsilon) \frac{2^k}{n}$ and $(1 + \varepsilon) \frac{2^k}{n}$ for all $b \in G_n$; here ε and δ are arbitrary small positive numbers (Theorem 2). We conjecture but could not prove up to now that the factor 2 of $\log n$ in Theorem 1 cannot be replaced by a smaller number.

The method which we apply to prove Theorem 1 consists of two steps: The first step consists simply in the evaluation of the expectation of the mean square deviation of the random distribution $\frac{V_k(b)}{2^k}$, where $V_k(b)$ denotes the number of representations of b in the form (1). This idea has been first applied to a particular problem of number theory by *P. Turán* [7]. The idea has been recently developed by *Ju. V. Linnik* [8] into a powerful method in number theory, called by him the "dispersion method". The second step may be characterized as utilizing the smoothing effect of random choice: if most of the numbers $V_k(b)$ are almost equal, but a few of them may be considerably smaller or larger than the average, then by choosing a relatively small number of further elements $a_{k+1}, \dots, a_{k+j}$ at random, the distribution gets smoothed out, i.e. the distribution $\{2^{-k+r} V_{k+r}(b)\} (b \in G_n)$ is usually much more uniform than the distribution $\{2^{-k} V_k(b)\}$.

§1. Finite Abelian groups

Let G_n be an Abelian group of order n . The elements of G_n will be denoted by $a, b, c, \dots$ with or without indices. The group operation will be written as addition; accordingly we denote by 0 the unit-element of the group, and by $-a$ the element for which $a + (-a) = 0$; for any $a \in G_n$ we put $1 \cdot a = a$ and $0 \cdot a = 0$. Let $a_1, a_2, \dots, a_k$ be k elements of G chosen at random, inde-

pendently of each other, so that each a_j may be equal to an arbitrary element of G_n with the same probability $\frac{1}{n}$. We denote by $V_k(b)$ the number of representations of an element b of G_n in the form

$$(1.1) \quad b = \varepsilon_1 a_1 + \varepsilon_2 a_2 + \cdots + \varepsilon_k a_k$$

where each of the numbers ε_j may have the value 0 or 1. Then for each $b \in G$ $V_k(b)$ is a random variable.

If the values of $a_1, \dots, a_k$ are fixed, clearly

$$\sum_{b \in G} V_k(b) = 2^k$$

and thus $\left\{ \frac{V_k(b)}{2^k} \right\}$ is a probability distribution. Let $P(\dots)$ denote the probability of the event in the brackets and let $E(\dots)$ denote the expectation of the random variable in the brackets.

In what follows we shall often use the following elementary inequality, called usually Markoff's inequality: if ξ is any nonnegative random variable and λ a real number, $\lambda > 1$, then

$$(1.2) \quad P(\xi \geq \lambda E(\xi)) \leq \frac{1}{\lambda}.$$

If A and B are events, ξ and η random variables, we shall denote by $P(A|B)$ the conditional probability of the event A under the condition B , by $E(\xi|B)$ the conditional expectation of ξ under the condition B and by $E(\xi|\eta)$ the conditional expectation of ξ given η .

We prove first the following

Lemma.

$$(1.3) \quad D_k^2 = E \left(\sum_{b \in G} \left(V_k(b) - \frac{2^k}{n} \right)^2 \right) = 2^k \left(1 - \frac{1}{n} \right)$$

Proof of the Lemma. We have clearly

$$(1.4) \quad D_k^2 = \sum_{b \in G} E(V_k^2(b)) - \frac{2^{2k}}{n}$$

Now

$$(1.5) \quad V_k(b) = \sum_{\varepsilon_1 a_1 + \dots + \varepsilon_k a_k = b} 1$$

where the summation has to be extended over all 2^k k -tuples $(\varepsilon_1, \dots, \varepsilon_k)$ of zeros and ones. Thus we obtain

$$(1.6) \quad \sum_b E(V_k^2(b)) = \sum \sum P(\varepsilon_1 a_1 + \dots + \varepsilon_k a_k = \varepsilon'_1 a_1 + \dots + \varepsilon'_k a_k)$$

where $(\varepsilon_1, \dots, \varepsilon_k)$ and $(\varepsilon'_1, \dots, \varepsilon'_k)$ run independently over all k -tuples of zeros and ones. For the sake of brevity, let us put $\varepsilon = (\varepsilon_1, \dots, \varepsilon_k)$, $\varepsilon' = (\varepsilon'_1, \dots, \varepsilon'_k)$ further $a = (a_1, \dots, a_k)$, $(\varepsilon, a) = \sum_{j=1}^k \varepsilon_j a_j$ and $(\varepsilon', a) = \sum_{j=1}^k \varepsilon'_j a_j$. Clearly if $\varepsilon = \varepsilon'$ then $P((\varepsilon, a) = (\varepsilon', a)) = 1$. Now let us suppose that ε and ε' are not identical. Then there is value of h ($1 \leq h \leq k$) such that $\varepsilon_h \neq \varepsilon'_h$, i.e. either $\varepsilon_h = 1$ and $\varepsilon'_h = 0$, or $\varepsilon_h = 0$ and $\varepsilon'_h = 1$. Then if the values of ε_j for j different from h are fixed the equation $(\varepsilon, a) = (\varepsilon', a)$ has exactly one solution for a_h and the probability that a_h is equal to this unique value is clearly $\frac{1}{n}$; thus if $\varepsilon \neq \varepsilon'$ we obtain $P((\varepsilon, a) = (\varepsilon', a)) = \frac{1}{n}$. Thus we get

$$(1.7) \quad \sum_{\varepsilon} \sum_{\varepsilon'} P((\varepsilon, a) = (\varepsilon', a)) = 2^k + \frac{2^k(2^k - 1)}{n}$$

which proves our Lemma.

We can deduce from the Lemma immediately

Theorem 1. If

$$(1.8) \quad k \geq \frac{2 \log n + 2 \log \frac{1}{\varepsilon} + \log \frac{1}{\delta}}{\log 2}$$

where $\varepsilon > 0$ and $\delta > 0$ are arbitrary small positive numbers then

$$(1.9) \quad P\left(\text{Max}_{b \in G} \left| V_k(b) - \frac{2^k}{n} \right| \leq \varepsilon \frac{2^k}{n}\right) > 1 - \delta$$

Proof of Theorem 1. Clearly

$$(1.10) \quad \text{Max}_{b \in G_n} \left| V_k(b) - \frac{2^k}{n} \right|^2 \leq \sum_{b \in G_n} \left(V_k(b) - \frac{2^k}{n} \right)^2$$

and thus by Markoff's well known inequality and the Lemma

$$(1.11) \quad P\left(\text{Max}_{b \in G} \left| V_k(b) - \frac{2^k}{n} \right| > \varepsilon \frac{2^k}{n}\right) < \frac{n^2}{2^k \varepsilon^2}$$

Thus if (1.8) holds

$$(1.12) \quad P\left(\text{Max}_{b \in G_n} \left| V_k(b) - \frac{2^k}{n} \right| > \varepsilon \frac{2^k}{n}\right) < \delta$$

which proves (1.8).

It follows from Theorem 1 that there exists in every Abelian group of order n for each $k \geq \frac{2 \log n + 2 \log \frac{1}{\varepsilon} + \log \frac{1}{\delta}}{\log 2}$ k elements $a_1, \dots, a_k$ such that each element b of G_n can be represented in the form $b = \varepsilon_1 a_1 + \dots + \varepsilon_k a_k$ where $\varepsilon_j = 0$ or 1 ($j=1, 2, \dots, k$) $\frac{2^k}{n} (1 + \varepsilon_b)$ times where $|\varepsilon_b| \leq \varepsilon$.

An interesting special case is obtained if G_n is the additive group of residues mod n .

Now we proceed to prove

Theorem 2. For any $\delta > 0$ if

$$(1.13) \quad k \geq \frac{\log n + 2 \log \frac{1}{\delta} + \log \frac{\log n}{\log 2}}{\log 2} + 5$$

then

$$(1.14) \quad P\left(\min_{b \in G} V_k(b) > 0\right) > 1 - \delta.$$

Proof of Theorem 2. Put

$$(1.15) \quad k_1 = \left\lceil \frac{\log n}{\log 2} \right\rceil + d + 1$$

where d is a positive integer, $d \geq \frac{2 \log \frac{1}{\delta}}{\log 2} + 2$.

Then by Lemma 1, denoting by N_{k_1} the number of elements b of G_n for which $V_{k_1}(b) = 0$, we have

$$(1.16) \quad E(N_{k_1}) \leq \frac{n^2}{2^{k_1}}.$$

Thus it follows by Markoff's inequality that for any $\lambda > 1$

$$(1.17) \quad P\left(N_{k_1} > \lambda \frac{n^2}{2^{k_1}}\right) \leq \frac{1}{\lambda}.$$

Let us denote by A_0 the event $N_{k_1} \leq \lambda \frac{n^2}{2^{k_1}} \leq \frac{\lambda \cdot n}{2}$. Supposing that A_0 holds, we select an element a_{k_1+1} at random. Let N_{k_1+1} denote the number of elements b of G_n for which $V_{k_1+1}(b) = 0$. Clearly $V_{k_1+1}(b) = 0$ if and only if $V_{k_1}(b) = 0$ and $V_{k_1}(b') = 0$ where $b' = b - a_{k_1+1}$; and this has probability $\frac{N_{k_1}}{n}$. Thus it follows

$$(1.18) \quad E(N_{k_1+1} | N_{k_1}) = \frac{N_{k_1}^2}{n}$$

which implies

$$(1.19) \quad E(N_{k_1+1} | A_0) \leq \frac{\lambda^2 n}{2^{2d}}$$

and thus

$$(1.20) \quad P\left(N_{k_1+1} > \frac{2\lambda^3 n}{2^{2d}}\right) \leq \frac{1}{2\lambda}$$

Let A_1 denote the event $N_{k_1+1} \leq \frac{2\lambda^3 n}{2^{2d}}$, and let us now suppose that both A_0 and A_1 hold. Choosing the element a_{k_1+2} at random and repeating the same argument, we obtain

$$(1.21) \quad E(N_{k_1+2} | N_{k_1+1}) = \frac{N_{k_1+1}^2}{n}$$

and thus

$$(1.22) \quad E(N_{k_1+2} | A_0 A_1) \leq \frac{4\lambda^6 n}{2^{4d}}.$$

(Here and in what follows the product of events denotes the joint occurrence of these events). This implies

$$(1.23) \quad P\left(N_{k_1+2} > \frac{16\lambda^7 n}{2^{4d}} \mid A_0 A_1\right) \leq \frac{1}{4\lambda}.$$

Let us continue this process; let the elements $a_{k_1+3}, \dots, a_{k_1+j}$ be chosen at random independently and with a uniform distribution in G_n . Let in general A_{k_1+i} denote the event

$$(1.24) \quad N_{k_1+i} \leq \frac{2^{2^{i-1}} \lambda^{2^{i+1}-1} \cdot n}{2^{2^{i-1}d}} = M_i \quad (i = 0, 1, \dots, j)$$

then we obtain, putting $B_i = A_0 A_1 \dots A_i$ ($i = 0, 1, \dots, j$)

$$(1.25) \quad P(A_i | B_{i-1}) \leq \frac{1}{2^{i\lambda}} \quad (i = 0, 1, \dots, j).$$

Now clearly if j is an integer for which

$$(1.26) \quad j \geq \frac{\log \frac{\log n}{\log 2}}{\log 2}$$

then

$$(1.27) \quad M_j \leq \frac{1}{2} n^{(2 \log \lambda / \log 2) + 2 - d}$$

On the other hand we have

$$(1.28) \quad P(\bar{B}_j) = P(\bar{A}_0) + \sum_{i=1}^j P(\bar{A}_i | B_{i-1})$$

and thus, in view of $P(CD) = P(C|D)P(D) \leq P(C|D)$

$$(1.29) \quad P(\bar{B}_j) \leq P(\bar{A}_0) + \sum_{i=1}^j P(\bar{A}_i | B_{i-1})$$

Thus we obtain that

$$(1.30) \quad P(\bar{B}_j) \leq \frac{1}{\lambda} + \frac{1}{2\lambda} + \frac{1}{4\lambda} + \dots \leq \frac{2}{\lambda}.$$

Now we shall choose

$$(1.31) \quad \lambda = 2^{(d-2)/2}.$$

Then we have $\frac{2 \log \lambda}{\log 2} = d - 2$, and thus by (1.27)

$$(1.32) \quad M_j \leq \frac{1}{2} < 1.$$

It follows that if the event B_j takes place, $N_{k_1+j} = 0$. Thus if (1.26) holds,

$$(1.33) \quad P(\text{Min}_{b \in G_n} V_{k_1+j}(b) > 0) \geq 1 - 2^{1 - ((d-2)/2)}$$

and thus if $d \geq \frac{2 \log \frac{1}{\delta}}{\log 2} + 4$ then

$$(1.34) \quad P(\text{Min}_{b \in G} V_{k_1+j}(b) > 0) \geq 1 - \delta. \bullet$$

As k_1 is defined by (1.15) and j is an integer for which (1.26) holds, clearly $k = k_1 + j$ is any integer for which (1.13) holds.

This proves Theorem 2.

§2. Some remarks

In order to obtain some further insight into the problem, it would be useful to compute the moments

$$(2.1) \quad \mu_r(n, k) = E\left(\sum_{b \in G_n} [V_k(b)]^r\right).$$

for $r = 3, 4, \dots$. It is easy to show that

$$(2.2) \quad \mu_3(n, k) = 2^k + \frac{3 \cdot 2^k(2^k - 1)}{n} + \frac{2^k(2^k - 1)(2^k - 2)}{n^2}.$$

Formula (2.2) follows from the fact that if $\varepsilon^{(1)}$, $\varepsilon^{(2)}$ and $\varepsilon^{(3)}$ are any three different k -tuples of zeros and ones

$$P((\varepsilon^{(1)}, a) = (\varepsilon^{(2)}, a) = (\varepsilon^{(3)}, a)) = \frac{1}{n^2}.$$

However

$$P((\varepsilon^{(1)}, a) = (\varepsilon^{(2)}, a) = (\varepsilon^{(3)}, a) = (\varepsilon^{(4)}, a))$$

is not equal to $\frac{1}{n^3}$ for any four different k -tuples $\varepsilon^{(1)}, \varepsilon^{(2)}, \varepsilon^{(3)}, \varepsilon^{(4)}$, and this makes the computation of $\mu_r(n, k)$ for $r \geq 4$ more difficult.

A surprising feature of our results is that they do not depend at all on the structure of the group G_n .

Let us mention that both theorems 1 and 2 can be generalized for arbitrary non-Abelian finite groups, in the following way: Let G_n be any group of order n , let us choose the elements $a_1, \dots, a_k$ of G_n at random (with uniform distribution) and independently. Let $V_k(b)$ denote the number of representations of b in the form $b = a_{i_1} a_{i_2} \dots a_{i_r}$ (we now write the group-operation as multiplication) where $1 \leq i_1 < i_2 < \dots < i_r \leq k$ and $0 \leq r \leq k$ (an empty product denotes the unity element). Then the statements of Theorems 1 and 2 are valid.

However if we consider all possible products of different elements $a_{i_1} a_{i_2} \dots a_{i_r}$ which can be formed from the elements $a_1, a_2, \dots, a_k$ chosen at random, and do not consider only such products in which $i_1 < i_2 < \dots < i_r$, then the situation changes completely. In this case the structure of the group G_n becomes relevant. We feel, that the supposition that only such products formed from the elements $a_1, \dots, a_n$ chosen at random should be considered in which a_i always precedes a_j if both occur and $i < j$, is unnatural. This is the reason why we restricted ourselves in §1. to formulate our theorems for the case of Abelian groups.

REFERENCES

1. A. Rényi, Probabilistic methods in number theory, *Proceedings of the International Congress of Mathematicians*, Edinburgh, 1958, p. 529–539.
2. P. Erdős-A. Rényi, On random graphs, I. *Publicationes Mathematicae (Debrecen)* 6/1959/290–297.
3. P. Erdős-A. Rényi, On the evolution of random graphs, International Statistical Institute, 32. Session, Tokyo, 1960, 119.1–5.
4. P. Erdős-A. Rényi, On the evolution of random graphs, *MTA Mat. Kut. Int. Közleményei* 5/1960/17–61.
5. P. Erdős-A. Rényi, On the strength of connectedness of a random graph, *Acta Math. Acad. Sci. Hung.* 12/1961/261–267.
6. A. Rényi, On random generating elements of a finite Boolean algebra, *Acta Sci. Math. Szeged*, 22/1961/75–81.

7. P. Turán, On a theorem of Hardy and Ramanujan, *Journal of the London Math. Soc.* 9/1934/274-176.

8. Yu. V. Linnik, The dispersion method in binary additive problems /in Russian/, University of Leningrad, 1961, 1-208.

NOTE

The problem whether the bound for k in Theorem 1 can be replaced by a smaller one is investigated in [1] and [2]. Both papers are studying the moments $\mu_r(n, k)$ and showing that the factor $\frac{2}{\log 2}$ of $\log n$ in the bound of k can be replaced by a smaller constant if the properties of the underlying group are nice enough. (P. R.)

REFERENCES

- [1] Miecz, R. I.: On a conjecture of Erdős and Rényi. *Illinois J. of Math.*, 11 (1967), 114-127.
- [2] Bognár, K.: On a problem of statistical group theory. *Studia Sci. Math. Hung.* 5 (1970), 29-36.

SOME REMARKS ON PERIODIC ENTIRE FUNCTIONS

By

ALFRÉD RÉNYI and CATHERINE RÉNYI
in Budapest, Hungary

The second named author has proved [1] some years ago the following

Theorem. If $F(z) = \sum_{n=0}^{\infty} a_n z^n$ is a periodic entire function and $Z(N)$ denotes the number of those among the numbers $a_0, a_1, \dots, a_{N-1}$ which are equal to 0, one has

$$\liminf_{N \rightarrow +\infty} \frac{Z(N)}{N} \leq \frac{1}{2}.$$

It follows from this theorem that if $f(z)$ is an arbitrary entire function, $f(z^s)$ can not be periodic if s is a positive integer, $s \geq 3$; as a matter of fact, for $F(z) = f(z^s)$ we have

$$\liminf_{N \rightarrow +\infty} \frac{Z(N)}{N} \geq 1 - \frac{1}{s} > \frac{1}{2} \text{ if } s \geq 3.$$

Let us mention that there exist entire functions $f(z)$ such that $f(z^2)$ is periodic. For example, put

$$f(z) = \sum_{k=0}^{\infty} \frac{z^k}{(2k)!} = \frac{e^{\sqrt{z}} + e^{-\sqrt{z}}}{2},$$

then

$$f(z^2) = \frac{e^z + e^{-z}}{2}$$

is periodic with period $2\pi i$.

In general, if $P(z)$ is an arbitrary polynomial of degree 2, there can be found

an entire function $f(z)$ such that $f(P(z))$ is periodical. As a matter of fact, if $P(z) = Az^2 + Bz + C$ where $A \neq 0$ and

$$f(z) = \cos \sqrt{4A(z-C) + B^2} = \sum_{k=0}^{\infty} (-1)^k \frac{(4A(z-C) + B^2)^k}{(2k)!}$$

then

$$f(P(z)) = \cos(2Az + B)$$

is periodic with period $\frac{\pi}{A}$.

This led us to conjecture that if $f(z)$ is an arbitrary non constant entire function and $P(z)$ an arbitrary polynomial of degree ≥ 3 , then $f(P(z))$ can not be periodic.

In what follows we shall prove that this conjecture is in fact true (see Theorem 1). One may ask in general under what conditions can $f(g(z))$ be a periodic entire function if $f(z)$ and $g(z)$ are entire functions, and $g(z)$ is not periodic, and not a polynomial of degree ≤ 2 . One can easily give examples of periodic entire functions which can be represented in the form $f(g(z))$. For instance if $g(z) = z + e^z$ and $f(z) = e^z$, then $f(g(z)) = e^{z+e^z}$ is periodic with period $2\pi i$. In this direction we proved a counterpart of Theorem 1 (Theorem 2) according to which if $g(z)$ is an arbitrary not periodic entire function and $P(z)$ an arbitrary polynomial of degree ≥ 1 , then $P(g(z))$ can not be periodic. The problem of finding all pairs $f(z)$, $g(z)$ of entire functions such that $f(g(z))$ is periodic, remains open.

The aim of this note is, besides proving the mentioned two theorems, to call the attention to this unsolved problem.

We prove now

Theorem 1. *If $f(z)$ is an arbitrary not constant entire function and $P(z)$ an arbitrary polynomial of degree ≥ 3 , then the entire function $f(P(z))$ can not be periodic.*

Proof of Theorem 1. The idea of the proof is very simple and can be sketched as follows. Let $L(R)$ denote the set of values of z for which $|P(z)| = R > 0$. We may suppose that $P(z) = z^s + c_1 z^{s-1} + \dots + c_s$,

i.e., that the leading coefficient of $P(z)$ is equal to 1. If R is sufficiently large, $L(R)$ is a simple closed curve (a Cassini oval) the form of which is not much different from a circle with radius $\sqrt[s]{R}$. Let us consider the function $f(P(z))$ on $L(R)$. Let z_0 be a point on $L(R)$ in which $|f(P(z))|$ takes on its maximum on $L(R)$, and put $|f(P(z_0))| = M$. If $P(z_0) = w_0$, then there are $s - 1$ other points $z_1, z_2, \dots, z_{s-1}$ for which $P(z_l) = w_0$ ($l = 1, 2, \dots, s - 1$). All the points $z_0, \dots, z_{s-1}$ are lying on $L(R)$ and the polygon, having the points $z_0, \dots, z_{s-1}$ as its vertices, is "nearly" regular. Now suppose that $f(P(z))$ is periodic with period $\tau \neq 0$. Then we have for each integral value of k and each $l = 0, 1, \dots, s - 1$

$$|f(P(z_l + k\tau))| = M.$$

But if R is sufficiently large, at least one of the points $z_l + k\tau$ ($l = 0, 1, \dots, s - 1$; $k = \pm 1, \pm 2, \dots$) has to lie inside the curve $L(R)$, and this is in contradiction with the maximum—modulus theorem. This contradiction proves that $f(P(z))$ can not be periodic.

Let us mention that no contradiction arises for $s = 2$, because in this case the two points z_0 and z_1 in which $|f(P(z))|$ takes on its maximum on $L(R)$ are nearly opposite, and τ may be such that the points $z_i \pm \tau k$ ($i = 0, 1$; $k = 1, 2, \dots$) are all lying outside the curve $L(R)$. (This happens if the vector connecting the points 0 and τ is nearly parallel to the tangent of the curve $L(R)$ in the points z_0 and z_1 .)

Let us pass now to the details of the proof.

For the proof of Theorem 1 we shall need some elementary facts about polynomials, which we shall state in the form of two lemmas.

These lemmas are of course well known, but we did not find them stated exactly in the form in which we need them, and therefore for the readers convenience we give them here with proof.

Lemma 1. *Let*

$$(1) \quad P(z) = z^s + c_1 z^{s-1} + \dots + c_s$$

be an arbitrary polynomial of degree $s \geq 3$ with the leading coefficient equal to 1. Let $L(R)$ denote the set of those points z for which $|P(z)| = R > 0$; then

$L(R)$ is for sufficiently large R a Jordan curve which intersects each line $\arg z = \delta$ in a single point, and if $r = r(\delta, R)$ is the equation of the line $L(R)$ in polar coordinates, one has, putting $|c_1| = \rho$, $\arg c_1 = \psi$

$$(2) \quad r(\delta, R) = R^{1/s} - \frac{\rho}{s} \cos(\psi - \delta) + O\left(\frac{1}{R^{1/s}}\right).$$

Thus there exists an R_1 such that for $R \geq R_1$ the curve $L(R)$ is contained between the circles with radii $R^{1/s} \pm \frac{2\rho}{s}$ around $z = 0$.

Proof of Lemma 1. Clearly if $|P(z)| = R$, one has $|z| = O(R^{1/s})$ and thus

$$(3) \quad \left| P(z) - \left(z + \frac{c_1}{s} \right)^s \right| = O(R^{-s-2/s}).$$

(2) follows from (3) immediately.

Lemma 2. Let $z_0(w), \dots, z_{s-1}(w)$ denote the values of z for which $P(z) = w$. Then if $|w| \geq R_2$ where R_2 is a constant depending on the coefficients of $P(z)$ only, the numbers $z_0(w), \dots, z_{s-1}(w)$ are different and can be labelled so that the inequalities

$$(4) \quad \left| \arg z_l(w) - \frac{2\pi l}{s} - \frac{1}{s} \arg w \right| < \frac{B}{\sqrt[s]{|w|}} \quad (l = 0, 1, \dots, s-1)$$

hold, where B is any constant such that $B > |c_1|$.

Proof of Lemma 2. If $P(z) = w$, we have

$$(5) \quad \log w = s \log z + \log \left(1 + \frac{c_1}{z} + \dots + \frac{c_s}{z^s} \right)$$

and thus if $|w| \geq R_1$, we have by Lemma 1

$$(6) \quad |\log w - s \log z| \leq \frac{B}{\sqrt[s]{|w|}}$$

where B is any positive constant exceeding $|c_1|$. Thus we have for some integer l

$$(7) \quad |\arg w + 2\pi l - s \arg z| \leq \frac{B}{\sqrt[s]{|w|}},$$

provided that $|w| \geq R_1$. Now one can easily prove by Rouché's theorem that, if $|w| \geq R_2$, for each l ($l = 0, 1, \dots, s-1$) there is exactly one value of z in the circle

$$(8) \quad |z - \sqrt[s]{|w|} e^{2\pi i l / s}| < \frac{B}{s}$$

for which $P(z) = w$, and thus exactly one value of z for which $P(z) = w$ and (7) holds, and therefore by a convenient labelling of the values $z_0(w), \dots, z_{s-1}(w)$ (if we choose the values of $\arg z$ and $\arg w$ conveniently) we have

$$(9) \quad \left| \arg z_l(w) - \frac{1}{s} \arg w - \frac{2\pi l}{s} \right| < \frac{B}{\sqrt[s]{|w|}}$$

for $l = 0, 1, \dots, s-1$.

Thus Lemma 2 is proved.

Now we are in the position to prove Theorem 1.

Let R be a large positive number, $R \geq \max(R_1, R_2)$. Let us consider the maximum M of $|f(P(z))|$ on the curve $L(R)$. Let us suppose that $|f(P(z))|$ takes on its maximal value on $L(R)$ in a point z_0 , and put $P(z_0) = w_0$. Then we have $|w_0| = R$, and there are exactly $s-1$ other values $z_1, \dots, z_{s-1}$ on $L(R)$ such that $P(z_l) = w_0$ ($l = 1, \dots, s-1$) and by appropriate labelling we have

$$(10) \quad \left| \arg z_l - \frac{1}{s} \arg w_0 - \frac{2\pi l}{s} \right| \leq \frac{B}{\sqrt[s]{R}} \quad (l = 0, \dots, s-1).$$

Now let us suppose that $f(P(z))$ is periodic with period $\tau \neq 0$. Evidently we may suppose that $\tau = 1$.

Clearly there is a value of l for which

$$(11) \quad \left| \frac{1}{s} \arg w_0 + \frac{2\pi l}{s} \right| \leq \frac{\pi}{s}.$$

It follows that

$$(12) \quad |\arg z_l| \leq \frac{\pi}{s} + \frac{B}{\sqrt[s]{R}}.$$

Thus, putting $\phi = \arg z_l$, we have for $R \geq R_3$

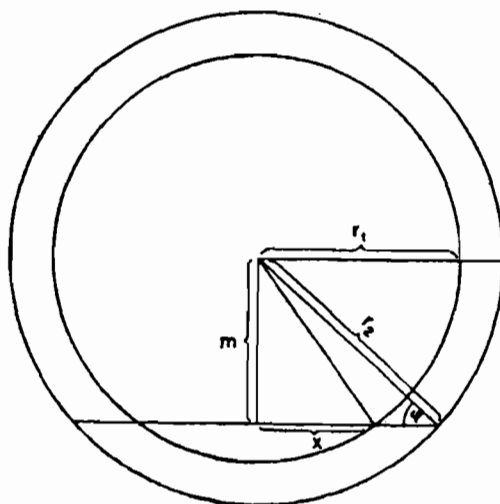
$$(13) \quad |\sin \phi| \leq 0,9.$$

Now let L denote the line through the point z_l , parallel to the real axis. Then, as shown by Fig. 1, the length of the segment of the line L lying inside the curve $L(R)$ exceeds for $R > R_4$

$$(14) \quad 2 \sqrt{\left(R^{1/s} - \frac{2|c_1|}{s} \right)^2 - 0,81 \left(R^{1/s} + \frac{2|c_1|}{s} \right)^2}$$

and thus tends to $+\infty$ for $R \rightarrow \infty$. As all points $z_l - k$ ($k = 0, 1, \dots$) are on the line L and the distance between two consecutive such points is 1, it follows that there is for $R \geq R_5$ at least one point $z_l - k$ which lies inside the curve $L(R)$. But by supposition

$$(15) \quad |f(P(z_l - k))| = |f(P(z_0))| = M$$



$$x = \sqrt{r_1^2 - m^2} = \sqrt{r_1^2 - r_2^2 \sin^2 \phi}$$

Figure 1.

and thus $|f(P(z))|$ would take on its maximum on the curve $L(R)$ also in an interior point. But this contradicts the maximum modulus theorem. This proves Theorem 1.

Let us pass now to the proof of

Theorem 2. *If $P(z)$ is an arbitrary not constant polynomial and $g(z)$ an entire function which is not periodic, then $P(g(z))$ can not be periodic either.*

Proof of Theorem 2. We may suppose that $P(z)$ is a polynomial of degree $s \geq 2$. Let us suppose that $P(g(z))$ is periodic with period $\tau \neq 0$.

Let us choose a large value of R such that if $|w| \geq R$, then $P(z)$ takes on the value w in s distinct points.

Clearly we can find a circle K such that for each z lying in K we have $|P(g(z))| > R$. Now let us choose any z in K . Clearly there are besides $g(z)$ $s-1$ other different complex numbers $\zeta_1(z), \dots, \zeta_{s-1}(z)$ such that $P(\zeta_l(z)) = P(g(z))$ ($l = 1, \dots, s-1$) and if $P(\zeta) = P(g(z))$, then ζ is equal to one of the numbers $g(z), \zeta_1(z), \dots, \zeta_{s-1}(z)$.

As by supposition $P(g(z + k\tau)) = P(g(z))$ for $k = 1, 2, \dots$, there exists a pair k and l of integers $0 \leq k < l \leq s$ such that

$$(16) \quad g(z + k\tau) = g(z + l\tau).$$

As to any z in K there corresponds such a pair (k, l) with $0 \leq k < l \leq s$ and the number of such pairs is finite, there exists at least one such pair such that (16) holds for an infinity of points z in K . Thus we can find a convergent sequence z_n ($n = 1, 2, \dots$) such that $g(z_n + k\tau) = g(z_n + l\tau)$ for $n = 1, 2, \dots$. It follows that $g(z + k\tau)$ is identical with $g(z + l\tau)$ for each complex value of z ; this however means that $g(z)$ is periodic with period $(k-l)\tau$, which contradicts our assumption that $g(z)$ is not periodic. This contradiction proves Theorem 2.

REFERENCE

1. Catherine Rényi, On periodic entire functions, *Acta Mathematica Acad. Sci. Hung.* **8** (1957) 227-233.

NOTE

As a special case of the general problem mentioned in the paper and a generalization of Theorem 1, they asked whether Theorem 1 holds for any transcendental function $P(z)$ of order less than 1. This has been proved in a special case by I. N. Baker, using a different approach and the full conjecture, by refining the method of the present paper, by G. Halász (*Per. Math. Hung.*, **2** (1-4), (1972), 73-83). Theorem 2 has been generalized independently by I. N. Baker and F. Gross for transcendental $g(z)$ of order less than $1/2$. (See the paper by G. Halász for references.) (G. H.)

On certain representations of real numbers and on sequences of equivalent events

By ALFRED RÉNYI in Budapest

Dedicated to Professor L. Kalmár at the occasion of his 60th birthday

Introduction

In § 1 of this paper we shall deal with certain representations of real numbers. Let a_n ($n=0, 1, \dots$) be an absolutely monotonic sequence of numbers, i. e. such that

$$(1) \quad \Delta^k a_n > 0 \quad (k=0, 1, \dots; n \geq k),$$

where $\Delta^0 a_n = a_n$, $\Delta^1 a_n = \Delta a_n = a_{n-1} - a_n$ ($n \geq 1$), and

$$\Delta^k a_n = \Delta(\Delta^{k-1} a_n) \quad (k \geq 1, n \geq k).$$

Let us also suppose that the sequence is *normed*, i. e.

$$(2) \quad a_0 = 1,$$

and *regular*, i. e.

$$(3) \quad a_n \rightarrow 0 \quad \text{and} \quad \Delta^n a_n \rightarrow 0 \quad (n \rightarrow \infty).$$

Then every real $x \in (0, 1]$ admits a uniquely determined representation of the form

$$(4) \quad x = \sum_{k=0}^{\infty} \Delta^k a_{n_k}$$

where the sequence of integers $1 \leq n_0 < n_1 < n_2 < \dots$ depends on x .

This representation can also be written in the form

$$(5) \quad x = \sum_{n=1}^{\infty} \varepsilon_n \Delta^{\varepsilon_1 + \dots + \varepsilon_{n-1}} a_n$$

where $\varepsilon_n = \varepsilon_n(x)$ equals 0 or 1; clearly $\varepsilon_n = 1$ if the number n occurs in the sequence n_k , and $\varepsilon_n = 0$ if not.

In § 2 we deal with the probability distribution of $n_k = n_k(x)$ provided that x is chosen at random with uniform distribution in $(0, 1]$. We shall show that the sequence of random variables n_k is then a Markov chain. In § 3 we deal with the joint probability distribution of the random variables ε_n ($n=1, 2, \dots$) defined above. We prove that if A_n denotes the random event that $\varepsilon_n(x) = 1$ then the events A_n

($n=1, 2, \dots$) form a sequence of *equivalent* (symmetrically dependent) events. such that

$$(6) \quad P(A_{m_1} A_{m_2} \dots A_{m_k}) = \Delta^k a_k$$

for $1 \leq m_1 < m_2 < \dots < m_k$. (Here and in what follows $P(A)$ stands for the probability of the event A .)

In § 4 we show that the strong law of large numbers for equivalent events implies that for almost all x the limit

$$(7) \quad \lim_{k \rightarrow \infty} \frac{k}{n_k(x)}$$

exists. (Previously in § 2 we obtain the weaker result that the distribution of k/n_k tends to a limit distribution.) On the other hand the above mentioned connection between equivalent events and the representation (4) or (5) leads to an effective construction of any sequence of equivalent events. A consequence of this is discussed in § 5. In § 6 we construct the corresponding measure preserving transformation to each sequence a_n , while in § 7 we discuss an example.

§ 1. Representation of real numbers by series of successive differences

We start with the following

Theorem 1. *Let a_n ($n=0, 1, \dots$) be a normed, regular, absolutely monotonic sequence of real numbers. Then any real number $x \in (0, 1]$ can be represented in the form*

$$(1.1) \quad x = \sum_{k=0}^{\infty} \Delta^k a_{n_k}$$

where the increasing sequence of natural numbers n_k is uniquely determined by x .

Proof. Let n_0 be the first natural number such that

$$(1.2) \quad a_{n_0} < x;$$

such a number exists because $a_0 = 1$ and $a_n \rightarrow 0$. Let n_1 be the first natural number such that

$$(1.3) \quad a_{n_0} + \Delta a_{n_1} < x;$$

such a number n_1 exists because $\Delta a_n \rightarrow 0$. Moreover, by the definition of n_0 we have $a_{n_0} < x \leq a_{n_0-1}$, i. e. $x - a_{n_0} \leq \Delta a_{n_0}$, hence it follows $n_1 > n_0$. Similarly if $n_0, n_1, \dots, n_r$ are already determined so that

$$(1.4) \quad \sum_{k=0}^r \Delta^k a_{n_k} < x \leq \sum_{k=0}^{r-1} \Delta^k a_{n_k} + \Delta^r a_{n_{r-1}},$$

let n_{r+1} be the least natural number such that

$$(1.5) \quad \sum_{k=0}^{r+1} \Delta^k a_{n_k} < x.$$

It follows from (1.4) that

$$(1.6) \quad 0 < x - \sum_{k=0}^r \Delta^k a_{n_k} \leq \Delta^{r+1} a_{n_r}$$

which implies — as by supposition $\Delta^{r+1} a_n$ is decreasing in n — that $n_{r+1} > n_r$.

Thus $n_{r+1} > r+1$. Therefore — using again the monotonicity of $\Delta^{r+1} a_n$ — it follows from (1.6) that

$$(1.7) \quad 0 < x - \sum_{k=0}^r \Delta^k a_{n_k} < \Delta^{r+1} a_{r+1}.$$

In view of the condition $\Delta^n a_n \rightarrow 0$ it follows that if the numbers n_k are determined by the algorithm described above, then (1.1) holds. This proves Theorem 1.

Let us note that according to a well-known theorem of F. HAUSDORFF [1] every normed absolutely monotonic sequence can be represented in the form

$$(1.8) \quad a_n = \int_0^1 t^n dF(t)$$

where $F(t)$ is non-decreasing on the closed interval $[0, 1]$, is continuous from the left in the interior, and such that $F(0)=0$ and $F(1)=1$. Evidently,

$$\lim_{n \rightarrow \infty} a_n = F(1) - F(1-0).$$

thus condition $\lim a_n = 0$ implies that $F(t)$ is continuous at $x=1$. We have further

$$(1.9) \quad \Delta^k a_n = \int_0^1 (1-t)^k t^{n-k} dF(t)$$

for $k=0, 1, \dots$ and $n \geq k$; thus in particular

$$(1.10) \quad \Delta^k a_k = \int_0^1 (1-t)^k dF(t).$$

Hence

$$\lim_{k \rightarrow \infty} \Delta^k a_k = F(+0).$$

Thus the condition of regularity $\lim \Delta^n a_n = 0$ implies that $F(t)$ is continuous at $t=0$. Thus every normed, regular, absolutely monotonic sequence a_n can be represented in the form (1.8) where $F(t)$ is the distribution function of a probability distribution in the open interval $(0, 1)$.

In view of formula (1.9) the representation (1.1) can be written in the form

$$(1.11) \quad x = \int_0^1 \left(\sum_{k=0}^{\infty} (1-t)^k t^{n_k-k} \right) dF(t).$$

Thus it follows that for every $x \in (0, 1]$ there is exactly one function $g(t)$ of the form

$$g(t) = \sum_{k=0}^{\infty} (1-t)^k t^{n_k-k}$$

with $1 \leq n_0 < n_1 < n_2 < \dots$, such that

$$x = \int_0^1 g(t) dF(t).$$

§ 2. Statistical theory of the difference-series representation of real numbers

Let x be a random variable, uniformly distributed in the interval $(0, 1)$. Let us consider the representation of x in the form

$$(2.1) \quad x = \sum_{k=0}^{\infty} \Delta^k a_{n_k}$$

where a_n is a given normed, regular, absolutely monotonic sequence. According to Theorem 1 the natural numbers $n_k = n_k(x)$ are uniquely determined by x ; thus they are well defined random variables. We shall study now the probability laws governing the behaviour of these random variables. It is easy to see that if $n_1, \dots, n_k$ are fixed, then x belongs to an interval of length $\Delta^{k+1} a_{n_k}$. It follows that denoting by $P(A|B)$ the conditional probability of the event A under condition B , we have

$$(2.2a) \quad P(n_k = n | n_0 = m_0, n_1 = m_1, \dots, n_{k-1} = m_{k-1}) = \frac{\Delta^{k+1} a_n}{\Delta^k a_{m_{k-1}}}$$

provided that $1 \leq m_0 < m_1 < \dots < m_{k-1} < n$. Thus the conditional distribution of n_k by given $n_0, \dots, n_{k-1}$ depends on n_{k-1} only, that is the sequence of random variables n_k ($k=0, 1, \dots$) is a Markov chain with the transition probabilities

$$(2.2b) \quad P(n_k = n | n_{k-1} = m) = \frac{\Delta^{k+1} a_n}{\Delta^k a_m}.$$

As the probability on the right-hand side of (2.2b) depends in general on k too, the Markov chain n_k is in general inhomogeneous. It is easy to see that the Markov chain is homogeneous if and only if $a_n = (1-p)^n$ ($n=0, 1, \dots$) where $0 < p < 1$. In this particular case

$$(2.3) \quad P(n_k = n | n_{k-1} = m) = p(1-p)^{n-m-1}.$$

This particular case corresponds to the representation of the real number x in the form

$$(2.4) \quad x = \sum_{k=0}^{\infty} p^k (1-p)^{n_k-k}.$$

In this case if A_n denotes the event that n is contained in the sequence n_k then the

events A_n ($n=1, 2, \dots$) are independent and each has the probability $P(A_n)=p$. Especially if $p=\frac{1}{2}$ the representation (2. 4) reduces to

$$(2. 5) \quad x = \sum_{k=0}^{\infty} \frac{1}{2^{n_k}} \quad \text{where} \quad 1 \leq n_0 < n_1 < \dots,$$

by other words to the representation of x in the binary number system.

Let us return to the random variables n_k in the general case. The unconditional distribution of n_k can be determined as follows: As mentioned above if $n_0, n_1, \dots, n_k$ are fixed, then x belongs to an interval of length $\Delta^{k+1}a_{n_k}$. Now if only n_k is fixed, $n_k=n$, then the values of $n_0, n_1, \dots, n_{k-1}$ can be chosen in $\binom{n-1}{k}$ different ways; thus we have

$$(2. 6) \quad P(n_k = n) = \binom{n-1}{k} \Delta^{k+1} a_n.$$

Especially in the case when $a_n = (1-p)^n$, we have

$$(2. 7) \quad P(n_k = n) = \binom{n-1}{k} p^{k+1} (1-p)^{n-k-1}$$

i. e. $n_k - k - 1$ has a negative binomial distribution of order $k+1$.

In the general case it follows from (2. 6) and (1. 9) that

$$(2. 8) \quad P(n_k = n) = \binom{n-1}{k} \int_0^1 (1-t)^{k+1} t^{n-k-1} dF(t)$$

for $n \geq k+1$.

The distribution (2. 8) may be called a *mixed negative binomial distribution of order $k+1$* . The characteristic function of $\frac{n_k}{k+1}$ is

$$(2. 9) \quad M\left(e^{\frac{iun_k}{k+1}}\right) = e^{iu} \int_0^1 \left(\frac{1-t}{1-te^{\frac{i u}{k+1}}}\right)^{k+1} dF(t).$$

(Here and in what follows M stands for "expectation".

We obtain by passing to the limit

$$(2. 10) \quad \lim_{k \rightarrow \infty} M\left(e^{\frac{iun_k}{k+1}}\right) = \int_0^1 e^{\frac{i u}{1-t}} dF(t).$$

It follows that the probability distribution of $\frac{k+1}{n_k}$ tends to the distribution having the distribution function $1 - F(1-z)$

$$(2. 11) \quad \lim_{k \rightarrow \infty} P\left(\frac{k}{n_k} \leq z\right) = 1 - F(1-z).$$

In the special case $a_n = (1-p)^n$ we have

$$F(t) = \begin{cases} 0 & \text{if } t \leq 1-p \\ 1 & \text{if } t > 1-p, \end{cases}$$

thus (2.11) implies that in this case k/n_k tends in probability to p . This is of course well known, because

$$(2.12) \quad \frac{k}{n_k} = \frac{\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_{n_k}}{n_k}$$

and the (weak) law of large numbers applies to the independent random variables ε_n , each having the expectation p .

We shall show in the next paragraph that much more is true than (2.11): not only does the distribution of k/n_k tend for $k \rightarrow \infty$ to the limit distribution $1 - F(1-z)$, but the random variables k/n_k themselves tend for $k \rightarrow \infty$ with probability 1 to a random variable z having the distribution function $1 - F(1-z)$.

Using the formula (2.8) we can of course compute all the moments of n_k . Especially we have

$$(2.13) \quad M(n_k) = (k+1) \int_0^1 \frac{dF(t)}{1-t}.$$

Thus the expectation of $\frac{n_k}{k+1}$ does not depend on k ; it is finite if and only if the integral on the right of (2.13) is convergent, otherwise it is equal to $+\infty$.

§ 3. Connection with the theory of equivalent events

Let A_n denote the event that the natural number n is contained in the sequence $n_k(x)$ where x is a random variable, uniformly distributed in the interval $(0, 1)$. We have evidently

$$(3.1) \quad P(A_n) = \sum_{k=0}^{n-1} P(n_k = n).$$

It follows from (2.8) that

$$(3.2) \quad P(A_n) = \int_0^1 \left(\sum_{k=0}^{n-1} \binom{n-1}{k} (1-t)^{k+1} t^{n-k-1} \right) dF(t) = \int_0^1 (1-t) dF(t)$$

for $n=1, 2, \dots$. Before proceeding further we have to compute the r -step transition probabilities of the Markov-chain n_k . Clearly we have for $r \geq 2$ and $n \geq m+r$

$$(3.3) \quad P(n_{k+r} = n | n_k = m) = \frac{\Delta^{k+r+1} a_n}{\Delta^{k+1} a_m} \sum_{m < m_1 < \dots < m_{r-1} < n} 1,$$

thus

$$(3.4) \quad P(n_{k+r} = n | n_k = m) = \binom{n-m-1}{r-1} \frac{\Delta^{k+r+1} a_n}{\Delta^{k+1} a_m}.$$

It follows that for $m < n$

$$(3.5) \quad P(n_{k+r} = n, n_k = m) = \binom{n-m-1}{r-1} \binom{m-1}{k} \Delta^{k+r+1} a_n.$$

Thus we have

$$(3.6) \quad P(A_m A_n) = \sum_{k=0}^{m-1} \sum_{l=k+1}^{k+n-m} \binom{n-m-1}{l-k-1} \binom{m-1}{k} \Delta^{l+1} a_n.$$

Taking (1.9) into account we obtain for $1 \leq m < n$

$$(3.7) \quad P(A_m A_n) = \int_0^1 (1-t)^2 dF(t).$$

We shall show now that for any $r \geq 1$ and for $1 \leq m_1 < m_2 < \dots < m_r$ we have

$$(3.8) \quad P(A_{m_1} A_{m_2} \dots A_{m_r}) = \int_0^1 (1-t)^r dF(t).$$

The proof is essentially the same as for $r=2$. We obtain in the same way as (3.5) was shown — using that n_k is a Markov chain — that for $k_1 < k_2 < \dots < k_r$, $m_1 < m_2 < \dots < m_r$

$$(3.9) \quad P(n_{k_1} = m_1, \dots, n_{k_r} = m_r) = \binom{m_1-1}{k_1} \prod_{j=1}^{r-1} \binom{m_{j+1}-m_j-1}{k_{j+1}-k_j-1} \cdot \Delta^{k_r+1} a_{m_r}.$$

Of course the probability (3.9) is positive only if $m_1 \geq k_1 + 1$ and $m_{j+1} - m_j \geq k_{j+1} - k_j$ ($j = 1, 2, \dots, r-1$). From (3.9) one obtains (3.8) by means of the identity

$$(3.10) \quad P(A_{m_1} A_{m_2} \dots A_{m_r}) = \sum_{k_1 < k_2 < \dots < k_r} P(n_{k_1} = m_1, \dots, n_{k_r} = m_r).$$

As clearly

$$(3.11) \quad \int_0^1 (1-t)^r dF(t) = \Delta^r a_r,$$

we have proved the following

Theorem 2. Let A_n denote the event that the natural number n is contained in the sequence $\{n_k(x)\}$ defined by Theorem 1, where x is a random variable uniformly distributed in the interval $(0, 1)$. Then the events A_n ($n = 1, 2, \dots$) are equivalent, and one has for $1 \leq m_1 < m_2 < \dots < m_r$ ($r = 1, 2, \dots$)

$$(3.12) \quad P(A_{m_1} A_{m_2} \dots A_{m_r}) = \Delta^r a_r.$$

Remark. Note that the sequence $W_r = \Delta^r a_r$ is absolutely monotonic too, because setting

$$(3.13) \quad G(t) = 1 - F(1-t+0)$$

we have

$$(3.14) \quad w_r = \int_0^1 t^r dG(t).$$

It is easy to see also that

$$(3.15) \quad \Delta^{h_{m_r}} = \Delta^{r-h} a_r.$$

Conversely let us be given a sequence of equivalent events B_n ($n=1, 2, \dots$) in a probability space $[\Omega, \mathcal{A}, P]$ where Ω is a non empty set, the generic element of which will be denoted by ω , $\mathcal{A}$ is a σ -algebra of subsets of Ω and P a probability measure on $\mathcal{A}$. It is known (see [2], [3]) that there exists an $\mathcal{A}$ -measurable function $\beta = \beta(\omega)$ on Ω — called the density of the sequence of events B_n — such that $0 \leq \beta \leq 1$ and for $r=1, 2, \dots$ and $m_1 < m_2 < \dots < m_r$ one has

$$(3.16) \quad P(B_{m_1} B_{m_2} \dots B_{m_r}) = \int_{\Omega} \beta^r dP.$$

Let us consider first the case when $\beta = 1$ on a set B of positive probability. Let β_n denote the indicator of the set B_n . It was shown in [3] that if $n_1 < n_2 < \dots < n_k$ $m_1 < m_2 < \dots < m$ and $n_i \neq m_j$, then

$$(3.17) \quad P(B_{n_1} B_{n_2} \dots B_{n_k} B_{m_1} B_{m_2} \dots B_{m_l}) = \int_{\Omega} \beta^k \beta_{n_1} \beta_{n_2} \dots \beta_{m_l} dP.$$

It follows that

$$(3.18) \quad P\left(\prod_{n=r}^{\infty} B_n\right) = \int_B \prod_{r \leq j < s} \beta_j dP.$$

As (3.18) holds for $s=r$ too (the empty product is equal to 1), we have

$$P\left(\prod_{n=r}^{\infty} B_n\right) = P(B).$$

Thus we obtain, putting $\prod_{n=1}^{\infty} B_n = B^*$.

$$P(B) = P(B^*) = P(BB^*).$$

This implies that the sets B and B^* are identical up to a set of P -measure 0. Let us denote now by $\bar{B}$ the complementary event of B , i. e. $\bar{B} = \Omega - B$. It follows that the events $A_n = \bar{B} B_n$ also are equivalent, and have the density α defined as follows:

$$\alpha(\omega) = \begin{cases} \beta(\omega) & \text{if } \omega \in \bar{B}, \\ 0 & \text{if } \omega \in B. \end{cases}$$

As a matter of fact we have

$$P(A_{m_1} A_{m_2} \dots A_{m_r}) = P(B_{m_1} B_{m_2} \dots B_{m_r}) - P(B) = \int_{\Omega} \alpha^r dP.$$

As $P(\alpha=1)=0$, we have shown that without restriction of generality one can suppose that $P(\beta=1)=0$.

Similarly one can suppose without restricting the generality that $P(\beta=0)=0$. As a matter of fact if C denotes the set on which $\beta=0$ and $0 < P(C) < 1$ then the set C is disjoint to all the sets B_n (up to a set of probability 0) and thus instead of the probability space $[\Omega, \mathcal{A}, P]$ we may consider the space $[\Omega, \mathcal{A}, P^*]$ where

$P^*(A) = \frac{P(A\bar{C})}{P(\bar{C})}$ and the events B_n will be equivalent with respect to this probability space too, with the same density β . Thus the case of an arbitrary sequence of equivalent events can be reduced to a sequence of equivalent events the density β of which is such that $P(\beta=0) = P(\beta=1) = 0$. Let us call such a sequence a *regular* sequence of equivalent events. If A_n is a regular sequence of equivalent events with density β and if we put

$$w_k = P(A_{n_1} A_{n_2} \dots A_{n_k}) = \int_{\Omega} \beta^k dP$$

then clearly we have

$$\lim_{k \rightarrow \infty} w_k = 0 \quad \text{and} \quad \lim_{k \rightarrow \infty} \Delta^k w_k = 0.$$

Putting $a_k = \Delta^k w_k$, clearly $w_k = \Delta^k a_k$ and the sequence a_k is a normed regular absolutely monotonic sequence. Thus the events $\{A_n\}$ can be realized as the events connected with the representation of the random real number x uniformly distributed in $(0, 1)$ in the form (1. 1), so that the event A_n is identified with the event that n is contained in the sequence n_k .

§ 4. The strong law of large numbers for the Markov chain n_k

We first give — to make this paper self-contained — a short proof of the following known result:²⁾

Theorem 3. *Let A_n be an arbitrary sequence of equivalent events; let α_n denote the indicator of A_n and α the density of the sequence A_n . Then we have*

$$(4. 1) \quad P\left(\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \alpha_k = \alpha\right) = 1.$$

Proof. Let us consider the random variables

$$(4. 2) \quad \delta_k = \alpha_k - \alpha$$

and let us put for $k_1 < k_2 < \dots < k_r$, $r = 1, 2, \dots$

$$(4. 3) \quad P(A_{k_1} A_{k_2} \dots A_{k_r}) = w_r.$$

It follows from (3. 17) that

$$(4. 4) \quad M(\delta_{k_1} \delta_{k_2} \delta_{k_3} \delta_{k_4}) = \begin{cases} A & \text{if } k_1 = k_2 = k_3 = k_4, \\ B & \text{if } k_1 = k_2 \text{ and } k_3 = k_4 \neq k_1, \\ & \text{or if } k_1 = k_3 \text{ and } k_2 = k_4 \neq k_1, \\ & \text{or if } k_1 = k_4 \text{ and } k_2 = k_3 \neq k_1, \\ 0 & \text{otherwise,} \end{cases}$$

²⁾ Theorem 3 can also be deduced from BIRKHOFF's ergodic theorem.

where

$$(4.5) \quad A = w_1 - 4w_2 + 6w_3 - 3w_4$$

and

$$(4.6) \quad B = w_2 - 2w_3 + w_4.$$

This implies

$$(4.7) \quad M\left(\left(\frac{\delta_1 + \dots + \delta_n}{n}\right)^4\right) = O\left(\frac{1}{n^2}\right).$$

Thus the series

$$(4.8) \quad \sum_{n=1}^{\infty} \left(\frac{\delta_1 + \dots + \delta_n}{n}\right)^4$$

is convergent with probability 1 and therefore (4.1) holds.

In view of (2.11) and the results of § 3 this implies that the following theorem holds:

Theorem 4. *If the sequence $n_k(x)$ is defined according to Theorem 1 then the limit*

$$(4.9) \quad \lim_{k \rightarrow \infty} \frac{k}{n_k(x)} = \kappa(x)$$

exists for almost all x in $(0, 1)$; denoting by $\mu(A)$ the Lebesgue measure of the set A one has

$$(4.10) \quad \mu(\kappa(x) \leq y) = 1 - F(1 - y) \quad \text{for } 0 \leq y \leq 1.$$

§ 5. Consequences for equivalent events

In the preceding § we applied the theory of equivalent sequences of events to prove the existence almost everywhere of the limit $\lim_{k \rightarrow \infty} \frac{k}{n_k(x)}$. Conversely, our results lead to the proof of a property of equivalent events which seems not to be noticed up to now. This is expressed by

Theorem 5. *Let A_n ($n = 1, 2, \dots$) be a regular sequence of equivalent events. Let us set*

$$P(A_{n_1} A_{n_2} \dots A_{n_k}) = w_k \quad (n_1 < n_2 < \dots < n_k; k = 1, 2, \dots).$$

Denote by α_n the indicator of the event A_n and define the random variables v_k as follows: v_k is the least value of n such that $\alpha_1 + \alpha_2 + \dots + \alpha_n = k$. By other words, v_k denotes the index of the k -th event in the sequence of events A_n ($n = 1, 2, \dots$) which takes place. Then the random variables v_k form a Markov chain with the transition probabilities

$$(5.1) \quad P(v_{k+1} = n | v_k = m) = \frac{\Delta^{n-k-1} w_n}{\Delta^{m-k} w_m}.$$

§ 6. The measure preserving transformation corresponding to a series of successive differences

To every representation (7) — i. e. to every normed, regular, absolutely monotonic sequence $\{a_n\}$ — there corresponds a measure preserving transformation T of the interval $(0, 1)$ defined as follows: If

$$(6.1) \quad x = \sum_{k=0}^{\infty} \Delta^k a_{n_k(x)}$$

then

$$(6.2) \quad n_k(Tx) = n_{k+\varepsilon_1(x)}(x) = 1 \quad (k=0, 1, \dots).$$

Clearly $1 \leq n_0(Tx)$, because if $n_0(x) = 1$ then $\varepsilon_1(x) = 1$ and thus $n_0(Tx) = n_1(x) - 1 \geq 1$ and if $n_0(x) \geq 2$ then $n_0(Tx) = n_0(x) - 1 \geq 1$; the inequality $n_{k+1}(Tx) > n_k(Tx)$ is evident. The inverse transformation $T^{-1}y$ can be defined as follows: $T^{-1}y$ is two-valued, namely if

$$(6.3) \quad y = \sum_{k=0}^{\infty} \Delta^k a_{n_k}$$

then $T^{-1}y$ has the two values x_1 and x_2 where

$$(6.4) \quad x_1 = \sum_{k=0}^{\infty} \Delta^k a_{n_k+1}, \quad x_2 = a_1 + \sum_{k=1}^{\infty} \Delta^k a_{n_{k-1}+1}.$$

Clearly if y belongs to the interval I_r defined by fixing the values of $n_0, n_1, \dots, n_r$ in (6.3) ($1 \leq n_0 < n_1 < \dots < n_r$) and having the length $\Delta^{r+1} a_{n_r}$ then x_1 belongs to an interval I'_r of length $\Delta^{r+1} a_{n_r+1}$ and x_2 to an interval I''_r of length $\Delta^{r+2} a_{n_r+1}$. As

$$(6.5) \quad \Delta^{r+1} a_{n_r+1} + \Delta^{r+2} a_{n_r+1} = \Delta^{r+1} a_{n_r}$$

it follows that denoting by $\mu(A)$ the Lebesgue measure of the set A one has

$$(6.6) \quad \mu(T^{-1}I_r) = \mu(I'_r) + \mu(I''_r) = \mu(I_r).$$

It follows from (6.6) that Tx is measure preserving.

The transformation Tx can of course also be defined by

$$(6.7) \quad \varepsilon_k(Tx) = \varepsilon_{k+1}(x) \quad (k=0, 1, \dots).$$

Thus T is equivalent to the shift transformation in the sequence-space $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n, \dots)$.

It is easy to see that the transformation T is ergodic if and only if $a_n = q^n$ with $0 < q < 1$, because it follows from (6.7) and Theorem 4 that

$$(6.8) \quad x(Tx) = x(x)$$

and thus each level set of x is an invariant set of T ; thus T is ergodic if and only if x is constant almost everywhere, i. e. if $a_n = q^n$. Especially in the case $a_n = 2^{-n}$, T is the well known transformation $Tx = (2x)$ where (Z) denotes the fractional part of Z .

§ 7. An example

As an example let us consider the sequence $a_n = \frac{1}{n+1}$ ($n=0, 1, 2, \dots$). Evidently,

$$(7.1) \quad \Delta^k a_n = \frac{1}{(n+1) \binom{n}{k}},$$

hence

$$(7.2) \quad \Delta^n a_n = a_n = \frac{1}{n+1}.$$

Thus a_n is a normed, regular, absolutely monotonic sequence. Theorem 1 asserts for this case that every real number x with $0 < x \leq 1$ has a unique representation of the form

$$(7.3) \quad x = \sum_{k=0}^{\infty} \frac{1}{(n_k+1) \binom{n_k}{k}}$$

where the n_k are integers, $1 \leq n_1 < n_2 < \dots$. The function $F(t)$ figuring in (1.8) is in this example equal to t ($0 \leq t \leq 1$). The transition probabilities (2.2b) are in this example

$$(7.4) \quad P(n_k = n | n_{k-1} = m) = \frac{(m+1) \binom{m}{k}}{(n+1) \binom{n}{k+1}}$$

and the distribution of n_k is given by

$$(7.5) \quad P(n_k = n) = \frac{k+1}{n(n+1)} \quad \text{for } n \geq k+1.$$

Thus the random variables n_k have an infinite expectation. The equivalent events A_n can in this case be interpreted as the events of the following Pólya urn model: Let us consider an urn containing one white and one red ball. Let us draw one of the balls at random (each having the probability $\frac{1}{2}$ to be drawn) and put it back into the urn together with another ball of the same colour, then draw another ball from the urn which now contains 3 balls, each ball having the same probability to be drawn, put it back together with another ball of the same colour and continue this procedure indefinitely. Let A_n denote the event that at the n -th occasion a red ball has been drawn from the urn. Clearly in this interpretation a red ball is drawn the $k+1$ -st time at the n_k -th drawing; the limit x of k/n_k is in this case of course uniformly distributed in the interval $(0, 1)$.

References

- [1] F. HAUSDORFF, Momentprobleme für ein endliches Intervall, *Math. Zeitschrift*, **16** (1923), 220–248.
- [2] A. RÉNYI, On stable sequences of events, *Sankhya* (Ser. A), **25** (1963), 293–302.
- [3] A. RÉNYI–P. RÉVÉSZ, A study of sequences of equivalent events as special stable sequences, *Publ. Math. Debrecen*, **10** (1963), 319–325.

ON THE THEORY OF RANDOM SEARCH

A. RÉNYI

Introduction. The problems of search dealt with in this paper can be described by the following simple model. Let S_n be a *finite* set having $n \geq 2$ distinguishable elements—called points—and suppose that we want to find an unknown point x of the set S_n ; the set S_n itself is supposed to be known to us. Let us suppose further that it is not possible to observe x directly, however we may choose some functions $f_1, f_2, \dots, f_N$ from a given set F of functions defined on S_n , and observe the values $f_1(x), f_2(x), \dots, f_N(x)$ taken on by these functions at the unknown point x . Of course if F would contain a function f which takes on different values at different points, a single observation of this function would be sufficient. We suppose however that all functions f belonging to the class F are such that the number of different values taken on by f is much smaller than n . (We shall be especially interested in the case when each $f \in F$ takes on only the two values 0 and 1 and n is a large number.) In such a case of course it is necessary to observe the value of a large number of functions f at the point x . Each such observation gives us only partial information on x (namely it specifies a subset A of S_n to which x must belong), but after making a fairly large number of such observations the information obtained accumulates and enables us to determine x . We want to find x by a not too large number of observations. We may e.g. suppose that each observation is connected with a certain cost (or that it requires a definite amount of time) and we want to keep the cost (or duration) of the whole procedure of search relatively low. We shall call a method for the successive choice of the functions $f_1, \dots, f_N$, which leads in the end to the determination of the unknown x , a *strategy of search*. Obviously one usually tries to choose a strategy with N (the number of functions to be observed) as small as possible. Of two search procedures the one which has a smaller (average) duration is the better one, however there may be other requirements. For instance a simple strategy which can e.g. be easily programmed on a computer is usually preferable to a complicated strategy. If A and B are two strategies such that A requires (in the average) the observation of a somewhat smaller number of functions than B (i.e. A is “better” than B) but the effective carrying out of A

An elaboration of an address delivered before the Chicago meeting of the Society on April 25, 1964, by invitation of the Committee to Select Hour Speakers for Western Sectional Meetings; received by the editors June 18, 1965.

requires much more work and time, then nevertheless B may be preferable to A from a practical point of view.

A strategy will be called a *pure strategy* if it uniquely specifies the choice of the functions $f_1, f_2, \dots, f_N$ and a *mixed strategy* if the choice of these functions depends to some extent on chance. A pure strategy will be called *predetermined* if the number N and the choice of each of the functions $f_1, \dots, f_N$ is determined in advance, before beginning the observations; it will be called *sequential* if only the choice of f_1 is decided in advance and the choice of f_k ($k \geq 2$) is made only after observing $f_1(x), f_2(x), \dots, f_{k-1}(x)$ and may depend on these observed values; in the case of a sequential (pure) strategy the number of observations N depends usually also on the value of x .

Problems of search occur in practically every field of human activity. Typical examples are: medical diagnosis, chemical analysis, search for a failure in a complicated mechanism, search for a lost or hidden object, search for a mistake in a long series of computations or in a program for a computer, search for some bibliographical data, search for the root of an equation, the maximum of a function, the parameter of a probability distribution, etc.

The theory of search should be considered—according to the author's point of view—as a chapter of information theory; this chapter of information theory is however not very far developed. Many interesting particular problems of random search have been investigated, but a systematic study of such problems has not yet been given.

In §§1 and 2 of the present paper we deal with certain basic notions which are of importance in search theory (separating systems of functions, different notions of homogeneity of such systems) and with certain combinatorial questions connected with these notions. We deal with these questions in somewhat greater detail than needed in what follows, because these combinatorial questions are interesting in themselves too, and in view of other applications, to be given elsewhere. In §3 we prove a few general theorems concerning the duration of search of random search procedures and shall show that in general these random search methods are almost as good as the best pure strategy, being at the same time usually much simpler. In §4 we give a few examples.

1. Separating systems of functions. Clearly in order that there should exist at least one strategy which leads to finding the unknown element x of S_n whatever it may be, it is necessary that the class F of available functions f should be rich enough. Let us introduce the following definition:

(I) Let us say that a system F of functions defined on the set S_n is separating the elements of S_n (or for the sake of brevity: is a separating system) if it has the following property:

To any pair of different elements x_1, x_2 ($x_2 \neq x_1$) of S_n there exists in F a function f such that $f(x_2) \neq f(x_1)$.

Clearly if F is not a separating system, i.e. if there are elements x_1 and $x_2 \neq x_1$ in S_n such that for each $f \in F$, $f(x_2) = f(x_1)$, one never can decide whether the unknown element x of S_n which we want to find, is x_1 or x_2 by observing the values of functions $f \in F$ at the point x . On the other hand if F is a family of functions on S_n separating the elements of S_n , then by observing $f(x)$ for all $f \in F$ x will be uniquely determined; thus there exists at least one successful strategy, namely the trivial one consisting in observing the value of $f(x)$ one by one for all functions $f \in F$.

Let F be a system of functions defined on the set S_n which separates the elements of S_n . We shall call F a *minimal separating system* of functions, if no proper subset of F does separate the elements of S_n .

Another way to characterize separating systems of functions is the following. For each $f \in F$ let us call the set $A \subset S_n$ a level-set of f if A contains all elements x of S_n for which $f(x) = a$, where a is any fixed value. Clearly the system F separates the elements of the set S_n if and only if the least algebra of sets containing all level-sets of all functions $f \in F$ is identical with the algebra of all subsets of S_n .

A third equivalent way of characterizing separating systems of functions is the following. To any set F of functions defined on the set S_n there corresponds a matrix M defined as follows: If the elements of the set S_n are $a_1, a_2, \dots, a_n$ and F consists of the functions $f_1, f_2, \dots, f_m$, the matrix M contains m rows and n columns and the k th entry of the j th row of M is $f_j(a_k)$. Clearly F is separating the elements of S_n if and only if the column-vectors of the matrix M are all different.

We shall prove now the following simple

LEMMA 1. Let F be a minimal separating system of functions separating the elements of the finite set S_n having n elements. If m denotes the number of elements of F we have $m \leq n - 1$.

PROOF. The statement of Lemma 1 can be expressed also in the following way: if F is a system of functions separating the elements of the set S_n , and if the number of functions belonging to F is $\geq n$, one can select from F $n - 1$ functions such that these selected functions separate the elements of S_n . This statement is evidently true for $n = 2$, because clearly there must be in F a function which is not

constant on S_2 , and a single such function clearly separates the two elements of S_2 .

Let us suppose that the statement of Lemma 1 holds for some $n \geq 2$; we shall show that in this case it holds also for $n+1$. Let us denote the $n+1$ elements of the set S_{n+1} by $a_1, a_2, \dots, a_{n+1}$. If the system F separates the elements of the set S_{n+1} , it separates a fortiori the n elements $a_1, \dots, a_n$; thus by supposition we can select from F $n-1$ functions $f_1, f_2, \dots, f_{n-1}$ which separate the elements $a_1, a_2, \dots, a_n$. Now let us consider the vector $(f_1(a_{n+1}), f_2(a_{n+1}), \dots, f_{n-1}(a_{n+1}))$: if this vector is different from each of the n vectors $(f_1(a_j), f_2(a_j), \dots, f_{n-1}(a_j))$ ($1 \leq j \leq n$), then the $n-1$ functions $f_1(x), \dots, f_{n-1}(x)$ separate all elements of the set S_{n+1} ; if not, the vector $(f_1(a_{n+1}), \dots, f_{n-1}(a_{n+1}))$ is identical with one (and only one) of the n different vectors $(f_1(a_j), \dots, f_{n-1}(a_j))$; suppose for instance that $f_i(a_{n+1}) = f_i(a_j)$ for $1 \leq i \leq n-1$. Then there is in F at least one function f such that $f(a_{n+1}) \neq f(a_j)$, because otherwise F would not separate a_{n+1} and a_j . But then the system of functions $f_1, \dots, f_{n-1}, f$ separates the elements of the set S_{n+1} . Thus Lemma 1 is proved by induction.

The following example shows that the statement of Lemma 1 is best possible. Let S_n consist of the elements $0, 1, \dots, n-1$; let F consist of the $n-1$ functions $f_i(x)$ ($0 \leq i \leq n-2$) defined as follows: put

$$f_i(x) = \begin{cases} 1 & \text{if } x = i, \\ 0 & \text{otherwise} \end{cases}$$

for $0 \leq i \leq n-2$. Then F is a minimal separating system for the set S_n .

Let us consider some examples of separating systems. In all the following examples, if not otherwise specified, S_n is the set consisting of the elements $0, 1, \dots, n-1$.

EXAMPLE 1. F is the set of all 2^n functions on S_n taking on only the values 0 and 1.

EXAMPLE 2. F_k is the set of all $\binom{n}{k}$ functions on S_n which take on the value 1 at k points and the value 0 at the remaining $n-k$ points ($1 \leq k \leq n-1$).

The set F is not minimal for $2 \leq k \leq n-2$. In his lectures at the University of Budapest, the author has proposed the question: to determine the least number $N(n, k)$ for which there exists a separating system F of functions on S_n such that each $f \in F$ takes on the value 1 at k points and the value 0 at the remaining $n-k$ points. The answer to this question is easy (and has been obtained independently by B. Bollobás, J. Galambos, Gy. Katona, T. Nemetz and D. Szász) if $n \geq k(k+1)/2 + 1$; in this case one has $N(n, k) = \{2(n-1)/(k+1)\}$ where $\{x\}$ denotes the least integer $\geq x$. On the other hand if n is

even and $k=n/2$ one has clearly $N(n, n/2) = \{\log n\}$. To find an explicit formula for $N(n, k)$ in general seems to be difficult; however Mr. Gy. Katona has obtained rather close lower and upper estimates for $N(n, k)$, which he will publish in a forthcoming paper.

EXAMPLE 3. Suppose $n = 2^r$. Let us represent each integer x ($0 \leq x \leq n-1$) in the binary number system:

$$x = \sum_{k=0}^{r-1} \epsilon_k(x) \cdot 2^k$$

where $\epsilon_k(x) = 0$ or $=1$, and consider the system $F_{[r]}$ of functions $\epsilon_0(x), \dots, \epsilon_{r-1}(x)$. Clearly the values $\epsilon_0(x), \dots, \epsilon_{r-1}(x)$ determine x uniquely; thus $F_{[r]}$ is a (minimal) separating system for the set S_2^r .

EXAMPLE 4. Let the matrix $M_{r,s}$ be defined as follows: $M_{r,s}$ contains r rows and $\binom{r}{s}$ columns, where $0 \leq s \leq r$. Let each column of $M_{r,s}$ contain s ones and $r-s$ zeros, and let all columns of $M_{r,s}$ be different; by other words the columns of $M_{r,s}$ are all possible sequences of r terms consisting of s ones and $r-s$ zeros. Let $f_j(x)$ be equal to the x th element of the j th row of $M_{r,s}$ ($1 \leq j \leq r; 1 \leq x \leq \binom{r}{s}$). Then the functions $f_1, \dots, f_r$ separate the elements of the set $\{1, 2, \dots, \binom{r}{s}\}$. Evidently each row of $M_{r,s}$ contains $\binom{r-1}{s-1}$ ones and $\binom{r-1}{s}$ zeros. Note that if we form from the matrices $M_{r,0}, M_{r,1}, \dots, M_{r,r}$ a single matrix having r rows and 2^r columns by putting the matrices $M_{r,s}$ side by side, we get the matrix of the minimal separating system of Example 3.

Note that the separating system of functions having the matrix $M_{r,s}$ is not minimal if $r \geq 2, s = 0, 1, \dots, r$, however if $1 \leq s \leq r-1$ and we omit any one of the functions from the separating system having the matrix $M_{r,s}$ we obtain a minimal separating system.

Let us introduce in the set S_n a probability measure, by supposing that each element of S_n has the same probability $1/n$. In this case each function $f(x)$ defined on S_n can be considered as a random variable. If the set of values of $f(x)$ taken on S_n is the set $\{y_1, \dots, y_r\}$ and $f(x)$ takes on the value y_j at K_j different points of S_n ($\sum_{j=1}^r K_j = n$) then the probability distribution of $f(x)$ is given by

$$(1.1) \quad P(f(x) = y_j) = \frac{K_j}{n} = P_j$$

and the entropy of f is

$$(1.2) \quad H(f) = \sum_{j=1}^r P_j \log \frac{1}{P_j}$$

(Here and in what follows $\log$ denotes logarithm with base 2.)

Now we prove the following simple

LEMMA 2. *If F is a system of functions separating the elements of the set S_n then*

$$(1.3) \quad \sum_{f \in F} H(f) \geq \log n.$$

PROOF OF LEMMA 2. Let $f_1, f_2, \dots, f_m$ be all the functions belonging to the set F , then the vector $\psi(x) = (f_1(x), \dots, f_m(x))$ takes on different values for different values of $x \in S_n$. Thus $H(\psi) = \log n$. As it is well known that the entropy of the joint distribution of a sequence of random variables can not exceed the sum of the entropies of these random variables, we obtain (1.3) which proves Lemma 2. Note that there is equality in (1.3) if and only if the functions $f_1, \dots, f_m$, considered as random variables, are independent.

If for a separating system F there is equality in (1.3) we call F an *optimal separating system*. Clearly an optimal separating system is always minimal, but not conversely.

The following remark shows the difference between these two notions: if $F = \{f_1, \dots, f_N\}$ is a minimal separating system, then omitting one function—say f_K —from F the remaining system $\{f_1, \dots, f_{K-1}, f_{K+1}, \dots, f_N\}$ is no more separating, i.e. there exist elements x_1 and $x_2 \neq x_1$ of S_n such that $f_j(x_1) = f_j(x_2)$ for $j \neq K$, $1 \leq j \leq N$. By other words, there exists an element x of S_n such that to find x we have to observe all functions f_j belonging to F at the point x , i.e. the process of search is *not always* finished before making N observations. However if F is an optimal system, the process of search is *never* finished before making N observations; as a matter of fact if the random variables $f_1, \dots, f_N$ are independent (and none of them is constant) then by fixing the values of $N-1$ among these functions, the remaining function takes on all its values under this condition too. It should be added that this property is necessary but not sufficient for F being an optimal system. For instance if the functions of the system F are independent random variables with respect to some other probability measure on S_n different from the uniform measure, then F has the mentioned property, without being an optimal system.

The minimal system of Example 3 is optimal, but the minimal system of Example 4 (obtained by omitting any one of the functions of the system corresponding to the matrix $M_{r,s}$) is not optimal if $r \geq 3$, $1 \leq s \leq r-1$.

An optimal separating system F can clearly be characterized by saying that the partial informations obtained from observing different functions f belonging to F never overlap. Thus an optimal separating system corresponds to a most economic strategy. The ratio $\log n / \sum_{f \in F} H(f)$ may be interpreted as the *efficiency* of the separating systems F .

2. Different notions of homogeneity of a separating system of functions. In our investigations we do not suppose the existence of any algebraical, geometrical or topological structure in the set S_n , and we suppose further that we have no prior knowledge on the unknown element x of S_n , i.e. that before we start the search all possibilities $x = a_K$ ($K = 1, 2, \dots, n$) have the same prior probability $1/n$. Accordingly it is natural to restrict ourselves to the case in which the separating system F of available functions f is in some sense symmetrical with respect to the elements a_K of S_n . We shall define different sorts of symmetry of systems of functions. First we adopt the following definition:

(II) *A system F of functions f defined on the set $S_n = \{a_1, a_2, \dots, a_n\}$ is called completely homogeneous, if denoting by π any permutation of the sequence $1, 2, \dots, n$ for any $f \in F$ the function g defined by*

$$g(a_j) = f(a_{\pi(j)})$$

belongs to F too.

Let us consider some examples. The separating systems of Examples 1 and 2 are clearly completely homogeneous; but the systems of Examples 3 and 4 are not completely homogeneous. A system F of functions which is completely homogeneous and contains at least one function which is not constant is obviously a separating system.

Let M denote the matrix corresponding to a separating system F . Clearly F is completely homogeneous if and only if by permuting in any possible way the columns of M we obtain a matrix M' which can be obtained from M also by a suitable permutation of the rows of M . Thus if F is a completely homogeneous system of functions separating the elements of the set S_n and the number of elements of F is m , then necessarily $m \geq n$, because otherwise there would be more permutations of the columns than permutations of the rows of the corresponding matrix M . As by Lemma 1 for a minimal separating system $m \leq n - 1$, it follows that a minimal separating system can never be completely homogeneous.

Let us introduce now the following definition:

(III) *A system of functions F defined on the set $S_n = \{a_1, a_2, \dots, a_n\}$*

is weakly homogeneous of order K ($2 \leq K \leq n$) if it has the following property: Let us choose K different elements $a_{j_1}, a_{j_2}, \dots, a_{j_K}$ of S_n and let R_K denote the number of functions $f \in F$ such that

$$f(a_{j_1}) = f(a_{j_2}) = \dots = f(a_{j_K}).$$

The R_K does not depend on the choice of the elements $a_{j_1}, a_{j_2}, \dots, a_{j_K}$. We shall call the number R_K the *parameter* of F .

If a system F of functions is weakly homogeneous of order 2 and $R_2 < R_1$ where R_1 is the number of elements of the set F (that is always true except the trivial case when F consists of constant functions only) then of course F is a separating system.

We shall need also another property of homogeneity which is stronger than homogeneity of order K ; we call this strong homogeneity of order K and define it as follows:

(IV) Let F be a set of functions f defined on the set $S_n = \{a_1, a_2, \dots, a_n\}$. Let us suppose that the values of every $f \in F$ belong to a set $Y = \{y_1, \dots, y_r\}$. We call the set F strongly homogeneous of order K if choosing any K different points $a_{j_1}, a_{j_2}, \dots, a_{j_K}$ of S_n and any sequence of elements $y_{1_i}, \dots, y_{K_i}$ of Y (the y_{1_i} ($i=1, 2, \dots, K$) are not necessarily different) the number $R_K(y_{1_i}, \dots, y_{K_i})$ of those functions $f \in F$ for which

$$f(a_{j_i}) = y_{1_i} \quad (i = 1, 2, \dots, K)$$

does not depend on the choice of the points $a_{j_1}, \dots, a_{j_K}$ but it may depend on the values $y_{1_i}, \dots, y_{K_i}$.

Evidently a strongly homogeneous set of order K is homogeneous of order K because we have

$$R_K = \sum_{y \in Y} R_K(y, y, \dots, y).$$

It also is easy to see that if F is strongly homogeneous of order K it is strongly homogeneous of every order $K' < K$. For the weak homogeneity a similar statement does not hold. As a matter of fact every set F of functions f defined on S_n is homogeneous of order n but not necessarily of order $K < n$. It can easily be shown that a completely homogeneous set F is strongly homogeneous of every order K . If each function f in F takes on only the values 0 and 1 and it takes on the value 1 at exactly k points, we can characterize F also as follows: to each function $f \in F$ there corresponds the K -tuple of those numbers j ($1 \leq j \leq n$) for which $f(a_j) = 1$. Thus F can be represented by a sequence of k -tuples of the integers $1, 2, \dots, n$. Now if F is strongly

homogeneous of order $l < k$ this implies that any l -tuple of the integers $1, 2, \dots, n$ is contained in the same number r of these k -tuples. Thus these k -tuples form a *balanced incomplete block design*.

EXAMPLE 5. Let F be the class of functions f_K ($K=1, 2, \dots, N$) defined on the set $S_n = \{1, 2, \dots, n\}$ and such that

$$f_K(j) = g_j(K) \quad 1 \leq j \leq n \quad (1 \leq k \leq N)$$

where the $g_j(k)$ ($1 \leq j \leq n$) are functions defined on the space $\Omega = \{1, 2, \dots, N\}$ such that if we introduce a uniform measure on Ω the g_j 's are equivalent (symmetrically dependent) random variables; then F is strongly homogeneous of every order.

EXAMPLE 6. Let n be arbitrary, $r < n$; let us form all possible $\binom{n}{r}$ sequences consisting of r ones and $n-r$ zeros, and let the matrix M of the family F consist of these rows. Then clearly F is strongly homogeneous of every order, because if $\epsilon_1, \dots, \epsilon_K$ ($K < n$) is any sequence of $l \leq K$ ones and $K-l$ zeros ($K \leq r$, $K-l \leq n-r$) the number of rows of M which have $\epsilon_1, \dots, \epsilon_K$ in the j_1 st, j_2 nd, $\dots$, j_K th column is $\binom{n-K}{r-l}$.

Now let us change the first row of M so that we replace every 1 by 0 and every 0 by 1. Clearly the matrix M^* so obtained is not strongly homogeneous of any order, but it is weakly homogeneous of every order. Evidently if the set of functions F^* has M^* as its matrix, for purposes of search F^* and F are equivalent, because F differs from F^* only in that f_1 has been replaced by $1-f_1$. This example shows that if F is a weakly homogeneous system of functions there sometimes exists an equivalent strongly homogeneous system; if we call two systems of functions F and F^* equivalent if their elements being f_K and f_K^* ($K=1, 2, \dots, N$), for every K and every pair of points x, y of S_n $f_K(x)=f_K(y)$ if and only if $f_K^*(x)=f_K^*(y)$. However not every weakly homogeneous system is equivalent to a strongly homogeneous one, as is shown by the next example.

EXAMPLE 7. The system of functions having the matrix

$$\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}$$

is weakly homogeneous of orders 2 and 3 but it is not equivalent to a strongly homogeneous system. The same holds if $n=2K$ is arbitrary and the rows of the matrix M of F are all possible sequences of K ones and K zeros starting with 1.

EXAMPLE 8. The system of functions having the matrix

$$\begin{array}{cccc}
 1 & 1 & 1 & 0 \\
 1 & 1 & 0 & 1 \\
 0 & 1 & 0 & 0 \\
 0 & 1 & 1 & 1 \\
 0 & 0 & 1 & 1
 \end{array}$$

is weakly homogeneous of order 3 but not of order 2.

EXAMPLE 9. The set F having the matrix

$$\begin{array}{ccccccc}
 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
 0 & 0 & 0 & 1 & 1 & 1 & 0
 \end{array}$$

is strongly homogeneous of order 2, weakly homogeneous of order 3, but not weakly homogeneous of order 4. In this example $R_1=7$, $R_2=3$, $R_3=1$.

We introduce still one further definition:

(V) A system of functions F is called homogeneous of order K if for any partition $K=K_1+K_2+\cdots+K_s$ of K the number $R_K[K_1, K_2, \cdots, K_s]$ of those $f \in F$ for which

$$\begin{aligned}
 f(x_{11}) &= f(x_{12}) = \cdots = f(x_{1K_1}) \\
 f(x_{21}) &= f(x_{22}) = \cdots = f(x_{2K_2}) \\
 &\vdots \\
 f(x_{s1}) &= f(x_{s2}) = \cdots = f(x_{sK_s})
 \end{aligned}$$

does not depend on the choice of the points x_{ij} from S_n provided they are all different.

Clearly if F is homogeneous of order K it is also homogeneous of any order $l < K$ further it is weakly homogeneous of any order $l \leq K$. Conversely if F is strongly homogeneous of order K it is also homogeneous of order K . Thus the notion of homogeneity is intermediate between strong and weak homogeneity.

Now we prove the following simple but rather surprising

LEMMA 3a. A set F of functions f taking on only the values 0 and 1

which is weakly homogeneous of order 2 is also weakly homogeneous of order 3.

PROOF.¹ Let A_i ($1 \leq i \leq n$), denote the set of those $f \in F$ for which $f(a_i) = 1$. Let us introduce a uniform measure on the set F . Then the A_i can be considered as random events, and the condition that F is weakly homogeneous of order 2 means that

$$P(A_i A_j) + P(\overline{A_i} \overline{A_j})$$

has the same value for any choice of the different indices i and j . (Here the product of two events denotes the joint occurrence of these events and $\overline{A}$ denotes the event that A does not occur.) Let us denote this value by C_2 , i.e. we put

$$C_2 = P(A_i A_j) + P(\overline{A_i} \overline{A_j}) \quad (1 \leq i < j \leq n).$$

To prove Lemma 2 we have to show that the value of $P(A_i A_j A_k) + P(\overline{A_i} \overline{A_j} \overline{A_k}) = C_3$ does not depend on the choice of the (different) indices i, j, k . As however

$$\begin{aligned} P(\overline{A_i} \overline{A_j} \overline{A_k}) &= 1 - P(A_i) - P(A_j) - P(A_k) + P(A_i A_j) + P(A_i A_k) \\ &\quad + P(A_j A_k) - P(A_i A_j A_k) \end{aligned}$$

and similarly

$$\begin{aligned} P(A_i A_j A_k) &= 1 - P(\overline{A_i}) - P(\overline{A_j}) - P(\overline{A_k}) + P(\overline{A_i} \overline{A_j}) + P(\overline{A_i} \overline{A_k}) \\ &\quad + P(\overline{A_j} \overline{A_k}) - P(\overline{A_i} \overline{A_j} \overline{A_k}) \end{aligned}$$

it follows

$$(2.1) \quad 2C_3 = 2(P(A_i A_j A_k) + P(\overline{A_i} \overline{A_j} \overline{A_k})) = 3C_2 - 1.$$

This proves Lemma 3a.

Note that if R_1 denotes the number of elements of F , R_2 the number of functions $f \in F$ for which $f(a_i) = f(a_j)$ for any pair (i, j) with $1 \leq i < j \leq n$ and R_3 the number of functions $f \in F$ for which $f(a_i) = f(a_j) = f(a_k)$ for any triple (i, j, k) ($1 \leq i < j < k \leq n$), then according to what has been proved above we have

$$(2.2) \quad 3R_2 - R_1 = 2R_3.$$

It follows from (2.2) that

$$(2.3) \quad \frac{1}{3} \leq \frac{R_2}{R_1} \leq 1.$$

¹ My first proof of Lemma 3a was slightly more complicated. Later, essentially the same simpler proof was found independently by Mrs. Vera T. Sós and Mr. T. Nemetz; the proof given here is a third version of their proof.

It is easy to prove that a weakly homogeneous system of order k is not necessarily of order $k+1$ if $k \geq 3$, e.g. for $k=3$ this can be seen from Example 9; thus the statement of Lemma 3a cannot be generalized by replacing 2 and 3 by k and $k+1$. However the following generalization of Lemma 3a is valid.

LEMMA 3b. *If the system F of functions with values 0 and 1 is weakly homogeneous of all orders $l \leq 2k$ then it is also weakly homogeneous of order $2k+1$ ($k=1, 2, \dots$).*

PROOF. Using the notations of the proof of Lemma 3a according to our suppositions

$$P(A_{i_1}A_{i_2} \cdots A_{i_l}) + P(\bar{A}_{i_1}\bar{A}_{i_2} \cdots \bar{A}_{i_l}) = C_l$$

does not depend on the choice of the different indices $i_1, i_2, \dots, i_l$ for $l \leq 2k$. Now similarly as we have proved (2.1) one can show that

$$(2.4) \quad \begin{aligned} & 2(P(A_{i_1}A_{i_2} \cdots A_{i_{2k+1}}) + P(\bar{A}_{i_1}\bar{A}_{i_2} \cdots \bar{A}_{i_{2k+1}})) \\ & = -(2k-1) + \sum_{l=2}^{2k} (-1)^l \binom{2k+1}{l} C_l. \end{aligned}$$

Thus Lemma 2b follows. Putting $c_l = R_l < R_1$ we obtain as a generalization of (2.2)

$$(2.5) \quad 2R_{2k+1} = -(2k-1)R_1 + \sum_{l=2}^{2k} (-1)^l \binom{2k+1}{l} R_l.$$

EXAMPLE 9. If the events A_i ($1 \leq i \leq n$) are symmetrically dependent, then the system F is clearly weakly homogeneous of every order. The same holds a fortiori if the events A_i are independent and have the same probability p . In this case

$$(2.6) \quad R_l = R_1(p^l + (1-p)^l) \quad (l = 1, 2, \dots)$$

and (2.5) is trivially satisfied.

Note that in case (2.6) holds we have $R_2 \geq R_1/2$.

It can be shown that weak homogeneity of every order l with $2 \leq l \leq 2k-1$ of a system of functions taking on the values 0 and 1 does not necessarily imply its weak homogeneity of order $2k$. This is shown e.g. by the following example, due to T. Nemetz (oral communication).

EXAMPLE 10. Let the function f defined on $S_{2k+1} = \{0, 1, 2, \dots, 2k\}$ belong to the family F if and only if the number of integers $1 \leq i \leq 2k$ for which $f(i)=0$ is even. Then clearly F is homogeneous of every order $l \leq 2k-1$ with $R_1 = 2^{2k}$, $R_l = 2^{2k-l+1}$ if $l \leq 2k-1$. However F is

not homogeneous of order $2k$ because the number of functions of $f \in F$ for which $f(1) = f(2) = \dots = f(2k)$ is 4 while the number of functions $f \in F$ for which $f(0) = f(1) = \dots = f(2k-1)$ is 2.

According to (2.3) if F is weakly homogeneous of order 2 then $R_2/R_1 \geq 1/3$. This inequality is best possible without restriction on n as is seen from Example 7. However a better lower bound can be given, which depends on n . We prove

LEMMA 4. Let F be a system of functions with values 0 and 1 on the set S_n which is weakly homogeneous of order 2. Let R_1 denote the number of elements of F and R_2 the number of functions $f \in F$ for which $f(a_i) = f(a_j)$ ($i \neq j$). Then we have

$$(2.7) \quad \frac{R_2}{R_1} \geq \frac{(n-2)}{2(n-1)}.$$

PROOF. Let $f_1, f_2, \dots, f_{R_1}$ denote the elements of F and $a_1, a_2, \dots, a_n$ the elements of S_n . Let us put

$$X = \sum_{j=1}^{R_1} \sum_{k=1}^n f_j(a_k).$$

By Cauchy's inequality we have

$$(2.8) \quad \begin{aligned} X^2 &= \left(\sum_{j=1}^{R_1} \sum_{k=1}^n f_j(a_k) \right)^2 \leq R_1 \sum_{j=1}^{R_1} \left(\sum_{k=1}^n f_j(a_k) \right)^2 \\ &= R_1 X + R_1 \sum_{k=1}^n \sum_{l=1}^n \sum_{j=1}^{R_1} f_j(a_k) f_j(a_l), \quad k \neq l. \end{aligned}$$

Now by supposition

$$(2.9) \quad \sum_{j=1}^{R_1} (1 - f_j(a_k) - f_j(a_l) + 2f_j(a_k)f_j(a_l)) = R_2$$

for all pairs k, l with $k \neq l$. Thus it follows that

$$(2.10) \quad n(n-1)R_2 = R_1 n(n-1) - 2(n-1)X + 2 \sum_{k=1}^n \sum_{l=1}^n f_j(a_k) f_j(a_l), \quad k \neq l.$$

Combining (2.8) and (2.10) we get

$$(2.11) \quad X^2 \leq R_1 X + \frac{1}{2} R_1 (n(n-1)(R_2 - R_1) + 2(n-1)X).$$

Thus it follows

$$(2.12) \quad \frac{R_2}{R_1} \geq 1 - \frac{2(n(X/R_1) - (X/R_1)^2)}{n(n-1)} \geq 1 - \frac{n}{2(n-1)} = \frac{n-2}{2(n-1)}$$

which proves Lemma 4.

3. On the duration of the random search. Let F be a set of R_1 functions on the set $S_n = \{a_1, a_2, \dots, a_n\}$ which separates the elements of S_n . Let x be an unknown element of S_n and let us suppose that we search for x in the following way: We choose first a function f_1 from F at random so that each element of F has the same probability $1/R_1$ to be chosen. We observe the value of $f_1(x)$, and after this choose again a function f_2 from F so that the choice of f_2 is independent from the choice of f_1 and each element f of F (including f_1) has the same probability $1/R_1$ to be chosen as f_2 . We observe $f_2(x)$ and choose an element f_3 of F independently from the choices of f_1 and f_2 , so that each element f of F has the same probability $1/R_1$ to be taken for f_3 . (Thus the possibility that f_3 is equal to f_1 or f_2 is not excluded.) We observe $f_3(x)$, etc. This process is repeated until $f_N(x)$ is selected. Let $P_1(n, N, F, x)$ denote the probability that the sequence $f_1(x), \dots, f_N(x)$ determines x uniquely. Let $P_2(n, N, F)$ denote the probability that the sequence $f_1(x), \dots, f_N(x)$ determines x whatever it may be. It has to be emphasized that $P_2(n, N, F)$ and $P_1(n, N, F, x)$ are usually different (even if $P_1(n, N, F, x)$ does not depend on x) and in general we can say only that $P_2(n, N, F) \leq \min_x P_1(n, N, F, x)$. This is shown for instance by the following:

EXAMPLE 11. Let S_3 be the set $\{1, 2, 3\}$ and let F consist of the three functions f_1, f_2 and f_3 where

$$\begin{aligned} f_1(1) &= 0, f_1(2) = 1, f_1(3) = 1, \\ f_2(1) &= 1, f_2(2) = 0, f_2(3) = 1, \\ f_3(1) &= 1, f_3(2) = 1, f_3(3) = 0. \end{aligned}$$

Evidently F separates the elements of S_3 because all columns of the corresponding matrix

$$\begin{array}{ccc} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

are different. Further F is weakly homogeneous of every order with $R_2=1$, $R_3=0$ and even strongly homogeneous of every order (with $R_2(1,1)=R_2(0,1)=R_2(1,0)=1$, $R_2(0,0)=0$ and $R_3(0,1,1)=R_3(1,0,1)=R_3(1,1,0)=1$). Now let us compute $P_1(3, 1, F, x)$. If $x=i$, x is

uniquely determined by the first chosen function if and only if this function is $f_i(x)$ ($i=1, 2, 3$) and otherwise not; thus for each fixed value of x , $P_1(3, 1, F, x) = 1/3$. On the other hand $P_2(3, 1, F) = 0$ because no function $f \in F$ determines x uniquely whatever x may be.

The difference between $P_1(n, N, F, x)$ and $P_2(n, N, F)$ can be made clear also as follows. Suppose the N functions which we have chosen by our random procedure are $f_1, \dots, f_N$. Consider the matrix M having N rows and n columns, in which the k th element of the j th row is $f_j(a_k)$.

Then a fixed unknown element x of S_n is determined by the observations $f_1(x), \dots, f_N(x)$ if and only if the x th column of this matrix M (containing the entries $f_j(x)$ ($j=1, 2, \dots, N$)) is different from every other column of M , while the observations $f_1(x), \dots, f_N(x)$ determine x whatever it may be if and only if any two columns of M are different, and this second condition imposes a much more severe restriction on M than the first and thus the probability of M having the second property is usually definitely less than the probability of M having the first property.

Thus we have to solve two different problems: to evaluate $\min_x P_1(n, N, F, x)$ and $P_2(n, N, F)$. First we give lower estimates for these quantities.

In what follows we shall repeatedly use the following well-known inequalities of elementary probability theory. Let $A_1, \dots, A_m$ be arbitrary events in a probability space; let the product of events denote the event consisting in the joint occurrence of the factors and let $\bar{A}$ denote the event contrary to the event A . Put $s_k = \sum P(A_{i_1} A_{i_2} \dots A_{i_k})$ ($1 \leq k \leq m$) where the summation is extended over all k -tuples $(i_1, i_2, \dots, i_k)$ which can be selected from the set $\{1, 2, \dots, m\}$, and put $s_0 = 1$. Then for $l=0, 1, 2, \dots$ the inequalities

$$(3.1) \quad \sum_{k=0}^{2l+1} (-1)^k s_k \leq P(\bar{A}_1 \dots \bar{A}_m) \leq \sum_{k=0}^{2l} (-1)^k s_k$$

hold, and one has

$$(3.2) \quad P(\bar{A}_1 \dots \bar{A}_m) = \sum_{k=0}^m (-1)^k s_k.$$

THEOREM 1. *If the system F of functions defined on the set $S_n = \{1, 2, \dots, n\}$ is weakly homogeneous of order 2, we have for all $x \in S_n$*

$$(3.3) \quad P_1(n, N, F, x) \geq 1 - (n-1) \left(\frac{R_2}{R_1} \right)^N$$

and

$$(3.4) \quad P_2(n, N, F) \geq 1 - \binom{n}{2} \left(\frac{R_2}{R_1} \right)^N.$$

PROOF. Let B_{ij} ($i \neq j$) denote the event that $f(i) = f(j)$ for all the N selected functions. Then we have

$$(3.5) \quad P_1(n, N, F, x) = P \left(\prod_{1 \leq i \leq n; i \neq x} \bar{B}_{ix} \right)$$

and

$$(3.6) \quad P_2(n, N, F) = P \left(\prod_{1 \leq i < j \leq n} \bar{B}_{ij} \right).$$

In view of $P(B_{ij}) = (R_2/R_1)^N$ we obtain from (3.1) immediately (3.3) and (3.4).

COROLLARY. If F_n is for each n a separating system for the set S_n which is weakly homogeneous of order 2, having $R_1(n)$ elements and the parameter $R_2(n)$, and if

$$(3.7) \quad \lim_{n \rightarrow \infty} \left(N_n \log \frac{R_1(n)}{R_2(n)} - \log n \right) = +\infty$$

then

$$(3.8) \quad \lim_{n \rightarrow \infty} \min_{x \in S_n} P_1(n, N_n, F_n, x) = 1.$$

If instead of (3.5) we suppose that

$$(3.9) \quad \lim_{n \rightarrow \infty} \left(N_n \log \frac{R_1(n)}{R_2(n)} - 2 \log n \right) = +\infty$$

we have

$$(3.10) \quad \lim_{n \rightarrow \infty} P_2(n, N_n, F_n) = 1.$$

Note that in order to be able to show that (3.10) holds, we had to choose N_n asymptotically twice as large as was needed to ensure the validity of (3.8).

To judge the "quality" of the random search procedures in question, one has to take into account that if only functions with values 0 and 1 are used, then $H(f) \leq 1$ and thus by Lemma 2 the duration of the best systematic search can not be less than $\log n$.

Thus Theorem 1 asserts that if we use a random search by means

of a family F of R_1 functions which is homogeneous of order 2, with parameters R_2 and if n is large, the duration of the search will be with probability near to 1 only about $(\log(R_1/R_2))^{-1}$ times, respectively about $2(\log(R_1/R_2))^{-1}$ times longer than with the best systematic method, according to whether we want to have a procedure which leads to the solution in a single given case, or one which is universally applicable. This shows that random search processes are under mild restrictions really almost as good as the best systematic method. The factor $(\log(R_1/R_2))^{-1}$ is of course usually larger than 1, but in case R_2/R_1 is equal to $\frac{1}{2}$ (or near to $\frac{1}{2}$) it is equal (near to) 1, and thus in such cases the random search procedure (for a single search) is with probability near to 1 if n is large asymptotically as good as the best systematic one.

Similarly we can get also an upper estimate for $P_1(n, N, F, x)$.

THEOREM 2a. *If the system F of functions with values 0 and 1 defined on the set is weakly homogeneous of order 2 (and thus by Lemma 3a also of order 3) we have for all $x \in S_n$*

$$(3.11) \quad P_1(n, N, F, x) \leq 1 - (n-1) \left(\frac{R_2}{R_1}\right)^N + \binom{n-1}{2} \left(\frac{R_3}{R_1}\right)^N$$

PROOF. (3.11) follows immediately from (3.5) and (3.1).

REMARK. By (2.2) we have $R_3/R_1 \leq \frac{1}{2}(3(R_2/R_1) - 1)$. Thus it follows that

$$\frac{R_3 R_1}{R_2^2} \leq \frac{3(R_2/R_1) - 1}{2(R_2/R_1)^2} \leq \frac{9}{8}.$$

Further, that in case

$$\frac{R_2}{R_1} \leq \frac{1}{2}$$

we have

$$\frac{R_3 R_1}{R_2^2} \leq 1.$$

Thus we get the following:

COROLLARY. *If for each n F_n is a system of functions with values 0 and 1 on the set S_n which is weakly homogeneous of order 2 and if $R_2(n)/R_1(n) \leq 1/2$ further*

$$\lim_{n_j \rightarrow \infty} \left(N_{n_j} \log \frac{R_1(n_j)}{R_2(n_j)} - \log n_j \right) = c > 0$$

then if x_{n_j} is any element of S_{n_j}

$$\begin{aligned} 1 - e^{-c} &\leq \liminf_{n_j \rightarrow \infty} P_1(n_j, N_{n_j}, F_{n_j}, x_{n_j}) \leq \limsup_{n \rightarrow \infty} P_1(n_j, N_{n_j}, F_{n_j}, x_{n_j}) \\ &\leq 1 - e^{-c} + \frac{e^{-2c}}{2}. \end{aligned}$$

A similar upper estimate can be given for $P_2(n, N, F)$ if F is supposed to be homogeneous of order 4.

THEOREM 2b. *If the system F is homogeneous of order 4 on the set S_n , then we have*

$$\begin{aligned} P_2(n, N, F) &\leq 1 - \binom{n}{2} \left(\frac{R_2}{R_1} \right)^N + \frac{3}{2} \binom{n}{3} \left(\frac{R_3}{R_1} \right)^N \\ &\quad + 3 \binom{n}{4} \left(\frac{R_4(2, 2)}{R_1} \right)^N. \end{aligned}$$

If we suppose that F is weakly homogeneous of every order, by using (3.2) we obtain an exact formula for $P_1(n, N, F, x)$, the value of which does not depend in this case on x .

THEOREM 3. *If the system F is weakly homogeneous of every order, then $P_1(n, N, F, x) = P_1(n, N, F)$ does not depend on x and we have*

$$P_1(n, N, F) = \sum_{K=0}^{n-1} (-1)^K \binom{n-1}{K} \left(\frac{R_{K+1}}{R_1} \right)^N.$$

As regards $P_2(n, N, F)$, to obtain a corresponding exact formula, we have to suppose that F is homogeneous of every order. The formula is however rather complicated, and therefore we do not write it out in detail here.

Let us add one final remark. A useful generalization of these results is obtained if we suppose that the values $f_1(x), \dots, f_N(x)$ are observed not directly, but through a noisy channel. This problem was considered in a special case in [5].

4. Examples.

EXAMPLE 12. Let $F(n)$ be the set of all 2^n functions with values 0 and 1 on S_n . Clearly $F(n)$ is homogeneous of every order with $R_K = 2^{n-K+1}$ ($K = 1, 2, \dots, n$). Thus we get from Theorem 3

$$P_1(n, N, F(n)) = \sum_{K=0}^{n-1} (-1)^K \binom{n-1}{K} \frac{1}{2^{NK}} = \left(1 - \frac{1}{2^N} \right)^{n-1}$$

This formula can of course be also directly verified (see [1] and [2]). It follows that if $N_{n_j} = \log_2 n_j + c + \epsilon_j$ where $\epsilon_j \rightarrow 0$ ($\log_2$ denotes logarithm with base 2) we have

$$\lim_{n_j \rightarrow \infty} P_1(n_j, N_{n_j}, F(n_j)) = \exp\left(-\frac{1}{2^c}\right).$$

In this case it is easy (see [1] and [2]) to determine $P_2(n, N, F(n))$ explicitly:

$$P_2(n, N, F(n)) = \prod_{l=1}^{n-1} \left(1 - \frac{l}{2^N}\right).$$

Thus if

$$N_{n_j} = 2 \log_2 n_j + c + \epsilon_j \quad \text{where} \quad \epsilon_j \rightarrow 0$$

we have

$$\lim_{n_j \rightarrow \infty} P_2(n_j, N_{n_j}, F(n_j)) = \exp\left(-\frac{1}{2^{c+1}}\right).$$

Note that the best systematic strategy requires the observation of $\{\log_2 n\}$ functions $f \in F(n)$. Thus if we are satisfied to find the unknown with probability 0.99, the number of necessary observations is only by 7 greater for the random strategy as for the best systematic strategy, independently of the value of n .

If for instance S_n is the set of all persons now living, then $\{\log_2 n\} = 32$. Thus with our random strategy we can find a person among all those living with ≤ 39 random dichotomies (instead of 32 dichotomies corresponding to the best systematic strategy).

EXAMPLE 13 (see [3]). Suppose that F consists of all functions taking on the values $0, 1, \dots, s-1$ on S_n . Then we obtain from Theorem 1 that $P_1(n, N, F)$ is near to 1 if $N - \log n / \log s$ is large, while $P_2(n, N, F)$ is near to 1 if $N - 2 \log n / \log s$ is large. Note that now $H(f) = \log_2 s$ for every $f \in F$, thus the best systematic strategy needs the observation of at least $\log n / \log s$ function $f \in F$.

EXAMPLE 14. Suppose that $F_n(P)$ consists of all functions which take on the value r for $l_r = p_r n$ different elements of S_n ($r = 1, 2, \dots, S$) where $P = \{p_1, \dots, p_s\}$ is a probability distribution. Then $F_n(P)$ is weakly homogeneous of order 2 with $R_2/R_1 \sim \sum_{r=1}^s p_r^2$. Thus by Theorem 1 $P_1(n, N, F_n(P))$ will be near to 1 if $N - \log_2 n / H_2(P)$ is large, where

$$H_2(P) = \log_2 \left(\sum_{r=1}^s p_r^2 \right)^{-1},$$

$H_2(P)$ is called (see [4]) *the entropy of order 2* of the probability distribution P .

The best systematic strategy needs the observation of about $\log_2 n/H_1(P)$ function $f \in F$ where

$$H_1(P) = \sum_{r=1}^s p_r \log_2 \frac{1}{p_r}.$$

Thus the efficiency of the random search is in this case $\sim H_2(P)/H_1(P)$.

It follows from the result of our paper [3] that for this example if

$$\lim_{n_j \rightarrow \infty} (N_{n_j} H_2(P) - 2 \log_2 n_j) = c$$

we have

$$\lim_{n_j \rightarrow \infty} P_2(n_j, N_{n_j}, F_{n_j}) = \exp\left(-\frac{1}{2^c}\right).$$

REFERENCES

1. A. Rényi, *On random generating elements of a finite Boolean algebra*, Acta Sci. Math. (Szeged) 22 (1961), 75–81.
2. ———, *Statistical laws of accumulation of information*, Bull. Inst. Internat. Statist. 39 (1962), 311–316.
3. ———, *Az információ-akkumuláció statisztikus törvényszerűségéről*, Magyar Tud. Akad. Mat. Fiz. Oszt. Közl. 12 (1962), 15–33.
4. ———, *On measures of entropy and information*, Proceedings of the 4th Berkeley Symposium, Vol. I, pp. 547–561, Univ. of California Press, Berkeley, Calif., 1961.
5. ———, *On a problem of information theory*, Publications of the Math. Inst. Hungarian Academy of Sciences 6 (1961), 505–516.

182, 187, 192, 193, 213, 256, 320, 344

ON THE MEAN VALUE OF NONNEGATIVE MULTIPLICATIVE
NUMBER-THEORETICAL FUNCTIONS

Paul Erdős and A. Rényi

INTRODUCTION

A complex-valued function $g(n)$ ($n = 1, 2, 3, \dots$) defined on the set of natural numbers is called *multiplicative* if, for all pairs n, m of relatively prime natural numbers,

$$(0.1) \quad g(n \cdot m) = g(n) \cdot g(m).$$

A multiplicative function $g(n)$ is called *strongly multiplicative* if for all primes p and all positive integers k it satisfies the additional condition

$$g(p^k) = g(p),$$

and *completely multiplicative* if (0.1) holds for all pairs n, m of natural numbers. We say that the number-theoretical function $g(n)$ has a *mean value* if the limit

$$\lim_{N \rightarrow +\infty} \frac{1}{N} \sum_{n=1}^N g(n) = M(g)$$

exists. The question of the existence of the mean value $M(g)$ has been much studied, but it has been solved only for certain subclasses. One of the definite results is the following theorem, due to H. Delange [2] (throughout the paper, p denotes a prime, and $\sum_p$ and $\prod_p$ denote a sum and a product, respectively, taken over all primes):

If $g(n)$ is a strongly multiplicative number-theoretical function such that $|g(n)| \leq 1$ for $n = 1, 2, \dots$, and such that the series

$$(0.2) \quad \sum_p \frac{g(p) - 1}{p}$$

converges, then $M(g)$ exists and

$$(0.3) \quad M(g) = \prod_p \left(1 + \frac{g(p) - 1}{p}\right).$$

Conversely, if $g(n)$ is a strongly multiplicative function such that $|g(n)| \leq 1$ ($n = 1, 2, \dots$), $M(g)$ exists, and $M(g) \neq 0$, then the series (0.2) converges, $g(2) \neq -1$, and (0.3) holds.

In the present paper we shall consider only *real, nonnegative* multiplicative functions.

The following theorem has been proved by P. Erdős [3]:

Received September 10, 1964.

THEOREM 1. If $g(n)$ is a nonnegative, strongly multiplicative function such that not only the series (0.2) but also the series

$$(0.4) \quad \sum_p \frac{(g(p) - 1)^2}{p}$$

converges, then $M(g)$ exists and (0.3) holds.

Erdős asked whether the convergence of the series (0.2) is in itself sufficient for the existence of $M(g)$, and if not, whether the requirement that the series (0.4) converges can be relaxed. The aim of this paper is to investigate these questions. While the answer to the first question is negative [that is, convergence of the series (0.2) does not by itself ensure the existence of $M(g)$], the following theorem, to be proved in Section 2, shows that the answer to the second question is affirmative.

THEOREM 2. Let $g(n)$ be a nonnegative and strongly multiplicative function such that the series (0.2) together with the series

$$(0.5) \quad \sum \frac{g^2(p)}{p^2}$$

converges, and such that for each $\varepsilon > 0$ there exist positive constants $\delta(\varepsilon)$ and $N(\varepsilon)$ with the property

$$(0.6) \quad \sum_{N \leq p \leq N(1+\varepsilon)} \frac{g(p) \log p}{p} \geq \delta(\varepsilon) \quad \text{for } N \geq N(\varepsilon);$$

then $M(g)$ exists and (0.3) holds.

Theorem 1 is not directly contained in Theorem 2, but Theorem 2 is nevertheless stronger than Theorem 1, in the sense that Theorem 1 can be deduced from Theorem 2. The relation between the two theorems is as follows: Suppose a function $g(n)$ satisfies the conditions in Theorem 1, and let $\mathcal{P}$ denote the set of primes for which $g(p) \leq 1/2$; then

$$\sum_{p \in \mathcal{P}} 1/p < \infty.$$

If for each prime $p \in \mathcal{P}$ we change the value of $g(p)$ to 1, then the function $g_1(n)$ thus obtained already satisfies the conditions of Theorem 2, and thus $M(g_1)$ exists; the existence of $M(g)$ and the validity of (0.3) follow easily from the existence of $M(g_1)$ and the validity of the corresponding formula for $M(g_1)$. On the other hand, Theorem 2 can be applied in many cases in which Theorem 1 gives no information.

In proving Theorem 2 we shall make use of an analytic method that H. Delange devised to prove his theorem mentioned above. The second-named author [6] has recently found a much simpler proof of Delange's theorem, but for the case studied in the present paper, the method of Delange seems more appropriate. Besides this method, we shall need an argument that resembles a step in the elementary proof of the prime number theorem (see [1], [4]).

In order to simplify the application of the method of Delange, we shall deal first with certain functions that we call exponentially multiplicative functions. A multiplicative function is called *exponentially multiplicative* if for all primes p and all natural numbers $k \geq 2$ it satisfies the condition

$$g(p^k) = \frac{(g(p))^k}{k!}.$$

In Section 1, we establish Theorem 3, which concerns a special class of exponentially multiplicative functions. In Section 2, we deduce Theorem 2 from Theorem 3 and show how Theorem 1 can be deduced from Theorem 2, while in Section 3 we deduce from Theorem 2 a corresponding result (Theorem 4) for general nonnegative multiplicative functions. In Section 4 we deal with cases where the mean value of a multiplicative function is 0 or ∞ , and we give some counterexamples.

1. EXPONENTIALLY MULTIPLICATIVE FUNCTIONS

THEOREM 3. *Let $g(n)$ be a nonnegative and exponentially multiplicative function such that the series (0.2) converges and condition (0.6) is satisfied. Then the limit*

$$M(g) = \lim_{N \rightarrow +\infty} \frac{1}{N} \sum_{n=1}^N g(n)$$

exists, and

$$M(g) = \prod_p \left(1 - \frac{1}{p}\right) \exp \frac{g(p)}{p}.$$

Proof. The Dirichlet generating series of a multiplicative function $g(n)$ evidently has the product-representation

$$\sum_{n=1}^{\infty} \frac{g(n)}{n^s} = \prod_p \left(\sum_{k=0}^{\infty} \frac{g(p^k)}{p^{ks}} \right).$$

If $g(n)$ is exponentially multiplicative, this can be written in the form

$$\sum_{n=1}^{\infty} \frac{g(n)}{n^s} = \exp \sum_p \frac{g(p)}{p^s}.$$

Now clearly the convergence of the series (0.2) implies the convergence of the infinite product

$$L(g) = \prod_p \left(1 - \frac{1}{p}\right) \exp \frac{g(p)}{p}.$$

Thus

$$\lim_{s \rightarrow +0} s \cdot \sum_{n=1}^{\infty} \frac{g(n)}{n^{1+s}} = \lim_{s \rightarrow +0} \frac{\sum_{n=1}^{\infty} \frac{g(n)}{n^{1+s}}}{\zeta(1+s)} = L(g).$$

From a well-known Tauberian theorem of G. H. Hardy and J. E. Littlewood [5] it now follows that

$$(1.1) \quad \lim_{N \rightarrow +\infty} \frac{\sum_{n=1}^N \frac{g(n)}{n}}{\log N} = L(g).$$

Thus the logarithmic mean value of the sequence $\{g(n)\}_1^\infty$ exists.

We shall need the identity

$$(1.2) \quad g(n) \log n = \sum_{p|n} g(p) g\left(\frac{n}{p}\right) \log p,$$

which we shall easily deduce from the definition of an exponentially multiplicative function.

As a matter of fact, if the canonical product representation of n is

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

then

$$(1.3) \quad g(n) \log n = \sum_{j=1}^r g(n) k_j \log p_j,$$

and for each j we have the formula

$$(1.4) \quad k_j g(n) = k_j g(p_j^{k_j}) g\left(\frac{n}{p_j^{k_j}}\right) = g(p_j) g\left(\frac{n}{p_j}\right).$$

From (1.3) and (1.4) we obtain (1.2). Let us now put

$$G(N) = \frac{1}{N} \sum_{n=1}^N g(n), \quad G^*(N) = \frac{1}{N \log N} \sum_{n=1}^N g(n) \log n.$$

Then

$$(1.5) \quad G(N) - G^*(N) = \Delta(N) = \frac{\sum_{n=1}^N G(n) n \log \left(1 + \frac{1}{n}\right)}{N \log N}.$$

We shall show now that

$$(1.6) \quad \lim_{N \rightarrow \infty} \Delta(N) = 0.$$

If we write $H(N) = \sum_{n=1}^N \frac{g(n)}{n}$, then

$$(1.7) \quad G(N) = H(N) - \frac{1}{N} \sum_{n=1}^{N-1} H(n).$$

Now (1.1) can be written in the form

$$(1.8) \quad \lim_{N \rightarrow \infty} \frac{H(N)}{\log N} = L(g),$$

and it follows from (1.8) that

$$(1.9) \quad \lim_{N \rightarrow \infty} \frac{\sum_{n=1}^{N-1} H(n)}{N \log N} = L(g).$$

Combining (1.7), (1.8), and (1.9), we conclude that

$$(1.10) \quad \lim_{N \rightarrow \infty} \frac{G(N)}{\log N} = 0.$$

From (1.5) and (1.10) it follows immediately that (1.6) holds.

From the identity (1.2) we deduce that

$$(1.11) \quad G(N) = \frac{1}{\log N} \sum_{p \leq N} \frac{g(p) \log p}{p} G\left(\left[\frac{N}{p}\right]\right) + \Delta(N),$$

where $\Delta(N)$ tends to 0 as $N \rightarrow +\infty$ ($[x]$ denotes the integral part of x). We shall now show that (1.11) implies that

$$(1.12) \quad \lim_{N \rightarrow \infty} G(N) = L(g),$$

which is the assertion of Theorem 3. To prove (1.12), let us put

$$A = \liminf_{N \rightarrow \infty} G(N), \quad B = \limsup_{N \rightarrow \infty} G(N).$$

It is easy to see that

$$(1.13) \quad \frac{H(N)}{\log N} = \frac{G(N)}{\log N} + \frac{\sum_{m=1}^{N-1} \frac{G(m)}{m+1}}{\log N}.$$

Taking into account (1.8) and (1.10), we see that $0 \leq A \leq L(g) \leq B \leq +\infty$. Thus if (1.12) were false, at least one of the inequalities $B > L(g)$ and $A < L(g)$ would hold. We shall show that either of these inequalities leads to a contradiction, and thus we shall establish (1.12).

In what follows, $C_1, C_2, \dots$ will denote positive constants. Let us suppose first that $B = +\infty$. Let $\{N_k\}$ be a sequence of natural numbers such that

$$\lim_{k \rightarrow +\infty} G(N_k) = +\infty \quad \text{and} \quad G(N_k) > G(n) \quad \text{for all } n < N_k.$$

Let us choose a number ε ($0 < \varepsilon < 1/2$), and let $\Gamma_k(\varepsilon)$ denote the set of those natural numbers n in the interval $1 \leq n \leq N_k$ for which $G(n) \leq G(N_k)(1 - \varepsilon)$. Putting $\text{Max}_N |\Delta(N)| = C_1$, we obtain the inequality

$$G(N_k) \leq \frac{G(N_k)(1 - \varepsilon)}{\log N_k} \sum_{\left[\frac{N_k}{p}\right] \in \Gamma_k(\varepsilon)} \frac{g(p) \log p}{p} + \frac{G(N_k)}{\log N_k} \sum_{\left[\frac{N_k}{p}\right] \notin \Gamma_k(\varepsilon)} \frac{g(p) \log p}{p} + C_1.$$

It follows that

$$(1.14) \quad \sum_{\left[\frac{N_k}{p}\right] \in \Gamma_k(\varepsilon)} \frac{g(p) \log p}{p} \leq \frac{1}{\varepsilon} \left(\sum_{p \leq N_k} \frac{g(p) \log p}{p} - \log N_k \right) + \frac{C_1 \log N_k}{\varepsilon G(N_k)}.$$

As is well known, it follows from the prime number theorem that

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + \alpha + o(1),$$

where α is a constant; together with the convergence of the series (0.2), this implies that

$$(1.15) \quad \sum_{p \leq x} \frac{(g(p) - 1) \log p}{p} = o(\log x).$$

Thus we obtain the estimate

$$(1.16) \quad \sum_{p \leq x} \frac{g(p) \log p}{p} \sim \log x.$$

Therefore we can find a natural number $k_1(\varepsilon)$ such that

$$(1.17) \quad \left| \sum_{p \leq N_k} \frac{g(p) \log p}{p} - \log N_k \right| \leq \varepsilon \cdot \delta \left(\frac{\varepsilon}{1 - 2\varepsilon} \right) \log N_k \quad \text{for } k \geq k_1(\varepsilon).$$

As $G(N_k) \rightarrow \infty$, we can by (1.14) and (1.16) choose $k_2(\varepsilon)$ so that

$$(1.18) \quad \sum_{\left[\frac{N_k}{p}\right] \in \Gamma_k(\varepsilon)} \frac{g(p) \log p}{p} \leq C_2 \cdot \varepsilon \left(\frac{\varepsilon}{1 - 2\varepsilon} \right) \log N_k \quad \text{for } k \geq k_2(\varepsilon),$$

where (for example) we can choose $C_2 = 2$.

We shall now show that (1.18) holds also (with some appropriate value of the constant C_2) if $B > L(g)$ is a finite number.

Let $\{N_k\}$ denote a sequence such that $G(N_k) \rightarrow B$. Let us choose $n_0(\varepsilon)$ so that

$$G(n) \leq B \left(1 + \varepsilon \cdot \delta \left(\frac{\varepsilon}{1 - 2\varepsilon} \right) \right) \quad \text{for } n \geq n_0(\varepsilon),$$

and let us put $\sup_n G(n) = C_3$. Let us further choose $k_3(\varepsilon)$ so that

$$|\Delta(N_k)| \leq \varepsilon \cdot \delta \left(\frac{\varepsilon}{1-2\varepsilon} \right) \quad \text{for } k \geq k_3(\varepsilon).$$

We obtain the inequality

$$G(N_k) \leq \frac{C_3}{\log N_k} \sum_{\frac{N_k}{p} < n_0(\varepsilon)} \frac{g(p) \log p}{p} + \frac{B \left(1 + \varepsilon \cdot \delta \left(\frac{\varepsilon}{1-2\varepsilon} \right) \right)}{\log N_k} \sum_{\left[\frac{N_k}{p} \right] \notin \Gamma_k(\varepsilon)} \frac{g(p) \log p}{p} \\ + \frac{G(N_k)(1-\varepsilon)}{\log N_k} \left(\sum_{\left[\frac{N_k}{p} \right] \in \Gamma_k(\varepsilon)} \frac{g(p) \log p}{p} \right) + \varepsilon \cdot \delta \left(\frac{\varepsilon}{1-2\varepsilon} \right) \quad \text{for } k \geq k_3(\varepsilon).$$

Now we choose $k_4(\varepsilon)$ so that

$$G(N_k) \geq B \left(1 - \varepsilon \cdot \delta \left(\frac{\varepsilon}{1-2\varepsilon} \right) \right) \quad \text{and} \quad N_k \geq n_0(\varepsilon) \quad \text{for } k \geq k_4(\varepsilon).$$

Then, for $k \geq k_5(\varepsilon) = \max(k_3(\varepsilon), k_4(\varepsilon))$, we have the inequality

$$\sum_{\left[\frac{N_k}{p} \right] \in \Gamma_k(\varepsilon)} \frac{g(p) \log p}{p} \leq \left(2 + \frac{1}{B} \right) \delta \left(\frac{\varepsilon}{1-2\varepsilon} \right) \log N_k + \frac{1}{\varepsilon} \left(\sum_{p < N_k} \frac{g(p) \log p}{p} - \log N_k \right) \\ + \frac{C_3}{B\varepsilon} \sum_{\frac{N_k}{n_0(\varepsilon)} < p < N_k} \frac{g(p) \log p}{p}.$$

Since the quantity

$$\sum_{\frac{N_k}{n_0(\varepsilon)} < p < N_k} \frac{\log p}{p}$$

is bounded (by a constant depending on ε), it follows from (1.15) that

$$\sum_{\frac{N_k}{n_0(\varepsilon)} < p < N_k} \frac{g(p) \log p}{p} = o(\log N_k).$$

Thus we can find a $k_6(\varepsilon)$ such that for $k \geq k_6(\varepsilon)$

$$\sum_{\frac{N_k}{n_0(\varepsilon)} < p < N_k} \frac{g(p) \log p}{p} \leq \frac{B\varepsilon}{C_3} \delta \left(\frac{\varepsilon}{1-2\varepsilon} \right).$$

Thus, by (1.17), if $k \geq k_7(\varepsilon) = \max(k_1(\varepsilon), k_5(\varepsilon), k_6(\varepsilon))$, then (1.18) holds also for the case where B is finite, if we choose the constant C_2 sufficiently large (in fact, $C_2 = 4 + 1/B$ is sufficient).

Let us now call those values of $n \leq N_k$ for which $n \in \Gamma_k(\varepsilon)$, that is, for which $G(n) \leq (1 - \varepsilon)G(N_k)$, ε -bad values. Clearly if n is 2ε -bad and $\frac{1-2\varepsilon}{1-\varepsilon}n \leq n' < n$, then

$$G(n') \leq \frac{n}{n'} G(n) \leq \left(\frac{1-\varepsilon}{1-2\varepsilon} \right) (1-2\varepsilon) G(N_k) = (1-\varepsilon) G(N_k),$$

and thus n' is ε -bad. Let $n_1, n_2, \dots, n_z$ denote all 2ε -bad values of n . Let us consider the sum

$$S_k(\varepsilon) = \sum_{n_j \in \Gamma_k(2\varepsilon)} \frac{1}{n_j} \sum_{\frac{1-2\varepsilon}{1-\varepsilon}n_j \leq \left[\frac{N_k}{p} \right] < n_j} \frac{g(p) \log p}{p}.$$

Since all values $\left[\frac{N_k}{p} \right]$ lying in an interval $\left[\frac{1-2\varepsilon}{1-\varepsilon}n_j, n_j \right)$ are ε -bad, it is evident that

$$S_k(\varepsilon) \leq \sum_{\left[\frac{N_k}{p} \right] \in \Gamma_k(\varepsilon)} \left(\frac{g(p) \log p}{p} \sum_{\frac{N_k}{p} < n < \frac{N_k}{p} \left(\frac{1-\varepsilon}{1-2\varepsilon} \right)} \frac{1}{n} \right).$$

Clearly, the sum over n in the right-hand member is less than $C_4 \varepsilon$, and therefore

$$(1.19) \quad S_k(\varepsilon) \leq C_4 \varepsilon \sum_{\left[\frac{N_k}{p} \right] \in \Gamma_k(\varepsilon)} \frac{g(p) \log p}{p}.$$

On the other hand,

$$S_k(\varepsilon) = \sum_{n_j \in \Gamma_k(2\varepsilon)} \left(\frac{1}{n_j} \sum_{\frac{N_k}{n_j} < p < \frac{N_k}{n_j} \left(1 + \frac{\varepsilon}{1-2\varepsilon} \right)} \frac{g(p) \log p}{p} \right),$$

and thus, by our supposition (0.6), if k is sufficiently large, then

$$(1.20) \quad S_k(\varepsilon) \geq \delta \left(\frac{\varepsilon}{1-2\varepsilon} \right) \cdot \sum_{n_j \in \Gamma_k(2\varepsilon), n_j \leq \frac{N_k}{N(\varepsilon)}} \frac{1}{n_j}.$$

Comparing (1.18), (1.19), and (1.20), we obtain the estimate

$$\sum_{n_j \in \Gamma_k(2\varepsilon), n_j < \frac{N_k}{N(\varepsilon)}} \frac{1}{n_j} \leq \frac{C_4 \varepsilon}{\delta \left(\frac{\varepsilon}{1-2\varepsilon} \right)} C_2 \delta \left(\frac{\varepsilon}{1-2\varepsilon} \right) \log N_k = C_5 \varepsilon \log N_k.$$

It follows by the definition of the set $\Gamma_k(2\varepsilon)$ that for sufficiently large k

$$(1.21) \quad \sum_{n=1}^{N_k} \frac{G(n)}{n} \geq \left(\sum_1^{\left[\frac{N_k}{N(\varepsilon)} \right]} \frac{1}{n} - C_5 \varepsilon \log N_k \right) (1 - \varepsilon) G(N_k) \geq (1 - C_6 \varepsilon) G(N_k) \log N_k.$$

In view of (1.8), (1.10), and (1.13), we have however the relation

$$(1.22) \quad \lim_{N \rightarrow \infty} \frac{1}{\log N} \sum_{n=1}^N \frac{G(n)}{n} = L(g).$$

Comparing (1.21) and (1.22), we conclude that

$$L(g) \geq (1 - C_6 \varepsilon) B,$$

which is impossible if $B = +\infty$, and also if B is finite and $B > L(g)$, provided that ε is chosen sufficiently small. This contradiction proves that $B = L(g)$.

Now we prove that the assumption $A < L(g)$ also leads to a contradiction. The proof is similar to that given above for the impossibility of $B > L(g)$, but is somewhat simpler because $0 \leq A \leq L(g)$ and thus A is always finite, wherefore we need not distinguish between two cases (as before between $B = +\infty$ and $B < +\infty$).

Let $\{N_k\}$ be a sequence of natural numbers such that $\lim_{k \rightarrow \infty} G(N_k) = A$. Let $\gamma_k(\varepsilon)$ denote the set of those integers n ($1 \leq n \leq N_k$) for which $G(n) > (1 + \varepsilon)A$, and let us call the values n belonging to $\gamma_k(\varepsilon)$ the ε -bad values. We choose $k_9(\varepsilon)$ so large that

$$G(N_k) \leq A \left(1 + \varepsilon \cdot \delta \left(\frac{\varepsilon}{1 + \varepsilon} \right) \right) \quad \text{and} \quad |\Delta(N_k)| \leq \varepsilon \cdot \delta \left(\frac{\varepsilon}{1 + \varepsilon} \right)$$

for $k \geq k_9(\varepsilon)$, and $D(\varepsilon)$ so that

$$G(n) \geq A \left(1 - \varepsilon \cdot \delta \left(\frac{\varepsilon}{1 + \varepsilon} \right) \right) \quad \text{for } n \geq D(\varepsilon).$$

It follows from (1.11) that if $k \geq k_{10}(\varepsilon)$, then

$$\sum_{\substack{[\frac{N_k}{p}] \\ \in \gamma_k(\varepsilon)}} \frac{g(p) \log p}{p} \leq C_7 \delta \left(\frac{\varepsilon}{1 + \varepsilon} \right) \log N_k.$$

Now if n is 2ε -bad and $n \leq n' \leq \left(\frac{1 + 2\varepsilon}{1 + \varepsilon} \right) n$, then

$$G(n') \geq \frac{n}{n'} G(n) \geq \left(\frac{1 + \varepsilon}{1 + 2\varepsilon} \right) (1 + 2\varepsilon) A = (1 + \varepsilon) A,$$

and thus n' is ε -bad. For the sum

$$\bar{S}_k(\varepsilon) = \sum_{n_j \in \gamma_k(2\varepsilon)} \left(\frac{1}{n_j} \sum_{\substack{n_j < \frac{N_k}{p} < n_j \left(\frac{1 + 2\varepsilon}{1 + \varepsilon} \right)}} \frac{g(p) \log p}{p} \right)$$

we obtain the inequalities

$$\bar{S}_k(\varepsilon) \leq C_8 \varepsilon \sum_{\substack{\left[\frac{N_k}{p} \right] \\ p \in \gamma_k(\varepsilon)}} \frac{g(p) \log p}{p}$$

and

$$\bar{S}_k(\varepsilon) \geq \delta \left(\frac{\varepsilon}{1+\varepsilon} \right) \sum_{\substack{n_j \in \gamma_k(2\varepsilon) \\ N_k(1+\varepsilon) \\ n_j < \frac{N_k(1+\varepsilon)}{(1+2\varepsilon)N(\varepsilon)}}} \frac{1}{n_j},$$

and thus it follows that

$$\sum_{\substack{n_j \in \gamma_k(2\varepsilon) \\ N_k(1+\varepsilon) \\ n_j < \frac{N_k(1+\varepsilon)}{(1+2\varepsilon)N(\varepsilon)}}} \frac{1}{n_j} \leq C_9 \varepsilon \log N_k.$$

This implies (since from the first part of the proof we already know that $G(n)$ is bounded) that for $k \geq k_{11}(\varepsilon)$

$$\sum_{n=1}^{N_k} \frac{G(n)}{n} \leq \frac{1}{\log N_k} \leq (1+\varepsilon)A + C_{10} \varepsilon,$$

and thus, in view of (1.22),

$$L(g) \leq (1+\varepsilon)A + C_{10} \varepsilon.$$

This contradicts the inequality $L(g) > A$, if ε is sufficiently small. Thus $L(g) > A$ is impossible, and Theorem 3 is proved.

Let us mention that the condition (0.6) is certainly satisfied if $g(p)$ has a positive lower bound.

2. STRONGLY MULTIPLICATIVE FUNCTIONS

Corresponding to two number-theoretical functions $g_1 = g_1(n)$ and $g_2 = g_2(n)$ we define the function $g_3 = g_1 * g_2$ (called the *convolution* of g_1 and g_2) by putting

$$g_3(n) = \sum_{d|n} g_1(d) g_2\left(\frac{n}{d}\right).$$

Clearly, if any two of g_1, g_2, g_3 are multiplicative, so is the third, and

$$(2.1) \quad \sum_{n=1}^{\infty} \frac{g_3(n)}{n^s} = \left(\sum_{n=1}^{\infty} \frac{g_1(n)}{n^s} \right) \left(\sum_{n=1}^{\infty} \frac{g_2(n)}{n^s} \right).$$

We shall use the following simple lemma, which is due to A. Wintner [8]:

LEMMA. If $g_3 = g_1 * g_2$, and if further the mean value $M(g_1)$ of g_1 exists and the series

$$(2.2) \quad \sum_{n=1}^{\infty} \frac{|g_2(n)|}{n}$$

converges, then $M(g_3)$ exists and

$$M(g_3) = M(g_1) \sum_{n=1}^{\infty} \frac{g_2(n)}{n}.$$

Proof of Theorem 2. Let $g_1(n)$ denote the exponentially multiplicative function whose values for primes are the same as those of $g(n)$. Then by virtue of (2.1),

$$g(n) = g_1(n) * g_2(n),$$

where

$$\sum_{n=1}^{\infty} \frac{g_2(n)}{n^s} = \prod_p \left(1 + \frac{\sum_{k=0}^{\ell-1} \frac{(-1)^k g(p)^{k+1}}{k!} + \frac{(-1)^\ell g(p)^\ell}{\ell!}}{p^{\ell s}} \right).$$

It follows from the convergence of the series (0.5) that the series (2.2) converges; thus by our lemma $M(g)$ exists and (0.3) holds. This proves Theorem 2.

Clearly the conditions (0.5) and (0.6) of Theorem 2 are satisfied if $g(p)$ has a positive lower bound and is also bounded from above.

Deduction of Theorem 1 from Theorem 2. Suppose that $g(n)$ satisfies the conditions of Theorem 1, and define the strongly multiplicative function $g_1(n)$ by putting

$$g_1(p) = \begin{cases} g(p) & \text{if } g(p) \geq 1/2, \\ 1 & \text{if } g(p) < 1/2. \end{cases}$$

Since the series (0.4) is supposed to converge, it follows that if S denotes the set of those primes p for which $g(p) < 1/2$, then the series

$$\sum_{p \in S} \frac{1}{p}$$

converges. Putting $g(n) = g_1(n) * g_2(n)$, we see that

$$\sum \frac{g_2(n)}{n^s} = \prod_{p \in S} \left(1 + \frac{g(p) - 1}{p^s} \right).$$

Thus the series

$$\sum \frac{|g_2(n)|}{n}$$

is convergent.

Clearly $g_1(n)$ satisfies the conditions of Theorem 2, because

$$\sum \frac{g_1^2(p)}{p^2} = \sum_{p \in S} \frac{1}{p^2} + \sum \frac{g^2(p)}{p^2} \leq \sum \frac{2(g(p) - 1)^2 + 3}{p^2}.$$

It follows that $M(g_1)$ exists; thus Lemma 1 can be applied, and we conclude that $M(g)$ exists and (0.3) holds. This proves Theorem 1.

3. GENERAL MULTIPLICATIVE FUNCTIONS

THEOREM 4. *Let $g(n)$ be a nonnegative multiplicative function for which the series (0.2) and the series*

$$(3.1) \quad \sum_p \frac{g^2(p)}{p^2} + \sum_p \sum_{k=2}^{\infty} \frac{g(p^k)}{p^k}$$

converge, and suppose that to every positive ε there correspond positive constants $\delta(\varepsilon)$ and $N(\varepsilon)$ such that condition (0.6) is satisfied. Then $M(g)$ exists and

$$(3.2) \quad M(g) = \prod_p \left(1 + \sum_{k=1}^{\infty} \frac{g(p^k) - g(p^{k-1})}{p^k} \right).$$

Proof. We deduce Theorem 4 from Theorem 2 by using again the lemma in Section 2. Let $g_1(n)$ be the exponentially multiplicative function that takes the same value as $g(n)$, when n is prime, and put $g = g_1 * g_2$. Then clearly g_1 satisfies the conditions of Theorem 2, and thus $M(g_1)$ exists. Further,

$$\sum_{n=1}^{\infty} \frac{g_2(n)}{n^s} = \prod_p \left(1 + \sum_{k=2}^{\infty} \frac{\sum_{\ell=0}^k g(p^\ell) (-1)^{k-\ell} \frac{g^{k-\ell}(p)}{(k-\ell)!}}{p^{ks}} \right).$$

Thus it follows from the convergence of the series (3.1) that

$$\sum \frac{|g_2(n)|}{n} < \infty;$$

therefore the lemma can be applied, and the existence of $M(g)$ and the validity of (3.2) follow.

COROLLARY. *Let $g(n)$ be a nonnegative multiplicative function, and suppose there exist positive constants a and b such that*

$$g(p) \geq a \quad \text{and} \quad g(p^k) \leq b$$

for all primes p and for $k = 1, 2, \dots$. Suppose further that the series (0.2) converges. Then $M(g)$ exists and (3.2) holds.

4. MULTIPLICATIVE FUNCTIONS WHOSE MEAN VALUE IS 0 OR $+\infty$

The condition in Theorem 2 that the series (0.5) should converge is necessary for the convergence (to a positive limit) of the infinite product on the right-hand side of (0.3). As a matter of fact, it is easy to see that if the series (0.2) converges and the series (0.5) diverges, then

$$\lim_{x \rightarrow +\infty} \prod_{p \leq x} \left(1 + \frac{g(p) - 1}{p}\right) = 0.$$

Thus one is led to the conjecture that if all the other conditions of Theorem 2 are satisfied but the series (0.5) diverges, then $M(g) = 0$. Similarly, if for instance $g(n)$ is completely multiplicative and the series (0.5) diverges, then the product on the right of (3.2) diverges to $+\infty$, and thus one is again led to the conjecture that if all the other conditions of Theorem 4 are satisfied for a completely multiplicative function but the series (3.1) diverges, then $M(g) = +\infty$. Both these conjectures are true, as is shown by the following theorems.

THEOREM 5. *Let $g(n)$ be a nonnegative, completely multiplicative function such that the series (0.2) converges and the series (0.5) diverges. Suppose further that condition (0.6) holds. Then $M(g) = +\infty$, that is,*

$$(4.1) \quad \lim_{N \rightarrow +\infty} \frac{1}{N} \sum_{n=1}^N g(n) = +\infty.$$

THEOREM 6. *Let $g(n)$ be a nonnegative, strongly multiplicative function such that the series (0.2) converges and the series (0.5) diverges. Suppose that condition (0.6) holds. Then $M(g) = 0$.*

It should be mentioned that if under the conditions of Theorem 5 we put

$$(4.2) \quad E(p) = 1 + \sum_{k=1}^{\infty} \frac{g(p^k) - g(p^{k-1})}{p^k},$$

then

$$E(p) = \frac{1 - \frac{1}{p}}{1 - \frac{g(p)}{p}}$$

and thus

$$\lim_{x \rightarrow \infty} \prod_{p < x} E(p) = \infty,$$

while under the conditions of Theorem 6

$$E(p) = 1 + \frac{g(p) - 1}{p}$$

and thus

$$\lim_{x \rightarrow +\infty} \prod_{p < x} E(p) = 0.$$

This shows that Theorems 2 and 6 can be combined and expressed in the form of the following single statement:

THEOREM 7. *If $g(n)$ is a nonnegative and strongly multiplicative function such that the series (0.2) converges and condition (0.6) is fulfilled, then $M(g)$ exists and*

$$(4.3) \quad M(g) = \lim_{x \rightarrow \infty} \prod_{p \leq x} \left(1 + \frac{g(p) - 1}{p} \right),$$

this limit being positive or zero according to whether the series (0.5) converges or diverges.

Similarly, combining Theorem 5 with what follows from Theorem 4 for completely multiplicative functions, we obtain the following result.

THEOREM 8. *Let $g(n)$ be a nonnegative and completely multiplicative function for which the series (0.2) converges and condition (0.6) is fulfilled; suppose further that $g(p) < p$ for all primes p . Then*

$$M(g) = \lim_{x \rightarrow \infty} \prod_{p < x} \frac{\left(1 - \frac{1}{p} \right)}{\left(1 - \frac{g(p)}{p} \right)},$$

this limit being either finite and positive or infinite according to whether the series (0.5) converges or diverges.

These theorems suggest the following conjecture: The mean value of a nonnegative multiplicative function $g(n)$ exists if and only if the limit

$$\lim_{x \rightarrow \infty} \prod_{p < x} E(p)$$

exists (where $E(p)$ is defined by (4.2)), and the two are equal whenever they exist, including the case where the limit is $+\infty$.

Proof of Theorem 5. Let $g(n)$ be a completely multiplicative function satisfying the conditions of Theorem 5. Let $g_1(n)$ be the exponentially multiplicative function for which $g_1(p) = g(p)$ for all primes. Then, by Theorem 3, $M(g_1)$ exists and is positive. Now clearly if

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} p_{r+1} \cdots p_s,$$

where $\alpha_i \geq 2$ ($i = 1, 2, \dots, r$), then

$$g(n) = \frac{1}{r} \sum_{i=1}^r g(p_i^2) g\left(\frac{n}{p_i^2}\right).$$

Since however $1/r \geq 1/2^{r-1} \geq \alpha_i! / \prod_{j=1}^r \alpha_j!$, it follows that

$$g(n) \geq \sum_{i=1}^r g^2(p_i) g_1\left(\frac{n}{p_i^2}\right),$$

and thus, for any fixed $D > 0$,

$$\frac{1}{N} \sum_{n=1}^N g(n) \geq \frac{1}{N} \sum_{p \leq D} \left(g(p^2) \sum_{\substack{m \leq N \\ p^2 \mid m}} g_1(m) \right).$$

However, for each fixed $p \leq D$,

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{\substack{m \leq N \\ p^2 \mid m}} g_1(m) = \frac{M(g_1)}{p^2},$$

and therefore

$$\liminf_{N \rightarrow +\infty} \frac{1}{N} \sum_{n=1}^N g(n) \geq M(g_1) \sum_{p \leq D} \frac{g^2(p)}{p^2}.$$

Since this holds for arbitrarily large values of D and the series (0.5) diverges, by hypothesis, it follows that

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N g(n) = +\infty,$$

and thus Theorem 5 is proved.

Proof of Theorem 6. Let $g(n)$ be a strongly multiplicative function satisfying the conditions of Theorem 5. Let $g_1(n)$ be the exponentially multiplicative function for which $g_1(p) = g(p)$, and $g_0(n)$ the multiplicative function defined by

$$g_0(p) = g(p) \quad \text{and} \quad g_0(p^k) = 0 \quad \text{for } k \geq 2.$$

First we prove that $M(g_0)$ exists and is equal to 0. To show this, let $g^{(D)}(n)$ be the multiplicative function defined as follows:

$$\begin{aligned} g^{(D)}(p) &= g(p) \quad \text{for all primes } p, \\ g^{(D)}(p^2) &= 0 \quad \text{for } p \leq D, \\ g^{(D)}(p^k) &= g_1(p^k) \text{ if } p \leq D \text{ and } k \geq 3 \text{ or } p > D \text{ and } k \geq 2. \end{aligned}$$

Clearly, for all n and D ,

$$g_0(n) \leq g^{(D)}(n) \leq g_1(n).$$

For each square-free integer d , let us further define $g_1^{(d)}(n)$ as the exponentially multiplicative function for which $g_1^{(d)}(p) = 0$ if $p \mid d$ and $g_1^{(d)}(n) = g_1(n)$ if n is relatively prime to d . Then

$$\begin{aligned} \frac{1}{N} \sum_{n=1}^N g^{(D)}(n) &= \frac{1}{N} \sum_{n=1}^N g_1(n) - \sum_{p \leq D} \left(\frac{g(p^2)}{2} \sum_{m \leq \frac{N}{p^2}} g_1^{(p)}(m) \right) \\ &+ \sum_{p \leq D, q \leq D, p \neq q} \left(\frac{g(p^2)g(q^2)}{4} \sum_{m \leq \frac{N}{p^2 q^2}} g_1^{(pq)}(m) \right) - \dots \end{aligned}$$

For each square-free d , $M(g_1^{(d)})$ clearly exists by Theorem 3, and

$$M(g_1^{(d)}) = M(g_1) \exp \left(- \sum_{p|d} \frac{g(p)}{p} \right);$$

it follows that $M(g^{(D)})$ exists and

$$M(g^{(D)}) = \prod_{p \leq D} \left(1 - \frac{g(p^2)}{2p^2} \exp \left(- \frac{g(p)}{p} \right) \right) M(g_1).$$

Since

$$\lim_{D \rightarrow \infty} \prod_{p \leq D} \left(1 - \frac{g(p^2)}{2p^2} \exp \left(- \frac{g(p)}{p} \right) \right) = 0,$$

it follows that $M(g_0) = 0$. Using the lemma in Section 2, we easily see that $M(g) = 0$. Thus Theorem 6 is proved.

In all our theorems we have supposed that the series (0.2) converges. If this condition is dropped, then $M(g)$ does not exist in general. As a matter of fact, it is easy to construct multiplicative (and strongly multiplicative) functions, bounded by positive constants both from below and above, for which the series (0.2) diverges and the logarithmic means

$$\frac{1}{\log N} \sum_{n=1}^N \frac{g(n)}{n}$$

oscillate between different upper and lower limits. For this purpose it is sufficient to put

$$g(p) = \begin{cases} 1/2 & (n_{2k} \leq p < n_{2k+1}), \\ 2 & (n_{2k+1} \leq p < n_{2k+2}), \end{cases}$$

for some rapidly increasing sequence $\{n_k\}$. It is well known that

$$\begin{aligned} \liminf_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N g(n) &\leq \liminf_{N \rightarrow \infty} \frac{1}{\log N} \sum_{n=1}^N \frac{g(n)}{n} \\ &\leq \limsup_{N \rightarrow \infty} \frac{1}{\log N} \sum_{n=1}^N \frac{g(n)}{n} \leq \limsup_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N g(n), \end{aligned}$$

and it follows that $M(g)$ does not exist.

We can also give a counterexample showing that the convergence of the series (0.2) alone does not ensure the existence of $M(g)$, not even if the values 0 and $+\infty$ are admitted, and not even if $g(p)$ has a positive lower bound. Let p_k denote the least prime p for which

$$p \geq e^{e^{\sqrt{k}}},$$

and let

$$g(p_k) = \frac{p_k}{4\sqrt{k}}, \quad g(p) = \frac{1}{2} \quad (p \notin \{p_k\}).$$

Then

$$\sum_{e^{e^{\sqrt{k}}} < p < e^{e^{\sqrt{k+1}}}} \frac{g(p) - 1}{p} = O(k^{-3/2}),$$

and thus the series (0.2) converges. Let us now put

$$\begin{aligned} g(p^2) &= 0 \quad (p \notin \{p_k\}), \\ g(p_k^2) &= \begin{cases} \frac{3}{4} g^2(p_k) & (n_{2j} \leq k < n_{2j+1}), \\ \frac{1}{4} g^2(p_k) & (n_{2j+1} \leq k < n_{2j+2}), \end{cases} \\ g(p^\ell) &= g(p^2) \quad (p \text{ prime}, \ell \geq 3). \end{aligned}$$

Then the series $\sum g(p_k^2)/p_k^2$ diverges, and Theorem 4 is not applicable.

It is easy to see that the product

$$\prod_{p < x} E(p) = \prod_{p < x} \left(1 + \frac{g(p) - 1}{p} + \frac{g(p^2) - g(p)}{p^2} \right)$$

oscillates between 0 and ∞ , if the sequence $\{n_j\}$ increases fast enough. It follows that the logarithmic mean values

$$\frac{1}{\log N} \sum_{n=1}^N \frac{g(n)}{n}$$

and thus the arithmetic mean values

$$\frac{1}{N} \sum_{n=1}^N g(n)$$

do the same. In our example $g(p)$ is bounded from below, and thus condition (0.6) is of course fulfilled.

Remark. After finishing this paper, we were informed by E. Wirsing that he has constructed a nonnegative multiplicative function $g(n)$ for which the series (0.2) and (3.1) converge but $M(g)$ does not exist. This example shows that the condition (0.6) in Theorem 4 is necessary. By modifying slightly the example one can show that the condition is necessary also in Theorems 2 and 3. Wirsing's example concerning Theorem 4 is as follows: Let p_k be defined as the least prime greater than e^k , and let

$$\begin{aligned} g(p_k) &= \frac{e^k}{k} & (k = 1, 2, \dots), \\ g(p) &= 0 & (p \notin \{p_k\}), \\ g(p^\ell) &= 0 & (p \text{ prime, } \ell \geq 2). \end{aligned}$$

Wirsing further proved that if $g(n)$ is a nonnegative multiplicative function for which $g(p^k)$ is bounded from above, then the convergence of the series (0.2) alone is sufficient for the existence of the mean value $M(g)$. His results will be published in a forthcoming paper.

REFERENCES

1. J. G. van der Corput, *Démonstration élémentaire du théorème sur la distribution des nombres premiers*, Math. Centrum Amsterdam, Scriptum no. 1 (1948), 32 pp.
2. H. Delange, *Sur les fonctions arithmétiques multiplicatives*, Ann. Sci. École Norm. Sup. (3) 78 (1961), 273-304.
3. P. Erdős, *Some asymptotic formulas for multiplicative functions*, Bull. Amer. Math. Soc. 53 (1947), 536-544.
4. ———, *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proc. Nat. Acad. Sci. U.S.A. 35 (1949), 374-384.
5. G. H. Hardy and J. E. Littlewood, *Tauberian theorems concerning power series and Dirichlet's series whose coefficients are positive*, Proc. London Math. Soc. (2) 13 (1914), 174-191.
6. A. Rényi, *A new proof of a theorem of Delange*, Publ. Math. Debrecen (to appear).
7. A. Wintner, *Eratosthenian averages*, Waverly Press, Baltimore, 1943.
8. ———, *The theory of measure in arithmetical semi-groups*, Waverly Press, Baltimore, 1944.

NOTE

The conjecture on p. 334 (?) has been, as remarked at the end of the paper, disproved by E. Wirsing (*Acta Math. Hung.*, **18** (1967), 411—467) where he also obtained the most general theorem known up to now on non-negative multiplicative functions, essentially under the restriction $g(P) = O(1)$ and as shown by G. Halász (*ibid.*, **19** (1968), 365—403), this restriction cannot be relaxed. However, the results of the present paper are not included in Wirsing's results: Owing to condition (0.6) they allow, in a surprising way, a much larger order of magnitude than Wirsing's $g(P) = O(1)$ and this fact might lead to interesting applications to real valued additive functions.

The procedure, attributed to Delange, of combining formula (1.2) (that goes back essentially to Tchebycheff) with the Tauberian theorem of Hardy and Littlewood was first used by Wirsing (*Arch. Math.*, **7** (1956), 263—272). Later both he (*Math. Ann.*, **143** (1961), 75—102) and in a simpler way Delange (*Proc. Amer. Math. Soc.*, **18** (1967), 743—749) dispensed with the Tauberian theorem. (G. H.)

A new proof of a theorem of Delange

By ALFRÉD RÉNYI (Budapest)

§ 1. Introduction

A complex-valued function $g(n)$ defined on the set of natural numbers is called a *multiplicative number theoretical function* if

$$(1.1) \quad g(n \cdot m) = g(n) \cdot g(m) \quad \text{for } (n, m) = 1.$$

Here and in what follows (n, m) denotes the greatest common divisor of n and m ; if besides (1.1) one has for any prime p

$$(1.2) \quad g(p^\alpha) = g(p) \quad \text{for } \alpha = 2, 3, \dots$$

then $g(n)$ is called *strongly multiplicative*.

A complex-valued function $f(n)$ defined on the set of natural numbers is called an *additive number theoretical function* if

$$(1.3) \quad f(n \cdot m) = f(n) + f(m) \quad \text{for } (n, m) = 1$$

and *strongly additive* if besides (1.3) for every prime p

$$(1.4) \quad f(p^\alpha) = f(p) \quad \text{for } \alpha = 2, 3, \dots$$

The theorem of DELANGE in question is the following (see [1] and [2]):

Theorem of Delange: Let $g(n)$ be a strongly multiplicative (complex-valued) number theoretical function such that

$$(1.5) \quad |g(n)| \leq 1 \quad \text{for } n = 1, 2, \dots$$

Suppose that the series

$$(1.6) \quad \sum_p \frac{g(p) - 1}{p}$$

is convergent, where p runs over all primes*). Then the limit

$$(1.7) \quad \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N g(n) = M(g)$$

*) Throughout this paper p always denotes a prime.

exists, and one has

$$(1.8) \quad M(g) = \prod_p \left(1 + \frac{g(p) - 1}{p} \right).$$

Remark. Delange has proved also that the convergence of the series (1.6) is also necessary for the existence of a *non-zero* mean value $M(g)$ of g , under the condition (1.5), but in what follows we shall deal only with the sufficiency of the convergence of the series (1.6) for the existence of (1.7).

H. DELANGE ([1], [2]) has given two different proofs for this theorem. The first is analytic and makes use of deep Tauberian theorems; the second is elementary but rather difficult, it is based on Selberg's sieve method. In what follows we give a third very simple and elementary proof.

This proof is based on the inequality: *If $f(n)$ is a strongly additive number theoretical function,*

$$(1.9) \quad A(N) = \sum_{p \leq N} \frac{f(p)}{p}$$

and

$$(1.10) \quad B^2(N) = \sum_{p \leq N} \frac{|f(p)|^2}{p}$$

then

$$(1.11) \quad \frac{1}{N} \sum_{n=1}^N |f(n) - A(N)|^2 \leq C_1 B^2(N)$$

where C_1 is a positive constant, not depending on the function $f(n)$.

We shall call (1.11) the *Turán—Kubilius inequality*, because the inequality (1.10) was proved by J. KUBILIUS ([3], p. 35, Lemma 3.1.) by generalizing an earlier inequality of P. TURÁN ([4]).

Let us note that the Turán—Kubilius inequality has an obvious probabilistic interpretation. Let us consider the finite probability space P_N consisting of the first N positive integers, these being supposed to be equiprobable. A strongly additive function $f(n)$ can be considered as a random variable on P_N and can be represented in the form

$$(1.12) \quad f(n) = \sum_{p \leq N} \varepsilon_p(n) f(p) \quad (n = 1, 2, \dots, N)$$

where

$$(1.13) \quad \varepsilon_p(n) = \begin{cases} 1 & \text{if } p|n \\ 0 & \text{if } p \nmid n. \end{cases}$$

(Here and in what follows $p|n$ denotes that p is a divisor of n and $p \nmid n$ that p does not divide n .) Clearly *)

$$\frac{1}{N} \sum_{m=1}^N f(m) = \sum_{p \leq N} f(p) \frac{1}{N} \left[\frac{N}{p} \right] = \sum_{p \leq N} \frac{f(p)}{p} + O\left(\frac{B(N)}{\sqrt{\log N}} \right).$$

*) $[x]$ denotes the integral part of x .

Thus (1. 11) can be written also in the equivalent form

$$(1. 11') \quad \frac{1}{N} \sum_{n=1}^N \left| f(n) - \frac{1}{N} \sum_{m=1}^N f(m) \right|^2 \leq C_2 B^2(N)$$

where C_2 is an absolute constant. As clearly the variance of the random variable $\varepsilon_p(n)$ on P_N is equal to $\frac{1}{p} \left(1 - \frac{1}{p}\right) + O\left(\frac{1}{N}\right)$, if the random variables $\varepsilon_p(n)$ ($p \leq N$) were pairwise independent, then the variance of the sum $f(n) = \sum_{p \leq N} \varepsilon_p(n) f(p)$ would be exactly equal to the sum of the variances of the summands; now while the variables $\varepsilon_p(n)$ are not exactly independent, their dependence is rather weak, and this is reflected in (1. 11') which says (for real valued f) that the variance (on P_N) of the sum $f(n) = \sum_{p \leq N} \varepsilon_p(n) f(p)$ is less than an absolute constant multiplied by the sum of the variances of the terms of this sum.

The importance of the theorem of Delange is shown by the remark, that it implies one of the main theorems of the statistical theory of additive number theoretic functions, namely the theorem of P. ERDŐS and A. WINTNER [5]. Recently in [6] we gave a new proof of this theorem by the standard methods of analytic number theory. When writing the paper [6] we were unaware of the fact that there exists such a simple proof of the theorem of Delange as presented below. After having obtained such a proof, the simplest way to obtain the Erdős—Wintner theorem is that through the theorem of Delange. This way of obtaining the Erdős—Wintner theorem is much simpler than that given in [6]. Let us mention that recently a quite different approach to the Erdős—Wintner theorem has been given by E. NOVOSELOV ([7]).

§ 2. Proof of Delange's theorem by the Turán—Kubilius inequality

Let us mention first that it is very easy to see (see [1]) that if $g_1(n)$ and $g_2(n)$ are strongly multiplicative functions, such that $|g_1(n)| \leq 1$ and $|g_2(n)| \leq 1$ ($n = 1, 2, \dots$) and if

$$g_1(p) = g_2(p)$$

except for $p \in P$ where P is a set of primes such that $\sum_{p \in P} \frac{1}{p} < +\infty$, then if $M(g_2)$ exists, so does $M(g_1)$ and if the formula (1. 8) holds for $g = g_2$ it holds for $g = g_1$ too. As further it follows from the convergence of the series (1.6) and the condition (1. 5) that the series *)

$$(2. 1) \quad \sum_p \frac{1 - \Re(g(p))}{p}$$

*) $\Re(z)$ denotes the real part of the complex number z .

is convergent too and its terms are nonnegative, and consequently the series

$$(2.2) \quad \sum_{\Re(g(p)) \leq \frac{1}{2}} \frac{1}{p}$$

is convergent too, we may suppose that

$$(2.3) \quad \Re(g(p)) > \frac{1}{2}$$

for all primes p , because if there would be primes p for which $\Re(g(p)) \leq \frac{1}{2}$, we could, in view of the convergence of the series (2.2) change the value of $g(p)$ for these primes (to 1 say) so that (2.3) should be satisfied for all primes p . From now on we shall therefore suppose that (2.3) holds for all primes p . Let us put

$$(2.4) \quad |g(p)| = r(p) \quad \text{and} \quad \arg g(p) = \vartheta(p)$$

where $-\pi < \vartheta(p) \leq +\pi$, i. e. we suppose that $g(p) = r(p)e^{i\vartheta(p)}$. It follows easily from the convergence of the series (1.6) and the condition (2.3) that the series with positive terms

$$(2.5) \quad \sum_p \frac{\log \frac{1}{r(p)}}{p}$$

$$(2.6) \quad \sum_p \frac{\log^2 r(p)}{p}$$

$$(2.7) \quad \sum_p \frac{\vartheta^2(p)}{p}$$

are convergent and the series

$$(2.8) \quad \sum_p \frac{\vartheta(p)}{p}$$

is convergent (however the series (2.8) is in general not absolutely convergent).

Let us define the strongly multiplicative function $g_N(n)$ by putting

$$(2.9) \quad g_N(p) = \begin{cases} g(p) & \text{if } p \leq \log N \\ 1 & \text{if } p > \log N. \end{cases}$$

By other words we put for any natural number n

$$(2.10) \quad g_N(n) = \prod_{\substack{p|n \\ p \leq \log N}} g(p)$$

Let us put further

$$(2.11) \quad h_N(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g_N(d)$$

where d runs over all (positive) divisors of n and $\mu(n)$ is the Möbius function. Then $h_N(n)$ is also a multiplicative function, (but not strongly multiplicative, because $h_N(p) = g_N(p) - 1$ and $h_N(p^2) = 0$ for $\alpha \geq 2$).

It is easy to see that

$$(2.12) \quad g_N(n) = \sum_{d|n} h_N(d)$$

and the series $\sum_{n=1}^{\infty} \frac{h_N(n)}{n}$ is convergent and we have

$$(2.13) \quad \sum_{n=1}^{\infty} \frac{h_N(n)}{n} = \prod_{p \leq \log N} \left(1 + \frac{g(p)-1}{p} \right).$$

We have clearly in view of (2.12)

$$(2.14) \quad \frac{1}{N} \sum_{n=1}^N g_N(n) = \frac{1}{N} \sum_{d=1}^N h_N(d) \left[\frac{N}{d} \right] = \sum_{d=1}^{\infty} \frac{h_N(d)}{d} + R_N$$

where *)

$$(2.15) \quad |R_N| \leq \frac{1}{N} \sum_{d=1}^{\infty} |h_N(d)| \leq \frac{1}{N} \prod_{p \leq \log N} (1 + |g(p)-1|) \leq \frac{2^{\pi(\log N)}}{N}$$

and thus

$$(2.16) \quad \lim_{N \rightarrow \infty} R_N = 0$$

As further

$$(2.17) \quad \lim_{N \rightarrow \infty} \prod_{p \leq \log N} \left(1 + \frac{g(p)-1}{p} \right) = \prod_p \left(1 + \frac{g(p)-1}{p} \right)$$

the convergence of the infinite product on the right of (2.17) (extended over all primes p) being a consequence of the convergence of the series (1.6), we have proved that

$$(2.18) \quad \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N g_N(n) = \prod_p \left(1 + \frac{g(p)-1}{p} \right).$$

Thus in order to prove (1.7) it is sufficient to show that putting

$$(2.19) \quad D_N = \frac{1}{N} \sum_{n=1}^N (g(n) - g_N(n))$$

we have

$$(2.20) \quad \lim_{N \rightarrow \infty} D_N = 0.$$

Now we clearly have

$$(2.21) \quad D_N = \frac{1}{N} \sum_{n=1}^N g_N(n) \left(\prod_{\substack{p|n \\ p > \log N}} g(p) - 1 \right)$$

and thus, putting

$$(2.22) \quad f_N(n) = \sum_{\substack{p|n \\ p > \log N}} \log g(p)$$

*) $\pi(x)$ denotes as usual the number of primes $p \leq x$.

we have

$$(2.23) \quad D_N \leq \frac{1}{N} \sum_{n=1}^N |e^{f_N(n)} - 1|$$

Now we need the simple inequality

$$|e^z - 1| \leq |z|$$

valid for $\Re(z) \leq 0$, which can be proved e. g. as follows

$$|e^z - 1| = \left| \int_0^z e^{\zeta} d\zeta \right| \leq \int_0^{|z|} dx = |z|.$$

It follows, in view of $\Re(f_N(n)) \leq 0$

$$(2.24) \quad D_N \leq \frac{1}{N} \sum_{n=1}^N |f_N(n)|.$$

By Cauchy's inequality we get

$$(2.25) \quad D_N^2 \leq \frac{1}{N} \sum_{n=1}^N |f_N(n)|^2.$$

Now evidently $f_N(n)$ is a strongly additive function, and thus, in view of the inequality $|a+b|^2 \leq 2(|a|^2 + |b|^2)$

$$(2.26) \quad \frac{1}{N} \sum_{n=1}^N |f_N(n)|^2 \leq \frac{2}{N} \sum_{n=1}^N \left| f_N(n) - \sum_{p \leq N} \frac{f_N(p)}{p} \right|^2 + 2 \left| \sum_{p \leq N} \frac{f_N(p)}{p} \right|^2.$$

As regards the second term on the right of (2.26) we have

$$\left| \sum_{p \leq N} \frac{f_N(p)}{p} \right|^2 = \left| \sum_{\log N < p \leq N} \frac{\log r(p)}{p} \right|^2 + \left| \sum_{\log N < p \leq N} \frac{\theta(p)}{p} \right|^2$$

and therefore in view of the convergence of the series (2.5) and (2.8) we have

$$(2.27) \quad \lim_{N \rightarrow \infty} \left| \sum_{p \leq N} \frac{f_N(p)}{p} \right|^2 = 0.$$

On the other hand, we can apply to the first term on the right of (2.25) the Turán-Kubilius inequality, and obtain

$$\frac{1}{N} \sum_{n=1}^N \left| f_N(n) - \sum_{p \leq N} \frac{f_N(p)}{p} \right|^2 \leq C_1 \cdot \sum_{p \leq N} \frac{|f_N(p)|^2}{p} = C_1 \left(\sum_{\log N < p \leq N} \frac{\log^2 r(p) + \theta^2(p)}{p} \right).$$

In view of the convergence of the series (2.6) and (2.7) it follows that

$$(2.28) \quad \lim_{N \rightarrow \infty} \frac{2}{N} \sum_{n=1}^N \left| f_N(n) - \sum_{p \leq N} \frac{f_N(p)}{p} \right|^2 = 0.$$

Thus we obtain from (2.25), (2.26), (2.27) and (2.28) that (2.20) holds. In view of what has been said above, this completes the proof of the theorem of Delange

References

- [1] H. DELANGE, Sur les fonctions arithmétiques multiplicatives, *Ann. Sci. École Norm. Sup.* **78** (1961), 273–304.
- [2] H. DELANGE, Application de la methode du crible à l'étude des valeurs moyennes de certaines fonctions arithmétiques, *Seminaire Delange-Pisot* (mimeographed lecture notes), Paris, 1962.
- [3] I. KUBILIUS, Probabilistic methods in the theory of numbers, *Amer. Math. Soc. Translations of Mathematical Monographs. Vol. 11* (1964), 1–182.
- [4] P. TURÁN, Über einige Verallgemeinerungen eines Satzes von Hardy und Ramanujan, *J. London Math. Soc.* **11** (1936), 125–133.
- [5] P. ERDŐS—A. WINTNER, Additive arithmetic functions and statistical independence, *Amer. J. Math.* **61** (1939), 713–721.
- [6] A. RÉNYI, On the distribution of values of additive number-theoretical functions, *Publ. Math. Debrecen* **10** (1963), 264–273.
- [7] E. V. NOVOSELOV, A new method in probabilistic number theory (in Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **28** (1964), 307–364.

210

NOTE

Dispensing with the analytic part of his paper No. 210 and introducing further simplifications, in this paper he arrives at the simplest proof known of Delange's theorem. It somewhat resembles in principle to the procedure followed by Kubilius in Chapter 4 of his book *Probabilistic Methods in the Theory of Numbers*.

This method turned out to be very useful for certain generalizations of Delange's theorem (J. Galambos, *J. London Math. Soc.* (2), **2** (1970), 405–419, K.—H. Indlekofer, *Journ. für die reine und angew. Math.* **256** (1972), 180–184. and via characteristic function, for Erdős—Wintner type theorems on the distribution of additive functions (J. Galambos, *Z. für Wahrscheinlichkeitstheorie und verw. Geb.*, (18), **4** (1971), 261–270) and in a refined form Kátai (*Acta Math. Hung.*, **20** (1969), 69–87).

Delange (*Proc. Amer. Math. Soc.*, **18** (1967), 743–749), too, simplified his own proof, making it completely elementary. Wirsing (*Acta Math. Hung.*, **18** (1967), 411–467) developed a very complicated elementary method that yielded the first deep results also for zero mean values and G. Halász (*ibid.*, **19** (1968), 365–403) returning to analytic tools, gave the necessary and sufficient condition for the existence of a (zero or non-zero) mean value. (G.H.)

ON A PROBLEM OF GRAPH THEORY

by

P. ERDŐS¹, A. RÉNYI¹ and V. T. SÓS²

§ 0. Introduction

Let G_n be a non-directed graph having n vertices, without parallel edges and slings. Let the vertices of G_n be denoted by $P_1, \dots, P_n$. Let $v(P_i)$ denote the valency of the point P_i and put

$$(0.1) \quad V(G_n) = \max_{1 \leq i \leq n} v(P_i).$$

Let $E(G_n)$ denote the number of edges of G_n . Let $H_d(n, k)$ denote the set of all graphs G_n for which $V(G_n) = k$ and the diameter $D(G_n)$ of which is $\leq d$, ($k = 1, 2, \dots, n-1$; $d = 2, 3, \dots, n-1$).

In the present paper we shall investigate the quantity

$$(0.2) \quad F_d(n, k) = \min_{G_n \in H_d(n, k)} E(G_n).$$

Thus we want to determine the minimal number N such that there exists a graph having n vertices, N edges and diameter $\leq d$ and the maximum of the valencies of the vertices of the graph is equal to k .

To help the understanding of the problem let us consider the following interpretation. Let be given in a country n airports; suppose we want to plan a network of direct flights between these airports so that the maximal number of airports to which a given airport can be connected by a direct flight should be equal to k (i.e. the maximum of the capacities of the airports is prescribed), further it should be possible to fly from every airport to any other by changing the plane at most $d-1$ times; what is the minimal number of flights by which such a plan can be realized? For instance, if $n=7$, $k=3$, $d=2$ we have $F_2(7, 3)=9$ and the extremal graph is shown by Fig. 1.

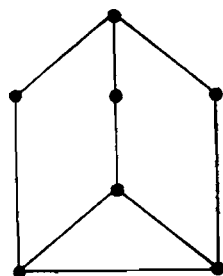


Fig. 1

The problem of determining $F_d(n, k)$ has been proposed and discussed recently by two of the authors (see [1]). In § 1 we give a short summary of the results of the paper [1], while in § 2 and 3 we give some new results which go beyond those of [1]. Incidentally we solve a long-standing problem about the maximal number of edges of a graph not containing a cycle of length 4.

In § 4 we mention some unsolved problems.

Let us mention that our problem can be formulated also in terms of 0–1 matrices as follows: Let $M = (\varepsilon_{ij})$ be a symmetrical n by n zero-one matrix such

¹ Mathematical Institute of the Hungarian Academy of Sciences.

² Eötvös L. University, Budapest.

that $\varepsilon_{ii} = 1$, $\max_{1 \leq i \leq n} \sum_{j=1}^n \varepsilon_{ij} = k+1$ and all elements of M^d are ≥ 1 . We want to determine

$$M_d(n, k) = \min \sum_{i=1}^n \sum_{j=1}^n \varepsilon_{ij}.$$

Clearly

$$(0.3) \quad M_d(n, k) = 2F_d(n, k) + n.$$

This formulation shows the connection of our problem with non-linear programming.

We give for the case $d=2$ a third formulation of our problem which displays its connection with the theory of block designs.

Let be given a sequence $A_1, A_2, \dots, A_n$ of subsets of the elements $1, 2, \dots, n$ such that if $j \in A_i$ then $i \in A_j$. Let us suppose that denoting by $|A|$ the cardinal number of the set A , we have $\max_{1 \leq j \leq n} |A_j| = k$. Let us suppose that for any i ($1 \leq i \leq n$) and any $j \neq i$ such that $j \notin A_i$ there is a set A_h which contains both i and j (this is equivalent by our supposition of symmetry to the statement that the sets A_i and A_j are not disjoint). The problem is to determine

$$(0.4) \quad \min \sum_{i=1}^n |A_i| = 2F_2(n, k).$$

§ 1. Some Basic Inequalities, and some Asymptotic Results

It is easy to see that if there exists a graph G_n with $V(G_n) = k$ and diameter $\leq d$, then

$$(1.1) \quad n \leq 1 + k \frac{(k-1)^d - 1}{k-2}.$$

(1.1) can be proved as follows: if $V(G_n) = k$ the number of points which can be reached from a given point, say, P_1 by an edge is $\leq k$; the number of points which can be reached from P_1 by a path of length 2 is $\leq k(k-1)$ and finally the number of points which can be reached by a path of length d is $\leq k(k-1)^{d-1}$. Thus if the graph has diameter $\leq d$ we have

$$(n-1) \leq k(1 + (k-1) + (k-1)^2 + \dots + (k-1)^{d-1}).$$

This proves (1.1). If both n and k are odd, then G_n must contain at least one point of valency $\leq k-1$ (because the number of points of odd valency cannot be odd); thus in this case we get

$$(1.2) \quad n \leq 1 + (k-1) \frac{(k-1)^d - 1}{k-2}.$$

Note that for the graph shown by Fig. 1, equality stands in (1.2). For the graph shown on Fig. 2 (the so-called Petersen-graph) equality stands in (1.1) with $n=10$, $k=3$, $d=2$.

As regards $F_d(n, k)$ we obtain easily the lower bound

$$(1.3) \quad F_d(n, k) \cong \frac{n(n-1)(k-2)}{2((k-1)^d - 1)}.$$

(1.3) can be proved as follows: every edge is itself a path of length 1; it can be contained in at most $2(k-1)$ paths of length 2, but in this way each path of length 2 is counted twice, thus the number of paths of length 2 cannot exceed $E(G_n)(k-1)$. In general each edge can be contained in at most $3(k-1)^2$ paths of length 3, but in this way each path of length 3 is counted three times, thus the number of paths of length 3 cannot exceed $E(G_n)(k-1)^2$, etc. As in case G_n has diameter

$\leq d$ the number of paths of length $\leq d$ has to be at least $\binom{n}{2}$, we obtain

$$(1.4) \quad E(G_n)(1 + (k-1) + \dots + (k-1)^{d-1}) \cong \binom{n}{2},$$

which implies (1.3). Note that one has equality in (1.4) for the Petersen graph shown on Fig. 2., further for $n=5$, $k=2$, $d=2$ because a cycle of length 5 has 5 vertices, each of which has valency 2, it has diameter 2 and the number of its edges is $5 = \frac{5 \cdot 4}{2 \cdot 2}$.

It is clear from the above proof that one can have equality in (1.4) only for a regular graph of order k , i. e. if $E(G_n) = \frac{nk}{2}$ and if any two points are joined by one and only one path of length $\leq d$.

The first condition implies that if equality stands in (1.4) then there is equality in (1.1) too. For the case $d=2$ this means that a necessary condition of equality in (1.4) is $n = k^2 + 1$. It has been shown by A. J. HOFFMAN and R. R. SINGLETON [4] that a regular graph of order k , having $k^2 + 1$ points and diameter 2 exists only for $k=2, 3, 7$ and perhaps for $k=57$. Thus for $d=2$ except for these values of k one has strict inequality in (1.3). However it has been shown in [1] that there exists an infinite sequence of pairs (k_j, n_j) such that $k_j \rightarrow \infty$, $n_j \rightarrow \infty$ and

$$(1.5) \quad \lim_{j \rightarrow \infty} \frac{F_2(n_j, k_j) k_j}{n_j(n_j - 1)} = \frac{1}{2}.$$

This is a consequence of the following

THEOREM 1. *If P is any prime power, there exists a graph G_n of order $n = P^2 + P + 1$ for which $V(G_n) = P + 1$, which has diameter 2 and for which $E(G_n) \leq \frac{1}{2}(n^{3/2} + n)$. The graph G_n has also the property that it does not contain any cycle of length 4.*

To make this paper self-contained we reproduce the proof of Theorem 1 given in [1].

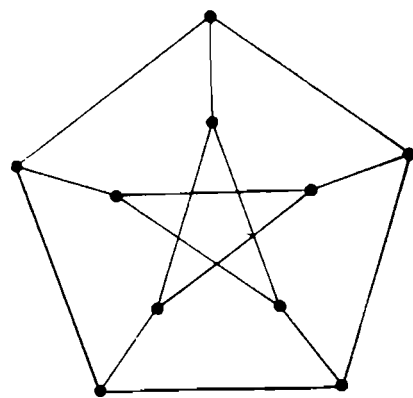


Fig. 2

PROOF OF THEOREM 1. Let $GF(P)$ be the Galois field with P elements. Let us represent the points of the finite plane geometry $PG(P, 2)$ by triples (a, b, c) where a, b, c are elements of $GF(P)$, not all three equal to 0, and $(\lambda a, \lambda b, \lambda c)$ with $\lambda \in GF(P)$, $\lambda \neq 0$ represents the same point as (a, b, c) . The number of different points of $PG(P, 2)$ is $P^2 + P + 1$. A straight line in $PG(P, 2)$ is the set of all points (x, y, z) which satisfy the equation $ax + by + cz = 0$; we denote this line by $[a, b, c]$. The point (a, b, c) and the line $[a, b, c]$ are clearly conjugate elements with respect to the conic $x^2 + y^2 + z^2 = 0$. As well known there are $P + 1$ points on each line, any two different lines have exactly one point in common and through any two given points there is exactly one straight line. Now we define the mapping T which maps the point $A = (a, b, c)$ into the line $\alpha = [a, b, c]$ and conversely. We write $TA = \alpha$, $T\alpha = A$. This mapping has evidently the properties: if the point B lies on the line $\alpha = TA$ then the point A lies on the line $\beta = TB$; if C is the point of intersection of the lines TA and TB then TC is identical with the line passing through the points A and B ; $A = (a, b, c)$ is on TA if and only if $a^2 + b^2 + c^2 = 0$, i.e. if A lies on the conic $x^2 + y^2 + z^2 = 0$. Now let us define a graph G_n ($n = P^2 + P + 1$) as follows: the vertices of G_n are the points of $PG(P, 2)$; the vertices $A = (a, b, c)$ and $A' = (a', b', c')$ are joined in G_n by an edge if and only if A' is lying on TA (and thus A is lying on TA'). Clearly a vertex A in G_n has the valency P or $P + 1$ according to whether A is on the conic $x^2 + y^2 + z^2 = 0$ or not.* Thus

$$(1.6) \quad \frac{1}{2} (n^{3/2} - n) \leq \frac{1}{2} P(P^2 + P + 1) \leq E(G_n)$$

and

$$E(G_n) \leq \frac{1}{2} (P + 1)(P^2 + P + 1) \leq \frac{1}{2} (n^{3/2} + n).$$

Finally the diameter of G_n is equal to 2. As a matter of fact any two points A and B can be joined by the path ACB where C is the point of intersection of the lines TA and TB . Besides this A and B can be joined by a single edge if A lies on TB . But the point C such that the edges AC and BC both belong to G_n is in any case unique; thus G_n does not contain any cycle of length 4.

Thus our Theorem is proved.

We deduce from Theorem 1 the following corollaries.

COROLLARY 1. Put $n_k = k^2 - k + 1$; then

$$(1.7) \quad \liminf_{k \rightarrow \infty} \frac{F_2(n_k, k)k}{n_k(n_k - 1)} = \frac{1}{2}.$$

* If P is prime, there are $P + 1$ points on the conic and thus

$$E(G_n) = \frac{P(P + 1)^2}{2} > \frac{1}{2} n^{3/2} \quad \text{if } n \geq n_0.$$

PROOF OF COROLLARY 1. By (1. 3)

$$(1. 8) \quad \frac{F_2(n, k)k}{n(n-1)} \cong \frac{1}{2}$$

further if $k = P + 1$, $n_k = P^2 + P + 1$, by Theorem 1

$$(1. 9) \quad F_2(P^2 + P + 1, P + 1) \leq \frac{1}{2} (P + 1)(P^2 + P + 1);$$

thus in this case

$$(1. 10) \quad \frac{F_2(n_k, k)k}{n_k(n_k-1)} \leq \frac{1}{2} \left(1 + \frac{1}{P} \right);$$

this proves our assertion.

Theorem 1 enables us also to solve — at least asymptotically — a problem which was raised by one of us 27 years ago (see [2]).*

Let $\mathbf{C}_n$ denote the class of graphs having n vertices and containing no cycle of order 4. Put

$$(1. 11) \quad \mu(n) = \max_{G_n \in \mathbf{C}_n} E(G_n).$$

The problem is to determine the value of $\mu(n)$. From Theorem 1 we deduce the following

COROLLARY 2. We have

$$(1. 12) \quad \lim_{n \rightarrow \infty} \frac{\mu(n)}{n^{3/2}} = \frac{1}{2}.$$

PROOF OF COROLLARY 2. It follows clearly from Theorem 1 that if P is a prime power, then putting $n = P^2 + P + 1$

$$(1. 13) \quad \mu(n) \cong \frac{1}{2} (n^{3/2} - n).$$

It is possible that for these n the graph of Theorem 1 is extremal but we cannot prove this. Clearly $\mu(n)$ is an increasing function of n , and thus it follows that for any n we have

$$(1. 14) \quad \mu(n) \cong \frac{1}{2} [P^2 + P + 1)^{3/2} - (P^2 + P + 1)]$$

where P is the largest prime power such that $P^2 + P + 1 \leq n$. Now evidently for $n \geq n_1$ one can choose a prime p so that

$$(1. 15) \quad \sqrt[n]{n} - \frac{\sqrt[n]{n}}{\log n} \leq p \leq \sqrt[n]{n} - 1$$

* After having written this paper we have been informed by W. G. BROWN that independently of us he has proved (1.12), in the same way as we did. His paper will be published in the Bulletin of the Canadian Mathematical Society.

which implies for $n \geq n_1$

$$n \left(1 - \frac{2}{\log n} \right) \leq p^2 + p + 1 \leq n.$$

Thus we have for any $n \geq n_1$

$$(1.16) \quad \mu(n) \leq \frac{1}{2} n^{3/2} \left(1 - \frac{3}{\log n} \right)$$

and thus

$$(1.17) \quad \liminf_{n \rightarrow \infty} \frac{\mu(n)}{n^{3/2}} \geq \frac{1}{2}.$$

On the other hand it is easy to see (this follows also from the results of I. REIMAN in [3]) that

$$(1.18) \quad \limsup_{n \rightarrow \infty} \frac{\mu(n)}{n^{3/2}} \leq \frac{1}{2}.$$

As a matter of fact, let G_n be a graph containing no cycle of order 4. Let $P_1, P_2, \dots, P_n$ be the vertices of G_n and let us denote their valencies by $v_1, v_2, \dots, v_n$. Now clearly one can select from the set E_i of vertices joined by an edge to P_i $\binom{v_i}{2}$ pairs, and no pair (P_j, P_h) can be contained in both E_i and E_l with $l \neq i$ because otherwise $P_i P_j P_l P_h$ would be a cycle contained in G_n . Thus we must have

$$(1.19) \quad \sum_{i=1}^n \binom{v_i}{2} \leq \binom{n}{2}.$$

Now we have

$$(1.20) \quad \left(\sum_{i=1}^n v_i \right)^2 \leq n \sum_{i=1}^n v_i^2$$

and thus

$$(1.21) \quad \left(\sum_{i=1}^n v_i \right)^2 - n \left(\sum_{i=1}^n v_i \right) \leq 2n \sum_{i=1}^n \binom{v_i}{2} \leq 2n \binom{n}{2} \leq n^3.$$

As clearly $\sum_{i=1}^n v_i = 2E(G_n)$, we have

$$(1.22) \quad 4E^2(G_n) - 2nE(G_n) \leq n^3$$

which implies

$$(1.23) \quad E(G_n) \leq \frac{n^{3/2}}{2} \sqrt{1 + \frac{1}{4n}} + \frac{n}{4}.$$

Thus

$$(1.24) \quad \frac{\mu(n)}{n^{3/2}} \leq \frac{1}{2} \sqrt{1 + \frac{1}{4n}} + \frac{1}{4\sqrt{n}}.$$

which implies (1.18). Thus Corollary 2 is proved.

Let us note that weaker results have been obtained previously by E. KLEIN (see [2]) and I. REIMANN [3], who proved $\liminf_{n \rightarrow \infty} \frac{\mu(n)}{n^{3/2}} \cong \frac{1}{2\sqrt{2}}$. REIMANN's extremal graph does not contain triangles either; it is possible that among such graphs it is optimal.

Note that for the pairs (n_j, k_j) for which according to Corollary 1 one has

$$(1.25) \quad \lim_{j \rightarrow \infty} \frac{F_2(n_j, k_j) k_j}{n_j(n_j - 1)} = \frac{1}{2}$$

one has $k_j \sim \sqrt{n_j}$. It was shown in [1] that there exists another sequence of pairs (k_j, n_j) such that

$$(1.26) \quad \lim_{j \rightarrow \infty} \frac{F_2(n_j, k_j) k_j}{n_j(n_j - 1)} = 1$$

but for this sequence of pairs one has $\lim_{j \rightarrow \infty} \frac{k_j^2}{n_j} = +\infty$.

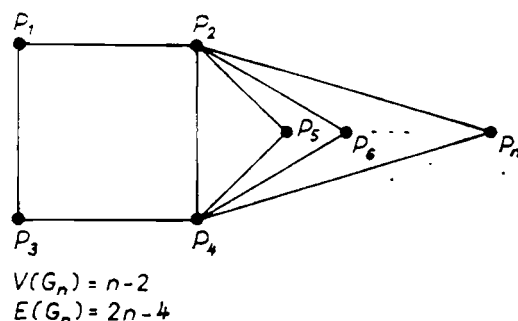
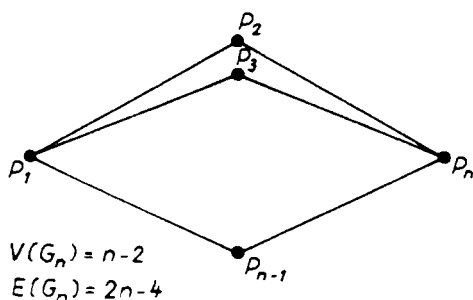
It remains an open question what is the value of the function $g(c)$ defined by

$$(1.27) \quad g(c) = \liminf_{\substack{k^2 > nc \\ n \rightarrow \infty}} \frac{F_2(n, k)k}{n(n-1)}$$

for $1 < c < +\infty$; we know only that $g(c)$ is nondecreasing. $\frac{1}{2} \cong g(c)$ and $\lim_{c \rightarrow \infty} g(c) \cong 1$.

§ 2. Some Exact Results for $d=2$.

In this § we deal with the exact value of $F_2(n, k)$ for $\frac{n}{2} \leq k \leq n-1$. Evidently, $F_2(n, n-1) = n-1$, because the graph G_n in which one vertex is joined by an edge with all others, has diameter 2, further $V(G_n) = n-1$ and $E(G_n) = n-1$. It has been shown in [1] that $F_2(n, n-2) = 2n-4$ (a graph G_n with $V(G_n) = n-2$ and $E(G_n) = 2n-4$ and having the diameter 2 is shown by Fig. 3; another graph with the same properties is shown by Fig. 4), further that $F_2(n, n-3) = F_2(n, n-4) = 2n-5$. (The corresponding extremal graphs are shown by Figs. 5 and 6.)



We shall prove now

THEOREM 2. We have for $n \geq 13$

$$(2.1) \quad F_2(n, k) = 2n - 4 \quad \text{for} \quad \frac{2n-2}{3} \leq k \leq n-5.$$

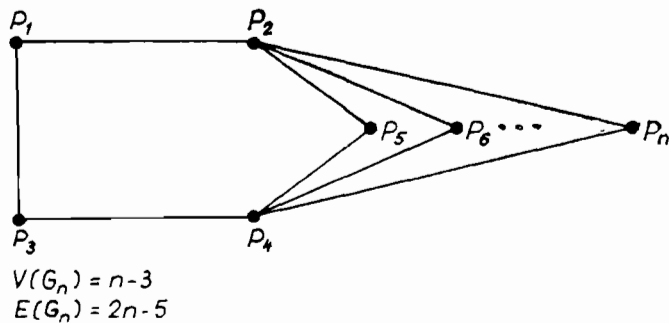


Fig. 5

PROOF OF THEOREM 2. The extremal graph G_n with

$$\tilde{V}(G_n) = k = n-l, \quad \left(5 \leq l \leq \frac{n+2}{3} \right)$$

and $E(G_n) = 2n-4$ and having diameter 2 is exhibited by Fig. 7.

$$V(G_n) = n-l, \quad E(G_n) = 2n-4, \quad 5 \leq l \leq \frac{n+2}{3}; \quad n \geq 13.$$

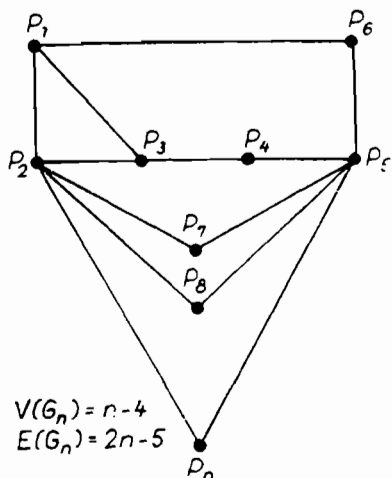


Fig. 6

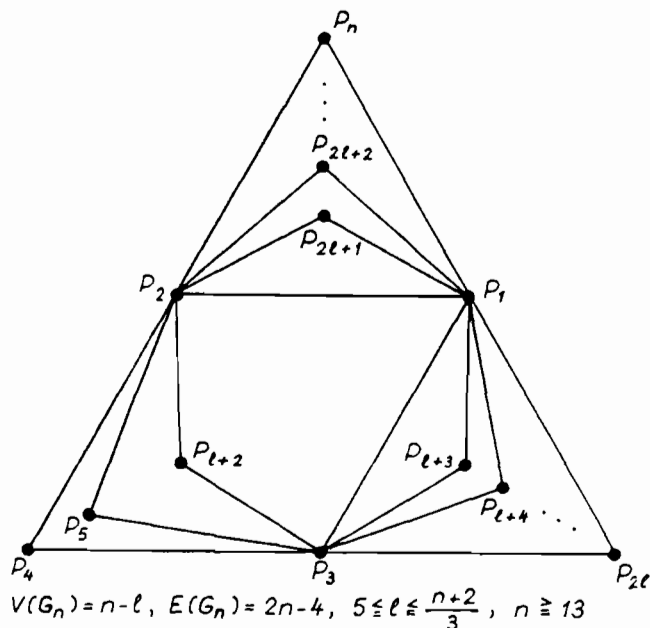


Fig. 7

Note that all vertices of G_n except P_1, P_2 and P_3 have the valency 2, further $v(P_1) = n - l$, $v(P_2) = n - l$, $v(P_3) = 2l - 2$ and by supposition $2l - 2 \leq n - l$. Thus $V(G_n) = n - l$. Clearly G_n has diameter 2 and the number of edges of G_n is

$$E(G_n) = \frac{2(n-l) + 2l - 2 + 2(n-3)}{2} = 2n - 4.$$

We prove that for any G_n with $n \geq 13$, $V(G_n) = n - l \left(5 \leq l \leq \frac{n+2}{3} \right)$ and diameter 2 one has $E(G_n) \geq 2n - 4$.

As $E(G_n) = \frac{1}{2} \sum_{i=1}^n v(P_i)$ we may suppose that G_n contains at least one point of degree ≤ 3 . If G_n would contain no point of degree ≤ 2 , then let us choose a point of degree 3; let this point be P_1 . Let the points connected by an edge with P_1 be denoted by P_2, P_3 and P_4 . As every point can be reached from P_1 by a path of length ≤ 2 , we must have $v(P_2) + v(P_3) + v(P_4) \geq n - 1$.

Now if there would be a point among the points $P_5, \dots, P_n$ which would be connected with more than one of the points P_2, P_3, P_4 we would have $v(P_2) + v(P_3) + v(P_4) \geq n$; as all other points have degree ≥ 3 it would follow

$$\sum_{i=1}^n v(P_i) \geq n + 3(n-3) = 4n - 9$$

and thus $E(G_n) > 2n - 5$ i.e. $E(G_n) \geq 2n - 4$, which was to be proved. Thus we may suppose that all points P_i ($5 \leq i \leq n$) are connected with one and only one of P_2, P_3 and P_4 ; similarly we can suppose that P_2, P_3 and P_4 are not connected with each other because this would again imply $v(P_2) + v(P_3) + v(P_4) \geq n$ and thus $E(G_n) \geq 2n - 4$. If there is at least one among the P_i with $5 \leq i \leq n$ which has degree > 3 , it again follows that $E(G_n) \geq 2n - 4$. If however all have degree 3, let us suppose that $v(P_2) = \min(v(P_2), v(P_3), v(P_4))$ which implies $v(P_2) \leq \frac{n-1}{3}$. Let P_5 be connected with P_2 . Then $v(P_5) = 3$ and let the three points connected with P_5 be P_2, P_i and P_j ; clearly $i > 5$ and $j > 5$. But then $v(P_2) + v(P_i) + v(P_j) \geq n - 1$ and thus

$$6 = v(P_i) + v(P_j) \geq \frac{2(n-1)}{3}$$

that is $n \leq 10$.

As we supposed $n \geq 13$, this case is settled.

The case when there is a point P_i of valency 1 is easily settled, because if this point is P_1 , and P_1 is connected with P_2 only, then P_2 has to be connected with the remaining $n - 2$ points too, and thus would have valency $n - 1$. Thus the only case which remains to be settled is when $\min_{1 \leq i \leq n} v(P_i) = 2$. Suppose $v(P_1) = 2$ and let P_1 be connected with P_2 and P_3 . Then all remaining points have to be connected either with P_2 or with P_3 or with both.

Let $\mathbf{C}_1$ denote the class of points P_i with $i \geq 4$ connected only with P_2 , and c_1 the number of elements of $\mathbf{C}_1$; let $\mathbf{C}_2$ be the class of points P_i with $i \geq 4$ connected only with P_3 and c_2 the number of elements of $\mathbf{C}_2$; finally let $\mathbf{C}_3$ be the class of points connected with both P_2 and P_3 , and c_3 the number of elements of $\mathbf{C}_3$. Clearly

$c_1 + c_2 + c_3 = n - 3$. As the valency of P_3 cannot exceed $n - l$ and P_3 is connected with every point in G_n except itself and the points in $\mathbf{C}_1$, we have $c_1 \cong l - 2 \cong 3$. Similarly $c_2 \cong l - 2 \cong 3$.

The number of edges in G_n the existence of which is already established is clearly $c_1 + c_2 + 2c_3 + 2 = n + c_3 - 1$. Let us call these the edges of the first kind, and the remaining edges those of the second kind. As the graph has diameter 2, every point of $\mathbf{C}_1$ has to be connected by a path of length ≤ 2 with every point of $\mathbf{C}_2$. Such a path can not contain an edge of the first kind. Thus the graph G' consisting of the edges of the second kind has to be connected. Now three cases are possible. Either G' contains besides the points of $\mathbf{C}_1$ and $\mathbf{C}_2$ at least one further point from the class $\mathbf{C}_3$; in this case it contains at least $c_1 + c_2 + 1$ points and thus there are at least $c_1 + c_2$ edges of the second kind, and thus the total number of edges is $E(G_n) \cong n + c_3 - 1 + c_1 + c_2 = 2n - 4$. Or P_2 and P_3 are connected by an edge; in this case we get again $E(G_n) \cong 2n - 4$. Or P_2 and P_3 are not connected and G' consists only of the points of $\mathbf{C}_1$ and $\mathbf{C}_2$. In this case the connected graph G' is either a tree or not. If it is not a tree, it contains at least $c_1 + c_2$ edges and thus we obtain again $E(G_n) \cong 2n - 4$. If G' is a tree, it must have at least two end-points. We may suppose that $\mathbf{C}_1$ contains an endpoint of G' . Let x be the total number of end-points of G' in $\mathbf{C}_1$. Then the sum of valencies (in G') of the points of $\mathbf{C}_1$ is at least $x + 2(c_1 - x)$. As G_n has diameter 2 and P_2 and P_3 are not directly connected, any endpoint of G' in $\mathbf{C}_1$ has to be connected by a path of length 2 to P_3 , it follows that for every endpoint P of G' in $\mathbf{C}_1$ the single edge starting from P ends in $\mathbf{C}_2$. Let y denote the number of points in $\mathbf{C}_2$ which are connected with an endpoint of G' in $\mathbf{C}_1$. If Q is such a point, clearly Q has to be connected with every other point of $\mathbf{C}_2$, because otherwise there would not exist a path of length 2 from P to these points. Now clearly no point of $\mathbf{C}_2$ can be an endpoint of G' , because it must be connected to at least one point in $\mathbf{C}_1$ and also to Q . Thus the sum of valencies in G' of the points of $\mathbf{C}_2$ is at least $2(c_2 - y) + y(c_2 - 1) + x$. It follows that the number of edges of the second kind is at least

$$\frac{1}{2} (x + 2(c_1 - x) + 2(c_2 - y) + y(c_2 - 1) + x) = c_1 + c_2 + y \left(\frac{c_2 - 3}{2} \right) \cong c_1 + c_2,$$

because, as we have shown, $c_2 \cong 3$.

Thus we have shown that $E(G_n) \cong 2n - 4$ and the proof of Theorem 2 is complete.

Note that the restriction $n \cong 13$ in Theorem 2 is necessary, because for $n < 13$ there is no value of k between $\frac{2n-2}{3}$ and $n-5$.

As regards the value of $F_2(n, k)$ for $k < \frac{2n-2}{3}$ we can show that for $n \cong 15$

$$(2.2) \quad F_2(n, k) = \begin{cases} 3n - k - 6 & \text{for } \frac{3n-3}{5} \leq k < \frac{2n-2}{3} \\ 5n - 4k - 10 & \text{for } \frac{5n-3}{9} \leq k < \frac{3n-3}{5} \\ 4n - 2k - 13 & \text{for } \frac{n+1}{2} \leq k < \frac{5n-3}{9}. \end{cases}$$

We give in what follows the extremal graphs for these 3 cases. That these are really extremal can be proved in a way similar to the proof of Theorem 2, therefore we leave the details to the reader.

THE EXTREMAL GRAPH FOR $\frac{3n-3}{5} \leq k < \frac{2n-2}{3}$.

The graph has four points of high degree; let us denote them by A, B, C, D and four groups of points.

There is a group denoted by AB , the points of which are joined to A and to B . The group contains $2k-n$ points. In the group BCD (connected with B, C and D) there are $n-k-1$ points. In the group AC (whose points are connected with A and C) there are $\left\lfloor \frac{n-k-3}{2} \right\rfloor$ points; finally in the group AD (the points of which are connected with A and D) there are $n-k-3 - \left\lfloor \frac{n-k-3}{2} \right\rfloor$ points. Further the graph contains the edges AB, AC, AD . The points A and B have the degree k . The whole graph has $3n-k-6$ edges.

THE EXTREMAL GRAPH FOR $\frac{5n-3}{9} \leq k < \frac{3n-3}{5}$.

There are 5 points of high order, A, B, C, D, E .

The group AB has $2k-n$ points,

The group BCD has $\left\lfloor \frac{n-k-1}{2} \right\rfloor$ points.

The group BCE has $n-k-1 - \left\lfloor \frac{n-k-1}{2} \right\rfloor$ points.

The group AC has $2k-n$ points.

The group ADE has $2n-3k-4$ points.

Further the edges AB, AC, AD, AE, DE belong to the graph. The points A, B and C have the valency $n-k$; the total number of edges is $5n-4k-10$.

THE EXTREMAL GRAPH FOR $\frac{n+1}{2} \leq k < \frac{5n-3}{9}$.

There are 6 points of high order, A, B, C, D, E, F .

The group AB contains $2k-n$ points.

The group BCE contains $\left\lfloor \frac{n-k-1}{2} \right\rfloor$ points.

The group BDF contains $n-k-1 - \left\lfloor \frac{n-k-1}{2} \right\rfloor$ points.

The group ADC contains $\left\lfloor \frac{n-k-5}{2} \right\rfloor$ points.

The group AEF contain $n-k-5 - \left\lfloor \frac{n-k-5}{2} \right\rfloor$ points.

The graph contains further the edges AB, AC, AD, AE, AF . The graph has $4n-2k-13$ edges.

For $k < \frac{n+1}{2}$ we cannot determine $F_2(n, k)$ exactly. However, we can get a fairly good upper bound by constructing graphs of diameter 2 by the following principles. We divide all but $\binom{r}{2}$ of the points of a graph G_n into r groups of approximately the same size. We connect the points of each pair of groups with one of the remaining points, and connect as many of these points with each other

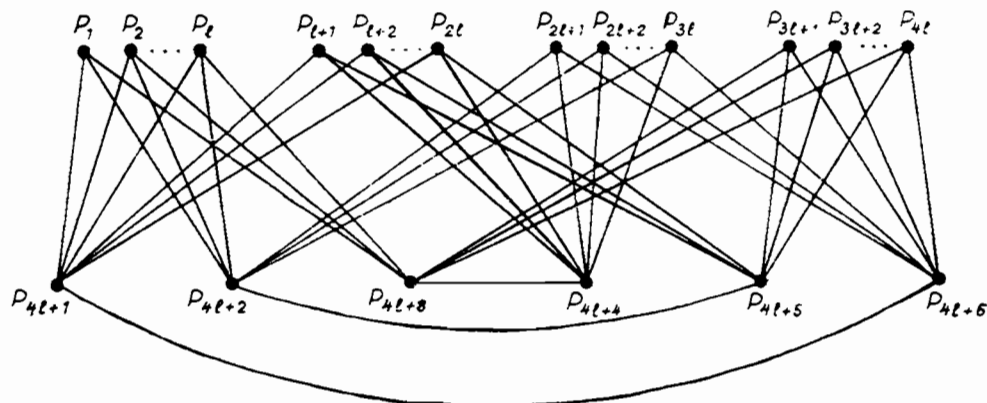


Fig. 8

as needed. For instance if $r = 4$, $n = 4l + 6$, we put l points in each of 4 groups, connect each of the 6 pairs of groups with one of the remaining 6 points, and connect each of these points with that point which is connected with the other two groups. The graph obtained is shown by Fig. 8. It follows that

$$(2.3) \quad F_2(4l+6, 2l+1) \leq 12l+3.$$

§ 3. Some Results for $d \geq 3$.

We prove first

THEOREM 3. We have for every n , every $k \leq n-1$ and $d \geq 3$

$$(3.1) \quad F_d(n, k) \geq \frac{n^2}{k^{d-1}} \left(1 - 4 \sqrt[3]{\frac{n}{k^d}} \right).$$

PROOF OF THEOREM 3. Let us put

$$(3.2) \quad \delta = 4 \sqrt[3]{\frac{n}{k^d}}.$$

Clearly we may suppose $\delta < 1$, because otherwise (3.1) is trivially fulfilled. We have evidently

$$(3.3) \quad \delta > \frac{4}{k^{d/3}}.$$

We may suppose $n > k^{d-1}$, because any graph G_n with diameter $\leq d$ is connected and thus has at least $n-1$ edges; thus $F_3(n, k) \geq n-1$ and if $n \leq k^{d-1}$ the inequality (3.1) is trivial. Thus we have to prove (3.1) only for $k^{d-1} < n < \frac{k^d}{64}$ i.e. for $(64n)^{1/d} < k < n^{1/d-1}$. *

Let G_n be a graph having n vertices, diameter d and such that $V(G_n) = k$. Let us denote by $X_1, \dots, X_s$ those vertices of G_n the valency of which is $< \frac{4n}{k^{d-1}\delta}$; let $Y_1, \dots, Y_{n-s}$ be the remaining vertices of G_n . We have clearly

$$(3.4) \quad E(G_n) = \frac{1}{2} \left(\sum_{i=1}^s v(X_i) + \sum_{j=1}^{n-s} v(Y_j) \right) > \frac{2(n-s)n}{k^{d-1}\delta}.$$

Thus if

$$s \leq n \left(1 - \frac{\delta(1-\delta)}{2} \right)$$

we have

$$(3.5) \quad E(G_n) \geq \frac{n^2}{k^{d-1}} (1-\delta).$$

Thus we have to consider only the case

$$(3.6) \quad s > n \left(1 - \frac{\delta(1-\delta)}{2} \right).$$

We distinguish two cases. Either every X_i ($1 \leq i \leq s$) is connected with at least $\left(1 - \frac{\delta}{2}\right) \frac{n}{k^{d-1}}$ of the vertices Y_j , or not. In the first case we have

$$(3.7) \quad E(G_n) \geq s \left(1 - \frac{\delta}{2} \right) \frac{n}{k^{d-1}} \geq (1-\delta) \frac{n^2}{k^{d-1}}.$$

Thus we may suppose that there is an X_i — say X_1 — which is connected with less than $\left(1 - \frac{\delta}{2}\right) \frac{n}{k^{d-1}}$ Y_j -s. We shall show that this case is impossible. By supposition we can reach, starting from X_1 , every vertex of G by a path of length $\leq d$. Let us consider first those paths starting from X_1 , the next vertex of which is an Y_j . As Y_j can be chosen in $< \left(1 - \frac{\delta}{2}\right) \frac{n}{k^{d-1}}$ ways, and all vertices of G_n have valency $\leq k$, the number of such pathes is at most

$$(3.8) \quad \left(1 - \frac{\delta}{2} \right) \frac{n}{k^{d-1}} (1 + (k-1) + (k-1)^2 + \dots + (k-1)^{d-1}) \leq \left(1 - \frac{\delta}{2} \right) n.$$

* We may also suppose that $k > 64$.

Let us count now the pathes of length $\leq d$ starting from X_1 , on which the point next to X_1 , is an X_i . The number of such pathes is clearly at most

$$(3.9) \quad \frac{4n}{k^{d-1}\delta} \left(1 + \frac{4n}{k^{d-1}\delta} (1 + (k-1) + \dots + (k-1)^{d-2}) \right) < \frac{\delta n}{3}.$$

It follows from (3. 8) and (3. 9) that the total number of vertices which can be reached from X_1 by a path of length $\leq d$, can not exceed $n \left(1 - \frac{\delta}{6} \right)$ which is $\leq n-2$ if $n \geq \frac{12}{\delta}$, and this is true if $n-1 \geq k \geq 64$; thus we arrived to a contradiction and this proves our theorem.

To show that the order of magnitude $\frac{n^2}{k^2}$ of the lower estimate of $F_3(n, k)$ is best possible, consider the following graph G_n : Take a complete graph G_r having r vertices, and connect each vertex of G_r with $r-1$ new points. Thus we obtain a graph G_n with $r(r-1) + r = r^2 = n$ vertices. Clearly one has $k = V(G_n) = 2r-2$, $D(G_n) = 3$ and $E(G_n) = \frac{3}{2} r(r-1)$. Thus $E(G_n) \sim \frac{6n^2}{k^2}$.

In this example $k = 2(\sqrt{n} - 1)$; by slightly modifying this example we obtain that

$$F_3(n, k) < \frac{n^2}{k^2} (c+1)^2 \left(\frac{1}{2} + \frac{1}{c} \right)$$

if $k \sim cn$ where $0 < c < 1$.

To show that $F_3(n, k)$ is of order of magnitude $\frac{n^2}{k^2}$ for $k \sim \lambda\sqrt{n}$ where $0 < \lambda < 1$ we have to apply a more involved construction. Let us consider a graph G_n which has the vertices P_{gij} where $1 \leq g \leq l$, $1 \leq i \leq s$, $1 \leq j \leq s$ and the vertices Q_{ghi} where $1 \leq g < h \leq l$ and $1 \leq i \leq s$; thus $n = ls^2 + \left(\frac{l}{2}\right)s$. Suppose that the edges of G_n are as follows:

- P_{gij} and P_{hij} are both connected with Q_{ghi} for $1 \leq g < h \leq l$, $i, j = 1, 2, \dots, s$.
- Q_{ghi_1} is connected with Q_{ghi_2} for $1 \leq i_1 \leq s$, $1 \leq i_2 \leq s$, $i_1 \neq i_2$, $1 \leq g < h \leq l$;
- $Q_{g_1h_1i}$ and $Q_{g_2h_2i}$ are connected for $1 \leq g_1 < h_1 \leq l$ and $1 \leq g_2 < h_2 \leq l$, $i = 1, 2, \dots, s$.

Clearly

$$E(G_n) = 2 \binom{l}{2} s^2 + \binom{l}{2} \binom{s}{2} + \left(\binom{l}{2} \right) s$$

further $v(P_{gij}) = s-1$ and

$$v(Q_{ghi}) = s + l - 1 + \binom{l}{2} - 1$$

and thus $V(G_n) = s + l + \binom{l}{2} - 2$. Thus we obtain

$$F_3 \left(ls^2 + \binom{l}{2} s, s + l + \frac{(l+1)l(l-1)(l-2)}{8} - 2 \right) \leq 2 \binom{l}{2} s^2 + \binom{l}{2} \binom{s}{2} + \binom{l}{2} s.$$

By other words by choosing for l an arbitrary fixed natural number and for s tending to $+\infty$, we obtain an infinite sequence of pairs n, k such that

$$k \sim \frac{\sqrt[3]{n}}{\sqrt{l}} \quad \text{and} \quad F_3(n, k) \leq \frac{5}{4} \frac{n^2}{k^2} l(l-1).$$

Thus for arbitrary small $\lambda > 0$ there exists an infinity of pairs n, k such that $k \sim \lambda \sqrt[3]{n}$ and

$$F_3(n, k) < \frac{5}{4\lambda^4} \cdot \frac{n^2}{k^2}.$$

Let us study now the behaviour of $F_3(n, k)$ for large values of k . Clearly $F_3(n, k) = n - 1$ if $k \geq \frac{n}{2}$ because the graph G_n shown on Fig. 9 has diameter 3 $V(G_n) = k$ and G_n is a tree, thus it has $n - 1$ edges; this result is best possible because a connected graph G_n cannot have less than $n - 1$ edges.

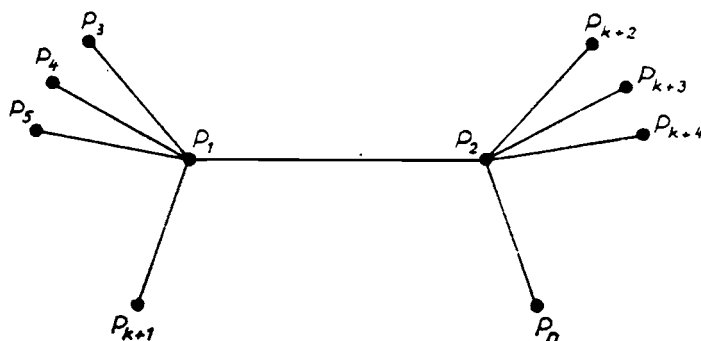


Fig. 9

We prove now the following

THEOREM 4. If $\frac{n}{s+1} + s - 1 \leq k \leq \frac{n}{s} + s - 2$ where $s = 1, 2, 3, \dots, \left\lceil \sqrt[3]{\frac{n}{2}} \right\rceil$ then

$$F_3(n, k) = n + \binom{s}{2} - 1.$$

PROOF OF THEOREM 4. The case $s = 1$ has been settled above. Let us consider first the case $s = 2$. Suppose G_n would be a tree of diameter 3 and $V(G_n) = k \leq \frac{n}{2}$, and let P_1 be an endpoint of G_n (such a point exists as every tree has at least two

endpoints). Let P_2 denote the single point connected with P_1 by an edge, and let $P_3, \dots, P_l$ be all the other points connected with P_2 ; as $V(G_n) = k$ we have $l \leq k+1$. The remaining $n-k-1 \geq k-1 \geq l-2$ points have to be connected with one of the points $P_3, \dots, P_l$ because otherwise it would be impossible to reach them from P_1 by a path of length ≤ 3 . But they can not be all connected with the same point P_j ($3 \leq j \leq l$) because this point would have valency $> k$. Let P_r and P_s be two points ($l < r < s \leq n$) such that P_r is connected with P_i and P_s with P_j ($3 \leq i < j \leq l$). Then the (unique) path from P_r to P_s has length 4; this contradiction shows that $F_3(n, k) \geq n$ for $k \leq \frac{n}{2}$.

On the other hand Fig. 10 shows a graph G_n with $V(G_n) = k$ where $\frac{n}{3} + 1 \leq k \leq \frac{n}{2}$ which has diameter 3 and contains exactly one cycle (a triangle) and thus $E(G_n) = n$. This completes the proof of the fact that $F_3(n, k) = n$ for $\frac{n}{3} + 1 \leq k \leq \frac{n}{2}$.

Note that for $n = 2k + 1$ there is another extremal graph G_{2k+1} of diameter 3, for which $V(G_{2k+1}) = k$ and $E(G_{2k+1}) = 2k + 1$, shown by Fig. 11.

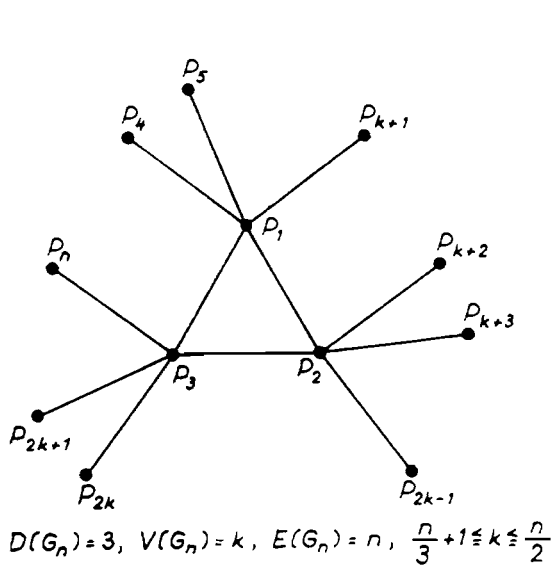


Fig. 10

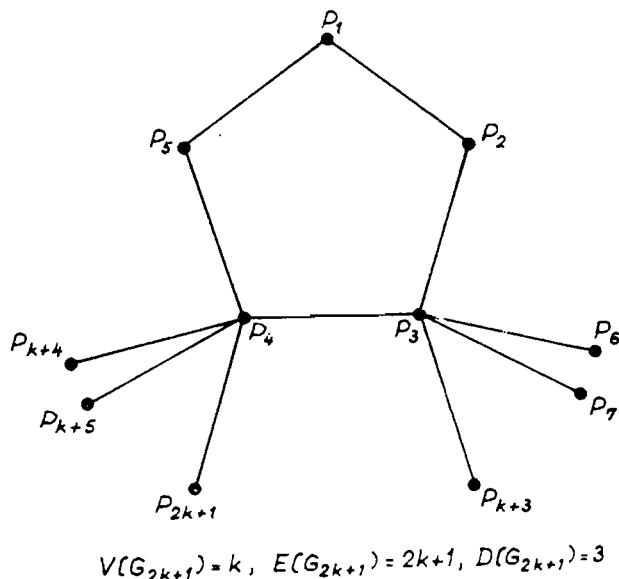


Fig. 11

Now we pass to the case $s \geq 3$.

Let G_n be a graph with $V(G_n) = k$ $\left(\frac{n}{s+1} + s - 1 \leq k \leq \frac{n}{s} + s - 2; s < \sqrt[3]{\frac{n}{2}} \right)$ and $D(G_n) = 3$. Let $X_1, \dots, X_l$ be the endpoints of G_n . As the remaining $n-l$ points all have valency ≥ 2 , and at least one among them has valency k , we have

$$E(G_n) \geq \frac{1}{2} (l + k + 2(n-l-1)) = n - \frac{l}{2} + \frac{k}{2} - 1.$$

Now if $E(G_n) \geq n + \binom{s}{2} - 1$, we have nothing to prove; if however $E(G_n) < n + \binom{s}{2} - 1$ we get

$$l > k - s(s-1) \geq s-1$$

thus $l \geq 2$. Let $Y_1, \dots, Y_v$ denote those vertices of G_n which are connected with at least one X_j ($1 \leq j \leq l$).

Clearly Y_i and Y_j are connected by an edge ($1 \leq i < j \leq v$) because otherwise there would not exist a path of length 3 connecting the X_h -s. Thus it is sufficient to consider the case $v \leq s$, because every connected graph G_n containing a complete $s+1$ -graph has at least $n-1 + \binom{s}{2}$ edges. Let us suppose therefore that $v \leq s$.

We prove first that $v \geq s$. Let the endpoint X_1 be connected to Y_1 . Let $Z_1, \dots, Z_r$ denote all the points connected with Y_1 which are not endpoints of G_n . As every point of G_n can be reached from X_1 by a path of length ≤ 3 , if Y_1 is connected with p endpoints then we have $\sum_{h=1}^r v(Z_h) \geq n-p-1$ thus

$$E(G_n) \geq \frac{1}{2} (n-p-1 + p+r+l + 2(n-l-r-1)) = \frac{3n-3}{2} - \frac{r+l}{2}$$

thus in case $E(G_n) < n + \binom{s}{2} - 1$ we get

$$l \geq n-r-s(s-1).$$

As however each Y_j has valency $\leq k$, it can be connected to at most k of the X_i -s, and Y_1 only to $k-r$ X_i -s; thus

$$(v-1)k + k - r \geq n - r - s(s-1)$$

and therefore, in view of $s \leq \sqrt[3]{\frac{n}{2}}$, we obtain $v > s-1$ i.e. $v \geq s$. Thus we have only

to consider the case $v=s$. Now if $v=s$ there exist in G_n at least s points which are not connected to any of the Y_j -s because these have valencies $\leq k$ and thus the total number of points connected with them is $\leq s(k-(s-1)) \leq n-s$. Let W be such a point.

Now clearly W has to be connected with each X_h by a path of length 3 and therefore with each Y_j by a path of length 2. Let $U_1, \dots, U_t$ be the points connected with W , then each Y_j is connected with some U_z . Thus it follows

$$\begin{aligned} E(G_n) &\geq \frac{1}{2} (2l + s(s-1) + 2s + 2t + 2(n-l-s-t-1)) = \\ &= l + \binom{s}{2} + s + t + n - l - s - t - 1 = n + \binom{s}{2} - 1. \end{aligned}$$

Thus $F_3(n, k) \geq n + \binom{s}{2} - 1$. On the other hand consider the graph G_n of the following structure: let us take a complete graph G_{s+1} having $s+1$ points, and connect

each of these points except one with $k-s$ endpoints, and the last with $n-s(k-s)-(s+1)$ points. (Clearly $0 \leq n-s(k-s)-(s+1) \leq k-s$).

Thus we obtain a graph G_n with $V(G_n)=k$, $D(G_n)=3$ and $E(G_n)=n+\binom{s}{2}-1$.

This completes the proof of Theorem 4.

Let us consider now $F_4(n, k)$. Clearly

$$F_4(n, k) = n-1 \quad \text{if } k \geq \sqrt[4]{n-1}.$$

This can be seen as follows. Fig. 12 exhibits a tree of diameter 4 showing that $F_4(k^2+1, k) = k^2$

Clearly if $(k-1)^2+1 < n < k^2+1$, we obtain a graph G_n exhibiting $F_4(n, k) = n-1$ by omitting from the graph on Fig. 12 k^2+1-n endpoints. We shall prove now

THEOREM 5.

$$F_4(k^2+2, k) \geq k^2+1 + \frac{1}{2} \sqrt[4]{k} \quad (k=2, 3, \dots).$$

PROOF OF THEOREM 5. Let G_{k^2+2} be an extremal graph i.e. one which has k^2+2 points, diameter 4, satisfies the condition $V(G_{k^2+2})=k$ and has $F_4(k^2+2, k)$ edges.

Let $X_1, \dots, X_m$ be the points of G_{k^2+2} having valency ≥ 2 , and let G_m^* be the subgraph of G_{k^2+2} spanned by these points. We assert that each point X_i has the valency ≥ 2 in G_m^* too. Suppose that X_1 is an endpoint of G_m^* , and that X_2 is the only point of G_m^* to which X_1 is connected. Clearly X_1 is connected with at least one endpoint Y_1 of G_{k^2+2} because it has valency ≥ 2 in G_{k^2+2} , thus it is connected with some point of G_{k^2+2} different from X_2 and this point cannot be in G_m^* and

thus is an endpoint of G_{k^2+2} . Every point of G_{k^2+2} can be reached by supposition from Y_1 by a path of length ≤ 4 . However the number of points which can be reached from Y_1 by such a path is clearly

$$\leq 2k-1 + (k-1)^2 = k^2$$

which is a contradiction. Thus in G_m^* each point has valency ≥ 2 . As the diameter of G_m^* is ≤ 4 , it follows from (1.1) that G_m^* contains at least one point of valency $\sqrt[4]{m-1}$; thus the number of edges of G_m^* exceeds $(m-1) \div \frac{1}{2} (\sqrt[4]{m-1})$. Each point in G_m^* can be connected with at most $k-2$ endpoints of G_{k^2+2} thus $k^2+2 \leq m + m(k-2) = m(k-1)$ and therefore $m \geq \frac{k^2+2}{k-1} \geq k+1$; thus

$$E(G_{k^2+2}) \geq k^2+1 + \frac{1}{2} (\sqrt[4]{m-1}) \geq k^2+1 + \frac{1}{2} \sqrt[4]{k}.$$

Thus Theorem 5 is proved.

Note that the statement of Theorem 5 is trivial for $k \leq 16$, because it states only what we know already that if $D(G_{k^2+2}) = 4$ then G_{k^2+2} can not be a tree.

To get an upper estimate for $F_4(k^2+2, k) - k^2$ consider the following graph. Take a graph G_{k+5} with $V(G_{k+5}) = k$, $D(G_{k+5}) = 2$ and $E(G_{k+5}) = 2k+6$; such a graph exists according to Theorem 2 if $k \geq 8$ (see Fig. 7 with $l=5$). This graph has $k+2$ points of valency 2. Connect k out of these points with $k-2$ new points each and one with $k-3$ new points. Thus we get a graph G_n with $n = k^2+2$ points, such that $V(G_n) = k$, $D(G_n) = 4$ and $E(G_n) = k^2 + k + 3$. Thus

$$F_4(k^2+2, k) \leq k^2 + k + 3.$$

§ 4. Some further Remarks and Unsolved Problems

First we formulate some general principles of construction which were implicitly used above.

If G_n is a graph of diameter d , and such that $V(G_n) = k$, then if G_n is not regular, we may construct from G_n a graph G_N of order $N = n + kn - E(G_n)$ with $V(G_N) = k$ and diameter $d+2$, by connecting each vertex P_i of G_n which has valency $v(P_i) < k$ with $k - v(P_i)$ new points. Thus

$$(4.1) \quad F_{d+2}(n + kn - 2F_d(n, k), k) \leq kn - F_d(n, k).$$

For instance we have shown that $F_2(n, n-5) = 2n-4$. It follows immediately from (4.1) that

$$F_4(n^2 - 8n + 8, n-5) \leq n^2 - 7n + 4.$$

Notice that for each value of d , the extremal graphs G_n with $V(G_n) = k$, $D(G_n) = d$ and having a minimal number of edges, are trees if k is sufficiently large, $k \geq U_d(n)$ say.

We have implicitly shown that

$$(4.2) \quad U_2(n) = n - 1$$

$$(4.3) \quad U_3(n) = \frac{n}{2}$$

$$(4.4) \quad U_4(n) = \sqrt{n-1}.$$

It can be shown that

$$(4.5) \quad U_5(n) = \frac{1 + \sqrt{2n-3}}{2}$$

further that for any fixed $s \geq 3$ and $n \rightarrow \infty$

$$(4.6) \quad U_{2s}(n) \sim \sqrt[s]{n}$$

and

$$(4.7) \quad U_{2s+1}(n) \sim \sqrt[s]{\frac{n}{2}}.$$

The extremal tree of diameter $2s$ has a center, while the extremal tree of diameter $2s+1$ has a central edge.

Notice that if k decreases by one below the critical value $U_d(n)$, i.e. to $U_d(n) - 1$, there is a considerable increase in the value of $F_d(n, k)$ if d is even, but not if d is odd. As a matter of fact

$$F_2(n, U_2(n) - 1) - F_2(n, U_2(n)) = (2n - 4) - (n - 1) = n - 3$$

$$F_3(2k + 1, k) - F_3(2k + 1, k + 1) = (2k + 1) - 2k = 1$$

and

$$F_3(2k + 2, k) - F_3(2k + 2, k + 1) = (2k + 3) - (2k + 1) = 2$$

further as proved by Theorem 5

$$F_4(k^2 + 2, k) - F_4(k^2 + 1, k) \cong \frac{1}{2} \sqrt[4]{k}.$$

The situation is similar for $d > 4$.

We call attention to the following problems, left open in this paper:

PROBLEM 1. Is the graph of Theorem 1 extremal in the sense that among all graphs with n vertices and not containing any cycle of length 4 does it have the maximal number of edges? (We have proved only that it is asymptotically extremal.)

We can prove the following result, which is connected with Problem 1.

THEOREM 6. If G_n is a graph in which any two points are connected by a path of length 2 and which does not contain any cycle of length 4, then $n = 2k + 1$ and G_n consists of k triangles which have one common vertex (see Fig. 13).

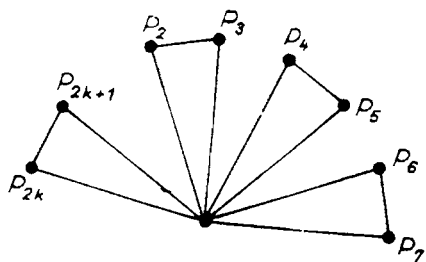


Fig. 13

PROOF OF THEOREM 6. Let G_n be a graph with the required properties. Let P_1 be a point of G_n having maximal valency. If P_1 is connected with all the remaining points of G_n then evidently these have to be connected by pairs, and G_n is of the type described in Theorem 6. Thus we may suppose that G_n contains at least one point P_2 which is not connected with P_1 . It is easy to see that in this case $V(P_2) = V(P_1)$.

As a matter of fact there is a point P_3 in G_n which is connected with both P_1 and P_2 . As there must be a path of length 2 between P_1 and P_3 there is a point P_4 which is connected with both P_1 and P_3 . As there has to be a path of length 2 between P_2 and P_3 , there is a point P_5 connected with both P_2 and P_3 , which is clearly different from P_1, P_2, P_3 and P_4 . Let $Q_1, Q_2, \dots, Q_{k-2}$ be the remaining points (besides P_3 and P_4) which are connected with P_1 . Clearly P_2 and P_5 are not among the Q_i ; we have $k \geq 4$ because $v(P_3) \geq 4$ and by supposition P_1 has the maximal valency.

Now from each of the points Q_i there is a path of length 2 to P_2 ; thus for each Q_i ($i = 1, 2, \dots, k - 2$) there exists a point R_i which is connected with both Q_i and P_2 . Clearly $R_i \neq R_j$ if $i \neq j$ because otherwise G_n would contain the cycle $P_1 Q_i R_i Q_j$. Further R_i is different from P_3 because if R_i would be identical with P_3 G_n would contain the cycle $P_1 Q_i P_3 P_4$. Finally R_i is different from P_5 because otherwise G_n

would contain the cycle $P_1 Q_i P_3 P_4$. Thus $v(P_2) \cong k$ and as $k = V(G_n)$ we obtain $v(P_2) = k = v(P_1)$. Thus any point of G_n which is not connected with P_1 has the valency $k = v(P_1)$. Repeating the same argument with P_2 instead of P_1 it follows that $v(Q_i) = k$ ($i = 1, 2, \dots, k-2$). As P_3 is not connected with Q_1 (because otherwise G_n would contain the cycle $P_1 Q_1 P_3 P_4$) repeating the same argument for Q instead of P_1 it follows that $v(P_3) = k$. Thus the graph G_n is regular.

Now if $V(P_i) = k$ ($i = 1, 2, \dots, n$) and G_n does not contain a cycle of length 4 and between any two points there is a path of length 2, then clearly if S_i denotes the set of points connected with P_i then the sets S_i and S_j have exactly one point in common, and for any two points P_i and P_j ($j \neq i$) there is exactly one point P_h such that S_h contains both P_i and P_j . Thus if we define the sets of points S_i as lines we obtain a finite plane geometry, with $k = P + 1$ points on a line, and thus having $n = P^2 + P + 1$ points. But then in this geometry there would exist a one-to-one mapping between points and lines such that no line contains the point corresponding to it, and such a mapping is known [5] to be impossible. This proves Theorem 6.

PROBLEM 2. To determine the exact value of $F_2(n, k)$ for $k < \frac{n}{2}$, or at least the asymptotic value of $F_2(n, [nc])$ with $0 < c < \frac{1}{2}$.

PROBLEM 3. Is the lower estimate in Theorem 3 asymptotically best possible, i.e. do there exist for each $d \cong 3$ a sequence of graphs G_n ($n \rightarrow \infty$) with $V(G_n) = k \sim cn^{\frac{1}{d-1}}$ where $c > 0$ is a constant, $D(G_n) = d$ and $E(G_n) \sim \frac{n^2}{k^{d-1}} \sim \frac{n}{c^{d-1}}$?

PROBLEM 4. Determine asymptotically $F_4(k^2 + 2, k) - k^2$.

Problems similar to those considered in this paper can be asked for directed graphs. We hope to return to these problems in an other paper.

REFERENCES

- [1] ERDŐS, P.—RÉNYI, A.: On a problem in the theory of graphs (in Hungarian, with English and Russian summaries), *Publ. Math. Inst. Hung. Acad. Sci.* 7/A (1962) 623—641.
- [2] ERDŐS, P.: On sequences of integers no one of which divides the product of two others and on some related problems, *Mitteilungen des Forschungsinstitutes für Math. und Mechanik, Tomsk*, 2 (1938) 74—82.
- [3] REIMAN, I.: Über ein Problem von K. Zarankiewicz, *Acta Math. Acad. Sci. Hung.* 9 (1958) 269—278.
- [4] HOFFMAN, A. J.—SINGLETON, R. R.: On Moore graphs with diameter 2 and 3, *IBM Journal of Research and Development* 4 (1960) 497—504.
- [5] BAER, R.: Polarities in finite projective planes, *Bulletin of the American Math. Soc.* 52 (1946) 77—93.

NOTE

If we fix the number n of vertices and the diameter (maximal distance) $d = 2$ of a graph and ask what is the minimum of the number of edges, the answer is trivial. It is given by a "star". It has a vertex with valency $n - 1$, thus the question, what happens if the valency is bounded, is natural. The first results are given in No. 201. These results are improved in No. 260. The case $d > 2$ is also considered. Bollobás [1] solved Problem 2 of No. 260 showing that $n/c < F_2(n, [cn]) < (1/c + (1/c)^{5/8})n$, so that n/c is the order of magnitude of $F_2(n, [cn])$. There are given some stronger but more complicated lower bounds for $F_2(n, k)$ for various values of n and k . As regards $d > 2$, the following results are obtained in [1]:

$$F_3(n, c \sqrt[n]{n}) < (2/c^2 + 1)n \quad (c > 2)$$

$$F_3(n, [c \sqrt[n]{n}]) < 6n/c^2 \quad (0 < c < 2)$$

$$k^2 + \sqrt[k]{k}/2 \leq F_4(k^2 + 2, k) \leq k^2 + k.$$

For directed graphs the original question without bounds on the valency is not trivial. Katona and Szemerédi [2] proved that the number of edges in a directed graph of n vertices is $\geq \frac{1}{2} n \log n$ if there is a directed path of length ≤ 2 between any two vertices. $n\{\log n\}$ can be constructed.

Some related results are contained in [3], [4] and [5].

Theorem 6 of No. 260 became famous as "friendship theorem": If there are n people, every pair (of different people) has exactly one common friend, then there is a man being the friend of everybody. This is strongly connected with the concept of strongly regular graphs introduced by R. C. Bose [6]. We say that a regular graph is strongly regular if to each pair of different joined vertices there are exactly p_1 vertices which are connected with both of them, and to each pair of different nonjoined vertices there are exactly p_2 such vertices. In Theorem 6 of No. 260 the regularity is not assumed, but the other assumptions of strongly regular graphs are with $p_1 = p_2 = 1$. New proofs of this "friendship theorem" are given by Higman [7] and Wilf [8]. Longyear and Parsons gave an elementary proof [9].

Bose and Shrikhande [10] generalized the problem. They considered the case $p_1 = p_2 = d$. They proved that the regularity follows if $d \geq 2$, and constructed some strongly regular graphs with these parameters.

In [9] a result of Ryser [11] is deduced from the "friendship theorem". This result characterizes the families of subsets $A_1, \dots, A_m$ with the following three properties:

1. If $x \in \bigcup_{i=1}^m A_i$, then x is contained in at least 2 of A_i 's.
2. If $i \neq j$, $|A_i \cap A_j| \leq 1$.
3. If $i \neq j$, then there is a unique k , such that $A_i \cap A_k \neq \emptyset$, $A_j \cap A_k \neq \emptyset$.

Recently Vera T. Sós and E. Fried observed [12] that the weakly associative lattices correspond to a "directed friendship theorem". The problem in directed graph terminology is the following. Let G be a directed graph, $V = V(G)$ its set of vertices, $E = E(G)$ its set of edges where E contains all the loops (a, a) with $a \in V$ and some of the ordered pairs (a, b) with $a, b \in V$ so that $a \neq b$,

$(a, b) \in E$ implies $(b, a) \notin E$. Moreover for any $a, b \in V$, $a \neq b$ there exists exactly one $x \in V$ and exactly one $y \in V$ such that (a, x) , (b, x) , (y, a) and (y, b) belong to E . If G has these properties, then either the vertices as points and the sets $A_x = \{x; (a, x) \in E\}$ as lines form a projective plane or G has two exceptional elements (0 and 1) such that consists of all the pairs of form (a, a) , $(1, 0)$, $(0, a)$, $(a, 1)$ ($a \in V$).

[13] is an expository paper on this field showing the connections with finite geometries and block designs. [Gy. K.]

REFERENCES

- [1] Bollobás, B.: Graphs with given diameter and maximal valency and with a minimal number of edges. *Combinatorial Math. its Appl. (Proc. Conf. Oxford 1969)*, Academic Press, London 1971, 25–37.
- [2] Katona, G. and Szemerédi, E.: On a problem of graph theory. *Studia Sci. Math. Hung.*, **2** (1967), 23–28.
- [3] Glivjak, F., Kys, P. and Plesnik, J.: On the extension of graphs with a given diameter without superfluous edges. *Mat. Časopis Sloven. Akad. Vied*, **19** (1969), 92–101.
- [4] Glivjak, F., Kys, P. and Plesnik, J.: On irreducible graphs of diameter two without triangles. *Mat. Časopis Sloven. Akad. Vied*, **19** (1969), 149–157.
- [5] Glivjak, F. and Pesnik, J.: On the existence of certain graphs with diameter two. *Mat. Časopis Sloven. Akad. Vied*, **19** (1969), 276–282.
- [6] Bose, R. C.: Strongly regular graphs. *Pac. J. Math.*, **13** (1963), 389–419.
- [7] Higman, G.: *Lecture given at Conference on Combinatorial Mathematics*. Oxford, 1969.
- [8] Wilf, M. S.: The friendship theorem. *Comb. Math. and its Appl.* Ed. D. J. A. Welsh, Acad. Press, N. Y., 1971, 307–309.
- [9] Longyear, J. Q. and Parsons, T. D.: The friendship theorem. *Indag. Math.*, **34** (1972), 257–262.
- [10] Bose, R. C. and Shrikhande, S. S.: Graphs in which each pair of vertices is adjacent to the same number d of vertices. *Studia Sci. Math. Hung.*, **4** (1970), 181–195.
- [11] Ryser, M. J.: Intersection properties of finite sets. *J. Combinatorial Th. A*, **14** (1973), 79–92.
- [12] Sós, V. T. and Fried, E.: Weakly associative lattices and projective planes (in print). *Alg. Univ.* **5** (1975), 114–119.
- [13] Sós, Vera T.: Some remarks on the connections of graph theory, finite geometry and block designs. *Proc. of Coll. on Combinatorics, Rome*, 1973 (in print).

ON THE EXISTENCE OF A FACTOR OF DEGREE ONE OF A CONNECTED RANDOM GRAPH

By

P. ERDŐS and A. RÉNYI (Budapest), members of the Academy

§ 0. Introduction

In a series of papers (see [1], [2], [3]) we have considered the structure of a random graph $\Gamma_{n,N}$ obtained as follows: we select at random N edges among the $\binom{n}{2}$ possible edges connecting n given points so that each of the $\binom{\binom{n}{2}}{N}$ possible choices has the same probability $\left(\binom{\binom{n}{2}}{N}\right)^{-1}$. In [1] we have proved that if n and N tend both to $+\infty$ so that

$$(0.1) \quad N = \frac{1}{2} n \log n + cn + o(n)$$

then denoting by C_0 the class of connected graphs and by $P_{n,N}(A)$ the probability that the graph $\Gamma_{n,N}$ belongs to the class A , we have

$$(0.2) \quad \lim_{\substack{n \rightarrow \infty \\ N = \frac{1}{2} n \log n + cn + o(n)}} P_{n,N}(C_0) = e^{-e^{-2c}}.$$

It follows from (0.2) that

$$(0.3) \quad \lim_{n \rightarrow \infty} P_{n,N}(C_0) = \begin{cases} 1 & \text{if } n \rightarrow \infty \text{ and } \frac{N - \frac{1}{2} n \log n}{n} \rightarrow +\infty \\ 0 & \text{if } n \rightarrow \infty \text{ and } \frac{N - \frac{1}{2} n \log n}{n} \rightarrow -\infty. \end{cases}$$

We have proved also that if C_k denotes the class of all graphs consisting of a connected component and k isolated points, we have

$$(0.4) \quad \lim_{\substack{n \rightarrow \infty \\ N = \frac{1}{2} n \log n + cn + o(n)}} P_{n,N}(C_k) = \frac{\exp(-2kc - e^{-2c})}{k!} \quad (k = 1, 2, \dots).$$

Note that the limits on the right of (0.4) are the terms of a Poisson distribution with mean value e^{-2c} , and thus their sum for $k=0, 1, \dots$ equals 1. Thus in case $N = \frac{1}{2} n \log n + O(n)$ the random graph $\Gamma_{n,N}$ consists with probability tending to 1 of a connected component and a certain number of isolated points.

A graph G is said to have a factor of degree one if one can select such a subset S of the edges of G that each point P of G is the endpoint of one and only one edge

belonging to the set S . Clearly a trivial necessary condition for the existence of a factor of degree one of a graph G is that the number of points of G should be even.

According to a celebrated theorem of TUTTE [4] a graph has a factor of degree one if and only if deleting arbitrarily r points of G ($r=0, 1, 2, \dots$) among the connected components of the remaining graph G^* the number of connected components consisting of an odd number of points is less than $r+1$.

Note that if G has n points and n is even, and G^* is obtained by deleting r points of G (of course the edges at least one of the endpoints of which is deleted are also deleted) and if G^* contains t odd components then $t \equiv r \pmod{2}$; thus the theorem of Tutte can be formulated also as follows: A graph G has a factor of degree one if and only if the number of points of G is even and if deleting arbitrarily r points of G ($r=0, 1, \dots$) among the connected components of the remaining graph G^* the number of odd components is less than $r+2$.

In the present paper we deal with the question: what is the probability that the random graph $\Gamma_{n,N}$ has a factor of degree one?

Clearly a graph having at least one isolated point cannot possess a factor of degree one. As according to our mentioned result in case $N = \frac{1}{2} n \log n + cn + o(n)$ the random graph $\Gamma_{n,N}$ contains with probability not tending to 0 isolated points, it seems natural to deal only with the case when $\frac{N - \frac{1}{2} n \log n}{n} \rightarrow +\infty$; of course one has to suppose also that n is even, $n=2m$. For this case we shall prove the following

THEOREM 1. *Let us suppose that n is even, $n=2m$ further that*

$$(0.5) \quad n \rightarrow \infty \quad \text{and} \quad N = \frac{1}{2} n \log n + \omega(n)n \quad \text{where} \quad \lim_{n \rightarrow +\infty} \omega(n) = +\infty.$$

Let F denote the class of graphs containing a factor of degree one; then we have under condition (0.5)

$$(0.6) \quad \lim P_{n,N}(F) = 1.$$

If $N = \frac{1}{2} n \log n + O(n)$, as mentioned above, with probability near to 1 $\Gamma_{n,N}$ consists of a connected component and a certain number of isolated points. With the same method as used to prove Theorem 1 one can prove that if the connected component of $\Gamma_{n,N}$ consists of an even number of points, it has with probability near to 1 a factor of degree one. As the proof of this result is almost the same as that of Theorem 1, we do not go into the details.

It should be mentioned that the results of the present paper are closely related to a previous result of ours (see [5]) concerning random zero-one matrices. As a matter of fact to every n by n zero-one matrix M there corresponds an even graph G , namely the graph consisting of n „red” and n „blue” points in which there is no edge connecting two points having the same colour and the j -th red point is connected with the k -th blue point if and only if the k -th entry of the j -th row of M is 1. Now clearly the graph G has a factor of degree one if and only if the permanent of M is positive; more exactly the permanent of M is equal to the number of different factors of degree one of G .

Now in [5] we have proved that if the n by n random zero-one matrix $M_{n,N}$ is obtained by choosing at random with uniform distribution one of the $\binom{n^2}{N}$ possible n by n zero-one matrices which contain N ones and $n^2 - N$ zeros, then the probability that $M_{n,N}$ has a positive permanent tends to 1 if $n \rightarrow +\infty$ and $\frac{N - n \log n}{n} \rightarrow +\infty$.

According to what has been said above, this result can be interpreted as a result concerning the existence of a factor of degree one of the even graph corresponding to the matrix $M_{n,N}$. It should be added that the problem investigated in the present paper is much more difficult than the corresponding problem for even graphs solved in [5]. Thus for instance in [5] we made use of the well known theorem of D. KÖNIG; the corresponding tool in the present paper is the much deeper theorem of TUTTE mentioned above.

In § 1 we collected some simple inequalities needed in the sequel. § 2 contains the proof of Theorem 1.

§ 1. Some inequalities

The following (well known or obvious) inequalities will be needed.

$$(1.1) \quad \binom{n}{r} \leq \frac{n^r}{r!} \quad (r=1, 2, \dots; \quad n=r, r+1, \dots),$$

$$(1.2) \quad \frac{x-a}{y-a} \leq \frac{x}{y} \quad \text{for } 0 < a \leq x \leq y,$$

$$(1.3) \quad \frac{\binom{B-A}{b-a}}{\binom{B}{b}} \leq \left(1 - \frac{A-a}{B-a}\right)^{b-a} \left(\frac{b}{B}\right)^a$$

if $0 \leq b-a \leq B-A$, $0 \leq a \leq b \leq B$, $0 \leq A$.

$$(1.4) \quad 1-x \leq e^{-x} \quad \text{if } x \geq 0.$$

$$(1.5) \quad n! \geq \left(\frac{n}{e}\right)^n \quad \text{for } n \geq 1.$$

$$(1.6) \quad \text{If } \lambda > 1, \quad 0 < \delta < \frac{1}{\lambda e}$$

we have

$$(1.7) \quad \sum_{n\delta\lambda e \leq r \leq n} \binom{n}{r} \delta^r = O\left(\frac{1}{\lambda^{\delta\lambda e n}}\right).$$

For $0 < p < \frac{1}{2}$ one has

$$\sum_{k \leq np} \binom{n}{k} = O(\sqrt{n} \cdot e^{nh(p)})$$

where $h(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$.

(1.8) If $0 < x < 1$, $c > 0$

$$\sum_{\substack{nc \\ \log n} \leq k} \binom{n}{k} \frac{1}{n^{2k}} = e^{-\alpha cn + o(n)}.$$

(1.9) $1 - x + \frac{x^2}{2} \leq e^{-x + \frac{x^3}{3}}$ if $0 \leq x < 1$.

(1.10) $\binom{n}{k} \leq \frac{n^k}{k!} e^{-\frac{k(k-1)}{2n}}$ if $0 < k \leq n$.

§ 2. Proof of Theorem 1

The proof consists of 8 steps. A characteristic feature of the proof is that we prove certain assertions first in a weak form and use this weak result to improve itself.

1st step. Let A_r denote the class of all graphs from which one can omit r points so that among the components of the remaining graph there are $\geq r+2$ odd components. In what follows $o(1)$ will denote a quantity which tends to 0 if n and N tend to $+\infty$ so that condition (0.5) is satisfied.

LEMMA 1.

$$\sum_{r \geq n \sqrt{\frac{2}{\log n}}} P_{n,N}(A_r) = o(1).$$

PROOF OF LEMMA 1. Let us consider a graph G belonging to the class A_r . Let us choose in each of $r+2$ odd components one point. Clearly these points cannot be connected with each other in G . Thus we get by using (1.3) and (1.4) for sufficiently large n

$$P_{n,N}(A_r) \leq \binom{n}{r+2} \frac{\binom{\binom{n}{2} - \binom{r+2}{2}}{N}}{\binom{\binom{n}{2}}{N}} \leq \binom{n}{r+2} \left(1 - \frac{(r+2)(r+1)}{n(n-1)}\right)^N \leq \binom{n}{r} e^{-n}$$

and thus

$$\sum_{r \geq n \sqrt{\frac{2}{\log n}}} P_{n,N}(A_r) \leq \left(\frac{2}{e}\right)^n.$$

2nd step. We prove now

LEMMA 2.

$$\sum_{\substack{4n \log \log n \\ \log n} < r < n \sqrt{\frac{2}{\log n}}} P_{n,N}(A_r) = o(1).$$

PROOF OF LEMMA 2. According to [1] we may suppose that G is connected because under condition (0.5) the probability of $\Gamma_{n,N}$ being disconnected is $o(1)$. Suppose now that $\Gamma_{n,N}$ belongs to the class A_r . Then by selecting r points from $\Gamma_{n,N}$ (we shall call these r points "separating points") the remaining graph contains $\cong r+2$ odd components.

From each of these components we can select at least one point which is connected with a separating point. We shall call these "contact-points". These points are certainly not connected with each other in $\Gamma_{n,N}$. The r separating points can be selected in $\binom{n}{r}$ ways; the mentioned contact points in the components can be selected in $\binom{n-r}{r+2}$ ways; each of these points may be connected with any one of the r separating points. As the contact-points can not be connected with each other, for the choice of the remaining $N-(r+2)$ edges of the graph there are only $\binom{n}{2} - \binom{r+2}{2}$ possibilities. Thus we get

$$P_{n,N}(A_r) \cong \binom{n}{r} \binom{n-r}{r+2} r^{r+2} \frac{\left(\binom{n}{2} - \binom{r+2}{2} \right)}{\binom{n}{N}}$$

and thus, using the inequalities (1.1)–(1.6) we obtain

$$\sum_{\frac{4n \log \log n}{\log n} \leq r < n \sqrt{\frac{2}{\log n}}} P_{n,N}(A_r) \leq \log^2 n \sum_{\frac{4n \log \log n}{\log n} < r} \binom{n}{r} \left(\frac{3}{\log n} \right)^r = O \left(e^{-\frac{n}{\sqrt{\log n}}} \right).$$

3rd step. Let $D(d)$ denote the set of those graphs G from the points of which one can select a subset S_1 of $k \geq d$ points and another subset S_2 disjoint from S_1 of $l \geq d$ points so that no point belonging to the set S_1 is connected with a point belonging to the set S_2 in G .

LEMMA 3.

$$P_{n,N} \left(D \left(n \sqrt{\frac{2}{\log n}} \right) \right) = o(1).$$

PROOF OF LEMMA 3. Clearly for sufficiently large values of n

$$P_{n,N} \left(D \left(n \sqrt{\frac{2}{\log n}} \right) \right) \leq \sum_{k, l \geq n \sqrt{\frac{2}{\log n}}} \sum_{k+l \leq n} \binom{n}{k} \binom{n}{l} \frac{\left(\binom{n}{2} - kl \right)}{\binom{n}{N}} \leq \left(\frac{2}{e} \right)^{2n}$$

4th step. We need the following very simple

LEMMA 4. If $a_0 \geq a_1 \geq \dots \geq a_s > 0$ is a sequence of positive numbers with sum $A = \sum_{i=0}^s a_i$ such that there does not exist a number j ($0 \leq j \leq s$) for which both $a_0 + \dots + a_j \geq B$ and $a_{j+1} + \dots + a_s \geq B$ where $0 < B \leq A/3$, then we have $a_0 > A - B$.

PROOF OF LEMMA 4. If $B \leq a_0 \leq A - B$ then $a_1 + \dots + a_s = A - a_0 \geq A - (A - B) = B$ which contradicts our hypothesis. Thus either $a_0 < B$ or $a_0 > A - B$; in the first case let i be defined by $a_0 + \dots + a_{i-1} < B \leq a_0 + \dots + a_i$; it follows $a_0 + \dots + a_i < B + a_0 < 2B$ and thus $a_{i+1} + \dots + a_s = A - (a_0 + \dots + a_i) > A - 2B \geq B$ which is again a contradiction. Thus we have $a_0 > A - B$.

Let $\Gamma_{n,N}$ belong to the class A_r . According to Lemmas 1 and 2 we may suppose that

$$r < \frac{4n \log \log n}{\log n}.$$

Let $a_0 \geq a_1 \geq \dots \geq a_s$ ($s \geq r+2$) denote the numbers of points of the connected components of the graph $\Gamma_{n,N}$ after the r separating points have been removed. In view of Lemma 3 one can suppose that the sequence a_i satisfies the conditions

of Lemma 4 with $A = n - r$, $B = \frac{\sqrt{2}n}{\sqrt{\log n}}$; thus by Lemma 4

$$a_0 \geq n - \frac{4n \log \log n}{\log n} - \frac{\sqrt{2}n}{\sqrt{\log n}}.$$

Thus

$$a_1 + \dots + a_s < \frac{4n \log \log n}{\log n} + \frac{\sqrt{2} \cdot n}{\sqrt{\log n}}.$$

5th step. We prove first the following

LEMMA 5. Let $H_n(k, r)$ denote the set of those graphs G having n points, among the points of which one can select a subset S_1 having k elements and another subset S_2 disjoint from S_1 having $n - k - r$ elements such that no point in S_1 is connected with a point in S_2 by an edge of G . Then if $0 < \delta < \frac{1}{2}$, $0 < \varepsilon < \frac{1}{2}$ and $c > \frac{h(\delta)}{1 - \varepsilon - \delta}$, we have

$$\sum_{\substack{\frac{cn}{\log n} < k < \varepsilon n \\ 0 \leq r < \delta n}} P_{n,N}(H_n(k, r)) = o(1).$$

PROOF OF LEMMA 5.

$$\begin{aligned} P_{n,N}(H_n(k, r)) &\leq \binom{n}{k} \binom{n-k}{r} \frac{\left(\binom{n}{2} - k(n-k-r) \right)}{\binom{\binom{n}{2}}{N}} \leq \\ &\leq \binom{n}{k} \binom{n}{r} e^{-\frac{k(n-k-r)}{n} \log n}. \end{aligned}$$

Thus, using (1.7) we get

$$\sum_{0 \leq r < \delta n} \sum_{\frac{cn}{\log n} < k < \varepsilon n} P_{n,N}(H_n(k, r)) = O \left(\sqrt{n} e^{nh(\delta)} \sum_{\frac{cn}{\log n} < k} \binom{n}{k} \frac{1}{n^{k(1-\varepsilon-\delta)}} \right)$$

and therefore by (1.8) it follows

$$\sum_{0 \leq r < \delta n} \sum_{\frac{cn}{\log n} < k < \varepsilon n} P_{n,N}(H_n(k, r)) = O \left(\sqrt{n} e^{n(h(\delta) - \varepsilon(1-\varepsilon-\delta) + o(n))} \right).$$

Thus our lemma is proved.

Applying Lemma 5 with

$$\delta = \frac{4 \log \log n}{\log n}, \quad \varepsilon = \frac{4 \log \log n}{\log n} + \sqrt{\frac{2}{\log n}}$$

we obtain that we may suppose

$$a_1 + \dots + a_s < \frac{8n \log \log^2 n}{\log^2 n}$$

because the probability of the opposite inequality tends to 0. Now we may suppose without restricting the generality that $s = r + 1$ and that the numbers $a_1, \dots, a_{r+1}$ are all odd. Thus we may suppose

$$r + 1 \leq a_1 + \dots + a_{r+1} = k < \frac{8n \log \log^2 n}{\log^2 n}.$$

6th step. We have reduced the problem to the investigation of graphs having $r < \frac{8n \log \log^2 n}{\log^2 n}$ separating points such that after removing these points the remaining graph contains $r + 1$ odd components with $a_1, \dots, a_{r+1}$ points, such that $k = a_1 + \dots + a_{r+1} < \frac{8n \log \log^2 n}{\log^2 n}$. Let us denote by s the number of edges connecting one of the separating points with one of the k points belonging to the $r + 1$ odd components. We distinguish two cases. Either $s \geq r + 8$ or $s < r + 8$. We deal first with the case $s \geq r + 8$. The probability of such a configuration clearly does not exceed

$$\Delta = \sum_{\substack{r < \frac{8n \log \log^2 n}{\log^2 n} \\ r + 1 \leq k < \frac{8n \log \log^2 n}{\log^2 n}}} \binom{n}{r} \binom{n-r}{k} \sum_{r+8 \leq s \leq kr} \binom{kr}{s} \frac{\left(\binom{n}{2} - k(n-k) \right)^{N-s}}{\left(\binom{n}{2} \right)^N}.$$

Using the inequalities (1.1)—(1.10) we obtain

$$\Delta \leq \sum_{r < \frac{8 \log \log^2 n}{\log^2 n}} \sum_{r+1 \leq k < \frac{8n \log \log^2 n}{\log^2 n}} \frac{n^{k+r}}{k! r!} \sum_{r+8 \leq s \leq kr} \binom{kr}{s} \left(\frac{\log n}{n} \right)^s \cdot \frac{1}{n^k} = O(n^{\epsilon^2-8}) = o(1).$$

7th step. It remains to deal with the case when $s \leq r+7$. We shall prove that one can suppose that $k \leq s$ because the probability of $k \geq s+1$ is $o(1)$. As a matter of fact the following lemma is valid.

LEMMA 6. *Let E_k denote the set of those graphs which contain a subset S of k points which are connected by $\leq k-1$ edges with points outside S . Then we have*

$$\sum_{1 \leq k \leq \frac{n}{2 \log n}} P_{n,N}(E_k) = o(1).$$

PROOF OF LEMMA 6. We shall call a subset S of a graph G a *loosely joined set* if S has k points and the number of edges connecting points of S with points outside S is less than k . We shall call S a *primitive loosely joined set* if it is loosely joined and no one of its proper subsets is loosely joined. It is easy to see that a primitive loosely joined set is a connected subgraph. As a matter of fact if S were a primitive loosely joined set, which can be splitted into two sets S_1 and S_2 such that there is no edge in G between points of S_1 and points of S_2 , let k_1 and k_2 denote the number of points in S_1 and S_2 respectively ($k_1 + k_2 = k$) and j_1 resp. j_2 denote the number of edges going out from the set S_1 resp. S_2 . According to our supposition S is primitive loosely connected; thus $j_1 \geq k_1$ and $j_2 \geq k_2$ which implies $j_1 + j_2 \geq k$; thus S is not loosely connected, which contradicts our supposition.

Let E_k^* denote the class of graphs containing a primitive loosely connected subset of order k . As $\sum_{k \leq K} E_k = \sum_{k \leq K} E_k^*$ it is sufficient to prove that

$$\sum_{1 \leq k \leq \frac{n}{2 \log n}} P_{n,N}(E_k^*) = o(1).$$

Now evidently

$$P_{n,N}(E_1^*) = o(1)$$

because a primitive loosely connected set of order 1 is nothing else than an isolated point, and we have proved that the probability of $\Gamma_{n,N}$ containing an isolated point tends to 0 for $n \rightarrow \infty$, $N = \frac{1}{2} n \log n + n\omega(n)$ with $\omega(n) \rightarrow \infty$.

Thus we have to prove only that

$$\sum_{2 \leq k \leq \frac{n}{2 \log n}} P(E_k^*) = o(1).$$

Clearly a primitive loosely connected set of order 2 is simple a pair of points P_1, P_2 such that P_1 and P_2 are connected by an edge, further P_1 is connected with a single

other point P_3 by an edge and P_2 is not connected with any other point except P_1 . Thus

$$P_{n,N}(E_2^*) \leq n(n-1)(n-2) \frac{\left(\binom{n}{2} - (2n-3) \right)}{\binom{N-2}{2}} = O\left(\frac{\log^2 n}{n}\right).$$

As any connected graphs of order k contains at least one spanning tree (having $k-1$ edges) and from k points a tree can be formed in k^{k-2} different ways, we have for $3 \leq k \leq \frac{n}{2 \log n}$

$$P_{n,N}(E_k^*) \leq \binom{n}{k} k^{k-2} \sum_{j=0}^{k-1} \binom{k(n-k)}{j} \frac{\left(\binom{n}{2} - k(n-k) \right)}{\binom{N-j-k+1}{2}} = O\left(\frac{\left(\frac{e^2 \log^2 n}{n}\right)^{k-1}}{k^2}\right).$$

Thus

$$\sum_{1 \leq k \leq \frac{n}{2 \log n}} P_{n,N}(E_k^*) = o(1)$$

which proves Lemma 6.

8th step. We have reduced the problem to the study of graphs G which are of the following type:

- a) There can be selected in G r separating points with $r \leq \frac{8n \log \log^2 n}{\log^2 n}$ such that removing these the graph G falls into components among which there are $r+1$ odd components $C_1, \dots, C_{r+1}$ of orders $a_1, \dots, a_{r+1}$.
- b) There are in G s edges connecting a separating point with a point in one of the components $C_1, \dots, C_{r+1}$ where $r+1 \leq s \leq r+7$.
- c) Putting $k = a_1 + \dots + a_{r+1}$ we have $k \leq s$.

As each of the components C_j ($j=1, \dots, r+1$) is connected with at least one separating point and the number of such points is less than the number of the C_j , there exist two components C_{i_1} and C_{i_2} which are connected with the same separating point P . Clearly the sum of orders a_{i_1} and a_{i_2} of C_{i_1} and C_{i_2} can not exceed 8, and the sum of the numbers b_1 and b_2 of edges going out from C_{i_1} and C_{i_2} does not exceed 8 either. Thus if K denotes the class of graphs with the above mentioned properties a), b), c), we have

$$P_{n,N}(K) \leq \sum_{\substack{1 \leq a_{i_1} \leq 7 \\ 1 \leq a_{i_2} \leq 8 - a_{i_1} \\ 1 \leq b_1 \leq 7 \\ 1 \leq b_2 \leq 8 - b_1}} \sum n \binom{n}{a_{i_1}} \binom{n}{a_{i_2}} \binom{na_{i_1}}{b_1-1} \binom{na_{i_2}}{b_2-1} \frac{\left(\binom{n-a_{i_1}-a_{i_2}}{2} \right)}{\binom{N-b_1-b_2}{2}}$$

from which we get

$$P_{n,n}(K) = O\left(\frac{\log^8 n}{n}\right).$$

Thus Theorem 1 is proved.

References

- [1] P. ERDŐS—A. RÉNYI, On random graphs. I, *Publicationes Mathematicae (Debrecen)*, **6** (1959), pp. 290—297.
- [2] P. ERDŐS—A. RÉNYI, On the evolution of random graphs, *Publ. Math. Inst. Hung. Acad. Sci.*, **5A** (1960), pp. 17—61.
- [3] P. ERDŐS—A. RÉNYI, On the strength of connectedness of a random graph, *Acta Math. Acad. Sci. Hung.*, **12** (1961), pp. 261—267.
- [4] W. T. TUTTE, The factorization of linear graphs, *Journal London Math. Soc.*, **22** (1947), pp. 107—111.
- [5] P. ERDŐS—A. RÉNYI, On random matrices, *Publ. Math. Inst. Hung. Acad. Sci.*, **8A** (1963), pp. 455—461.

158, 167, 172, 179, 183

NOTE

All the questions concerning encountering certain families of graphs can be considered as random graph problems. However, it is possible to determine an exact formula or a generator function in a few cases, only. The sequence of papers of Erdős and Rényi (Nos. 158, 167, 172, 179, 183, 263) started a new direction. They determined directly the asymptotics, and by this method they could go much further than earlier.

Since these years a great number of papers have appeared concerning the connectedness of random graphs. First, it should be noted that two papers appeared on this subject [1], [2] in the year when No. 158 appeared. These papers, using the classical combinatorial encountering methods, obtain some asymptotics for the probability of connectedness and on the number of components. Later Wright [23] determined estimations which give asymptotical results if the number of edges is much less or much more than $\frac{1}{2} n \log n$.

In the papers of Erdős and Rényi the probability that an edge is chosen is independent of the edge. The first step to the generality to consider a fixed graph whose edges can be chosen with equal probability but the edges not belonging to the graph cannot be chosen. Palásti [3] considered the case of a complete bipartite graph in this sense. The results are similar to the case of the complete graph. This is generalized by Kel'mans [4] for complete r -chromatic graphs (r components, no edge in one component, but all the possible edges between the components). (See also [24].) Somewhat weaker results are determined for general graphs satisfying the strong condition, that the degree of all the vertices is $> n/2$ (n is the number of vertices). An even more general treatment is the following: the edge between the vertices v_i and v_j can be chosen with probability p_{ij} (it may be $= 0$). The first step into this direction was made by Stepanov [5], [6]. He considered the case when p_{ij} depends on i and j in a special manner (more exactly, the probability that v_i and v_j are

connected in the moment t is $1 - e^{-\lambda_i \lambda_j t}$ where λ_i and λ_j are constants associated with v_i and v_j , respectively). The most general case of p_{ij} 's is solved by Kovalenko [7]. The conditions $\prod_{j=1}^n (1 - p_{ij}) \rightarrow 0$ and $\sum_{i=1}^n \prod_{j=1}^n (1 - p_{ij})$ is bounded are supposed ($n \rightarrow \infty$). These conditions heuristically mean that the possibility of leaving the vertex v_i is large enough (like in [4], where the degree is large enough). However, under this condition even the strong statement is proved, that the random graph has one gigantic component and many isolated vertices with probability near 1 if n is large, and the distribution of the number of components has a Poisson-distribution. There is no result for the case, when the possibility of leaving a vertex is small (for instance the degree is small). In these cases probably there are more large components, not only one.

In [8] and [9] Stepanov proposes a new modified model for random graphs. Let x and h fixed non-negative numbers. Let G be a given graph with n (fixed) vertices, m edges and k components. The probability that this G is chosen is $x^k h^m / \sum_G x^k h^m$. In this model it is very easy to count. A surprising analogy is found between these random graphs and the phase transitions in statistical physics. This reminds for the jumps emphasized in No. 172.

For directed graphs only the simplest case is solved (Palásti [10]), when all the possible directed edges are chosen with equal probabilities. Of course, it is considered the strong connectedness.

Ivčenko [11] considers the m^{th} (m is fixed) smallest degree v_m in the random graph. The limit distributions are determined, which are different depending on whether

$$p \frac{n}{\log n} \rightarrow \infty, \lim p \frac{n}{\log n} > 1 \text{ or } \lim p \frac{n}{\log n} = 1$$

($p = p(n)$ is the probability of choosing an edge, n is the number of vertices $\rightarrow \infty$). The last case gives a surprising result. The m^{th} smallest degree v_m has at most two different values with probability near 1 if $n \rightarrow \infty$. Similar results are on the m^{th} largest degree v_{n-m+1} . Finally, the author considers $v_n - v_1$, the difference of the largest and smallest degrees.

In another paper [12] Ivčenko extends the results of No. 183. In No. 183 it is that the strength of connectedness is given by the minimal degree, if this proved degree is small. [12] extends this result for larger degrees, too.

Palásti [13] investigated the number of cycles in a directed random graph.

In No. 172 the question is asked, what the situation is regarding Hamilton cycles of the random graphs. O'Neil proved, if $n^{3/2}$ edges are chosen randomly, then the random graph is Hamiltonian with probability near 1. $n^{3/2}$ is improved by

Pósa [14] to $2n \log n$, and recently by Komlós and Szemerédi [15] to $\left(\frac{1}{2} + \varepsilon\right)n \log n$

This means roughly speaking that if a random graph is connected, it is almost Hamiltonian. A related question proposed by Erdős and Rényi: what is the number of Hamilton cycles having exactly r common edges with a fixed Hamilton cycle in a complete graph of n vertices? Results can be found in [16]—[20].

As survey paper on this subject is written by Raynaud [21] with applications. For potential biological applications see [22] (Gy. K.)

REFERENCES

- [1] Austin, T. L., Fagen, R. E., Penney, W. F. and Riordan, J.: The number of components in random linear graphs. *Ann. Math. Stat.*, **30** (1959), 747 – 754.
- [2] Gilbert, E. N.: Random graphs. *Ann. Math. Stat.*, **30** (1959), 1141 – 1144.
- [3] Palásti, I.: On the connectedness of bichromatic random graphs. *Publ. Math. Inst. Hung. Acad. Sci.*, **8** (1963), 431 – 441.
- [4] Кельманс, А. К.: Асимптотические формулы для вероятности k -связности случайных графов. *Теория вероятностей и ее прим.*, **17** (1972), 253 – 265.
- [5] Степанов, В. Е.: Комбинаторная алгебра и случайные графы. *Теория вероятностей и ее прим.*, **14** (1969), 393 – 420.
- [6] Степанов, В. Е.: О вероятности связности случайных графов. *Теория вероятностей и ее прим.*, **15** (1970), 56 – 68.
- [7] Коваленко, И. Н.: К теории случайных графов. *Кибернетика*, Киев 1971, № 4, 1 – 4.
- [8] Степанов, В. Е.: Фазовые переходы в случайных графах. *Период вероятностей*, **1** (1970), 200 – 216.
- [9] Степанов, В. Е.: Строение случайны графов $G_m(x/h)$. *Теория вероятностей*, **17** (1972), 238 – 252.
- [10] Palásti, I.: On the strong connectedness of directed random graphs. *Studia Sci. Math. Hung.*, **1** (1966), 205 – 214.
- [11] Ивченко, Г. И.: Об асмптотическом поведении степеней вершин в случайном графе. *Теория вероятностей и ее прим.*, **18** (1973), 195 – 203.
- [12] Ивченко, Г. И.: О силе связности случайного графа. *Теория вероятностей и ее прим.*, **18** (1973), 417 – 424.
- [13] Palásti, I.: On the threshold distribution function of cycles in a directed random graph. *Studia Sci. Math. Hung.*, **6** (1971), 67 – 73.
- [14] Pósa, L.: Hamilton cycles in random graphs *Discrete Math.*, **14** (1976), 359 – 364.
- [15] Komlós, J. and Szemerédi, E.: Hamilton cycles in random graphs *Coll. Math. Soc. János Bolyai* **10**. (1973), Infinite and finite sets.
- [16] Palásti, I.: On the common edges of Hamilton-cycles of a complete linear graph (in Hungarian). *Mat. Lapok*, **20** (1969), 71 – 98.
- [17] Palásti, I.: On the common edges of Hamilton-cycles of a complete linear graph, Combinatorial Theory and its Applications. *Colloquia Math. Soc. J. Bolyai*, **4**. North-Holland, Amsterdam – London, 1970, 829 – 868.
- [18] Nemetz, T.: On the number of Hamilton-cycles having common edges of given number with a fixed Hamilton-cycle. *Mat. Lapok*, **21** (1970), 65 – 81.
- [19] Nemetz, T.: On a problem about Hamiltonian cycles. *Mat. Lapok*, **22** (1971), 59 – 64.
- [20] Baróti, G.: On the number of certain Hamilton circuits of a complete graph (to appear).
- [21] Raynaud, H.: Sur les graphes aléatoires. *Ann. Inst. Henri Poincaré. Sect. B.*, **4** (1968), 255 – 329.
- [22] Juhász-Nagy, P.: On some “characteristic areas” of plant community stands, Proc. *Colloqu. on Information Theory*, Debrecen 1967. Ed. by A. Rényi, J. Bolyai. Math. Soc. Budapest, 1969.
- [23] Wright, E. M.: Asymptotic enumeration of connected graphs. *Proc. Roy. Soc. Edinburgh*, Ser. A, **68** (1968/70), 298 – 308.
- [24] Hwa Sung, Na and Rapaport, A.: A formula for the probability of obtaining a tree from a graph constructed randomly except for an “exogamous bias”. *Ann. Math. Statist.*, **38** (1967). 226 – 241.

On the Amount of Missing Information and the Neyman–Pearson Lemma

ALFRÉD RÉNYI BUDAPEST

Introduction

Let $\xi_1, \xi_2, \dots, \xi_n, \dots$ be a sequence of random variables whose distribution depends on a parameter θ . Let us suppose that there are only two possible values, θ_0 and θ_1 of θ . We suppose that the random variables ξ_n are independent and identically distributed under the condition $\theta = \theta_0$ as well as under the condition $\theta = \theta_1$. Let the common density function of the variables ξ_n under condition $\theta = \theta_0$ be denoted by $f_0(x)$ and under the condition $\theta = \theta_1$ by $f_1(x)$. We suppose that $f_0(x) \neq f_1(x)$ on a set of positive linear measure. Let us suppose that we have observed the sample $\zeta_n = (\xi_1, \xi_2, \dots, \xi_n)$.

We want to investigate the question *how much information is contained in the sample ζ_n concerning the unknown parameter θ ?* From the point of view of information theory this question makes sense only if we consider θ as a random variable, that is, we attribute to the events $\theta = \theta_0$ and $\theta = \theta_1$ prior probabilities. Thus in order that our question should admit a definite answer, we have to take the ‘Bayesian’ point of view. As a matter of fact, the amount of information in a random variable concerning another random variable is a quantity well known in information theory (see, for example, Geifand and Yaglom, 1958), while the amount of information in a random variable concerning a constant—whether known or not—is always 0.

If θ is considered a random variable with the prior distribution

$$W_0 = P(\theta = \theta_0),$$

$$W_1 = P(\theta = \theta_1), \quad (W_0 + W_1 = 1, \quad W_0 > 0, \quad W_1 > 0)$$

the amount of information $I_n = I(\zeta_n, \theta)$ in the sample ζ_n concerning θ is defined (see Lindley, 1956) by

$$I_n = H(\theta) - E[H(\theta | \zeta_n)] \quad (1)$$

where $H(\theta)$ is the entropy of θ , that is

$$H(\theta) = W_0 \log \frac{1}{W_0} + W_1 \log \frac{1}{W_1} \quad (2)$$

and $H(\theta | \zeta_n)$ is the conditional entropy of θ given ζ_n , that is

$$\begin{aligned} H(\theta | \zeta_n) = P(\theta = \theta_0 | \zeta_n) \log \frac{1}{P(\theta = \theta_0 | \zeta_n)} \\ + P(\theta = \theta_1 | \zeta_n) \log \frac{1}{P(\theta = \theta_1 | \zeta_n)} \end{aligned} \quad (3)$$

while $E[H(\theta | \zeta_n)]$ denotes the expectation of the random variable $H(\theta | \zeta_n)$, that is the mean entropy of θ given the sample ζ_n . $H(\theta)$ measures the total uncertainty about θ , that is, the amount of information concerning θ missing before making any observations, while $E[H(\theta | \zeta_n)]$ measures the *average* uncertainty about θ after observing the sample ζ_n , that is, the amount of information about θ still missing after having observed the sample ζ_n .

Recently we have shown (Rényi, 1965) under the more general assumption that θ may take on any finite number of values, that there exists constants A and λ with $A > 0$, $0 < \lambda < 1$ for which

$$0 \leq H(\theta) - I_n = E[H(\theta | \zeta_n)] \leq A\lambda^n \quad (4)$$

The author (Rényi, 1965) has proved (4) for the case when the variables ζ_n are discrete and has mentioned that the result is valid for the continuous case too. In Section 1 of the present paper we prove (4) directly for the continuous case; the proof given here leads in general to a better (that is, smaller) value of λ than the proof given previously (Rényi, 1965). In Section 2 a 'Bayesian' variant of the fundamental lemma of Neyman and Pearson is proved. In this form the statement of the Neyman-Pearson lemma is that the decision procedure for which the probability of an error is minimal is that which we call the 'standard' decision: to accept $\theta = \theta_0$ if $P(\theta_0 | \zeta_n) > P(\theta_1 | \zeta_n)$ and to accept $\theta = \theta_1$ if $P(\theta_0 | \zeta_n) < P(\theta_1 | \zeta_n)$ while in the case $P(\theta_0 | \zeta_n) = P(\theta_1 | \zeta_n)$ to accept θ_0 with probability W_0 and θ_1 with probability W_1 . In Section 2 we show that the error of the standard decision cannot be larger than twice the amount of missing information $[H(\theta) - I_n]$. This shows that when we apply the likelihood ratio test, the sum of the errors of the first and second kinds is of the same order of magnitude as the amount of missing information.

1 Estimation of the amount of missing information

We shall need the following elementary lemma.

Lemma. For any α with $0 < \alpha < 1$ there exists a constant $C_\alpha > 0$ such that for $0 \leq p \leq 1$, we have

$$p \log \frac{1}{p} + (1 - p) \log \frac{1}{1 - p} \leq C_\alpha p^\alpha$$

where here, and subsequently, $\log$ denotes logarithm with base 2.

The proof of Lemma 1 is evident, because

$$\frac{p \log p + (1 - p) \log (1 - p)}{p^\alpha}$$

is continuous in the closed interval $0 \leq p \leq 1$.

Now we prove the following:

Theorem 1. There exist constants A and λ with $A > 0$ and $0 < \lambda < 1$, depending of course on $f_0(x)$, $f_1(x)$ and W_0 , such that

$$0 \leq H(\theta) - I_n \leq A\lambda^n \quad (n = 1, 2, \dots)$$

For λ we may take the value

$$\lambda = \inf_{0 \leq \alpha \leq 1} \left(\int_{-\infty}^{+\infty} f_1^\alpha(x) f_0^{1-\alpha}(x) dx \right) \quad (5)$$

Proof. We have clearly

$$H(\theta) - I_n = W_0 E[H(\theta | \zeta_n) | \theta = \theta_0] + W_1 E[H(\theta | \zeta_n) | \theta = \theta_1] \quad (6)$$

where $E(\dots | B)$ denotes conditional expectation under condition B . Now by (3) and lemma 1 we have for any α with $0 < \alpha < 1$,

$$E[H(\theta | \zeta_n) | \theta = \theta_0] \leq C_\alpha E[P(\theta = \theta_1 | \zeta_n)^\alpha | \theta = \theta_0]$$

By the theorem of Bayes we have

$$P(\theta = \theta_1 | \zeta_n) = \frac{W_1 \prod_{k=1}^n f_1(\xi_k)}{W_0 \prod_{k=1}^n f_0(\xi_k) + W_1 \prod_{k=1}^n f_1(\xi_k)} \leq \frac{W_1}{W_0} \prod_{k=1}^n \frac{f_1(\xi_k)}{f_0(\xi_k)} \quad (7)$$

and thus we obtain, making use of the independence of the random variables ξ_k under the condition $\theta = \theta_0$,

$$E[P(\theta = \theta_1 | \zeta_n)^\alpha | \theta = \theta_0] \leq \left(\frac{W_1}{W_0} \right)^\alpha \left[\int_{-\infty}^{+\infty} f_1^\alpha(x) f_0^{1-\alpha}(x) dx \right]^n$$

We obtain in the same way, only replacing α by $1 - \alpha$,

$$E[H(\theta | \zeta_n) | \theta = \theta_1] \leq C_{1-\alpha} E[P(\theta = \theta_0 | \zeta_n)^{1-\alpha} | \theta = \theta_1]$$

and

$$E[P(\theta = \theta_0 | \zeta_n)^{1-\alpha} | \theta = \theta_1] = \left(\frac{W_0}{W_1} \right)^{1-\alpha} \int_{-\infty}^{+\infty} f_1^\alpha f_0^{1-\alpha} dx$$

Thus we obtain finally

$$H(\theta) - I_n \leq (C_{1-\alpha} + C_\alpha) W_1^\alpha W_0^{1-\alpha} \left(\int_{-\infty}^{+\infty} f_1^\alpha(x) f_0^{1-\alpha}(x) dx \right)^n \quad (8)$$

It follows that

$$0 \leq H(\theta) - I_n \leq A \lambda^n$$

with λ being defined by (5) and

$$A = (C_{1-\alpha^*} + C_{\alpha^*}) W_1^{\alpha^*} W_0^{1-\alpha^*}$$

where α^* is a value of α for which the infimum in (5) is taken on. Clearly

$$\int_{-\infty}^{+\infty} f_1^\alpha(x) f_0^{1-\alpha}(x) dx = \lambda(\alpha)$$

is a convex function of α with $\lambda(0) = \lambda(1) = 1$. Thus $\min \lambda(\alpha) = \lambda < 1$ and $0 < \alpha^* < 1$ provided that the density functions $f_0(x)$ and $f_1(x)$ are not equal almost everywhere; further $\lambda > 0$ except in the trivial case when $f_0(x) \cdot f_1(x) = 0$ almost everywhere, when of course $\lambda = 0$; that is, a single observation is sufficient to decide with probability 1 whether $\theta = \theta_0$ or $\theta = \theta_1$.

2 A variant of the fundamental lemma of Neyman and Pearson

The fundamental lemma of Neyman and Pearson states that the most powerful test for testing the hypothesis $\theta = \theta_0$ against the alternative hypothesis $\theta = \theta_1$ is the likelihood ratio test. In the usual formulation of this lemma there is a definite distinction between the two hypotheses. From the point of view taken in this present paper there is no such distinction: the problem is completely symmetric. We need therefore a variant of the Neyman-Pearson lemma, which however is easily obtained along the same lines.

Let us introduce the following definitions. A *decision* is a Borel measurable function $\Delta = \Delta(\zeta_n)$ of the sample taking on only the

values θ_0 and θ_1 ; if $\Delta = \theta_0$ we decide in favour of the hypothesis $\theta = \theta_0$ while in the case $\Delta = \theta_1$ we decide in favour of the hypothesis $\theta = \theta_1$. The *error* ε of a decision is the probability of our decision being false, that is,

$$\varepsilon = P(\Delta \neq \theta) \quad (9)$$

Clearly

$$\varepsilon = W_0 P(\Delta = \theta_1 \mid \theta = \theta_0) + W_1 P(\Delta = \theta_0 \mid \theta = \theta_1) \quad (10)$$

Let us define the *standard decision* as follows: We decide always in favour of the hypothesis having the larger conditional probability given the sample, while in case these conditional probabilities are equal we decide at random according to the prior probabilities W_0 and W_1 .

Now we prove the following variant of the Neyman-Pearson lemma:

Theorem 2. No decision can have a smaller error than the standard decision.

Proof. Let us divide the sample space into the disjoint sets S_1 , S_0 , and S defined as follows:

$$\left. \begin{aligned} \zeta_n \in S_1 & \quad \text{if} \quad P(\theta_1 \mid \zeta_n) > P(\theta_0 \mid \zeta_n) \\ \zeta_n \in S_0 & \quad \text{if} \quad P(\theta_0 \mid \zeta_n) > P(\theta_1 \mid \zeta_n) \\ \zeta_n \in S & \quad \text{if} \quad P(\theta_0 \mid \zeta_n) = P(\theta_1 \mid \zeta_n) \end{aligned} \right\} \quad (11)$$

Let us put $\bar{x} = (x_1, \dots, x_n)$ and $f_i(\bar{x}) = \prod_{k=1}^n f_i(x_k)$.

Let us put further

$$\delta(\bar{x}) = \begin{cases} 1 & \text{for } \bar{x} \in S_1 \\ 0 & \text{for } \bar{x} \in S_0 \\ W_1 & \text{for } \bar{x} \in S \end{cases} \quad (12)$$

According to (7), (11), and (12) an equivalent definition of δ follows:

$$\delta(\bar{x}) = \begin{cases} 1 & \text{if } f_1(\bar{x})W_1 > f_0(\bar{x})W_0 \\ 0 & \text{if } f_0(\bar{x})W_0 > f_1(\bar{x})W_1 \\ W_1 & \text{if } f_0(\bar{x})W_0 = f_1(\bar{x})W_1 \end{cases} \quad (13)$$

The error of the standard decision is clearly

$$\varepsilon = W_0 \int \delta(\bar{x}) f_0(\bar{x}) d\bar{x} + W_1 \int [1 - \delta(\bar{x})] f_1(\bar{x}) d\bar{x} \quad (14)$$

where $d\bar{x}$ stands for $dx_1 dx_2 \dots dx_n$ and the integrals are over the whole sample space.

Let us denote by Δ^* any decision different from the standard decision. Let us denote by $\delta^*(\bar{x})$ the function which is equal to 1 for $\Delta^* = \theta_1$ and equal to 0 for $\Delta^* = \theta_0$. Then we have, denoting by ϵ^* the error of the decision Δ^* ,

$$\epsilon^* = W_0 \int \delta^*(\bar{x}) f_0(\bar{x}) d\bar{x} + W_1 \int [1 - \delta^*(\bar{x})] f_1(\bar{x}) d\bar{x} \quad (15)$$

It follows that

$$\epsilon^* - \epsilon = \int [\delta^*(\bar{x}) - \delta(\bar{x})] [W_0 f_0(\bar{x}) - W_1 f_1(\bar{x})] d\bar{x} \quad (16)$$

As clearly the integrand is everywhere non-negative, it follows that $\epsilon^* \geq \epsilon$, which proves our theorem.

It should be added that equation (13) shows that the standard decision means the application of the likelihood ratio test, namely that we accept the hypothesis $\theta = \theta_1$ if

$$\frac{f_1(\bar{x})}{f_0(\bar{x})} > \frac{W_0}{W_1}$$

and the hypothesis $\theta = \theta_0$ if

$$\frac{f_1(\bar{x})}{f_0(\bar{x})} < \frac{W_0}{W_1}$$

while in the case

$$\frac{f_1(\bar{x})}{f_0(\bar{x})} = \frac{W_0}{W_1}$$

a random choice is made between $\theta = \theta_1$ and $\theta = \theta_0$ with probabilities W_1 and W_0 respectively.

3 Estimation of the error of the standard decision by the amount of missing information

In this section we prove the following

Theorem 3. Let ϵ denote the error of the standard decision. Then we have

$$\epsilon \leq [H(\theta) - I_n]$$

Proof. We start again from (6). As both terms of $p \log (1/p) + (1 - p) \log 1/(1 - p)$ are non-negative we obtain

$$\begin{aligned} H(\theta) - I_m \\ \geq \int_{S_1+S} f_0(\bar{x}) W_0 \log \left[1 + \frac{f_1(\bar{x}) W_1}{f_0(\bar{x}) W_0} \right] dx \\ + \int_{S_0+S} f_1(\bar{x}) W_1 \log \left[1 + \frac{f_0(\bar{x}) W_0}{f_1(\bar{x}) W_1} \right] dx \end{aligned}$$

As in S_1

$$\frac{f_0(\bar{x}) W_0}{f_1(\bar{x}) W_1} \leq 1$$

it follows that

$$\int_{S_1+S} f_0(\bar{x}) W_0 \log \left[1 + \frac{f_1(\bar{x}) W_1}{f_0(\bar{x}) W_0} \right] dx \geq W_0 P(\Delta = \theta_1 \mid \theta = \theta_0)$$

Similarly we obtain

$$\int_{S_0+S} f_1(\bar{x}) W_1 \log \left[1 + \frac{f_0(\bar{x}) W_0}{f_1(\bar{x}) W_1} \right] dx \geq W_1 P(\Delta = \theta_0 \mid \theta = \theta_1)$$

Thus it follows that

$$H(\theta) - I_n \geq \epsilon$$

which proves Theorem 3.

Combining Theorem 3 with Theorem 1 we obtain, denoting by ϵ_n the error of the standard decision after taking the sample ζ_n ($n = 1, 2, \dots$), that

$$\epsilon_n \leq A \lambda^n$$

This implies that the series $\sum_{n=1}^{\infty} \epsilon_n$ is convergent; thus by the Borel-Cantelli lemma if we continue the sampling indefinitely and from each n take the standard decision, then with probability 1 from some point onwards all our decisions will be correct.

REFERENCES

- Gelfand, I. M., Yaglom, A. M. (1958). Über die Berechnung der Menge an Information über eine zufällige Funktion die in einer anderen zufälligen Funktion enthalten ist. Arbeiten zur Informationstheorie, II. VEB Deutscher Verlag der Wissenschaften, Berlin, 7-56.

Lindley, D. V. (1956). On a measure of the information provided by an experiment. *Ann. Math. Statist.*, **27**, 986–1005.

Rényi, A. (1965). On the amount of information concerning an unknown parameter in a sequence of observations. *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, **9**, 617–625.

231, 236, 266, 267, 285, 288, 305, **328**

ON THE AMOUNT OF INFORMATION IN A RANDOM VARIABLE CONCERNING AN EVENT

ALFRED RÉNYI

§ 1. An inequality on the missing information

Let $S = [\Omega, \mathbf{A}, P]$ be a probability space, i.e., Ω an arbitrary non-empty set, $\mathbf{A}$ a σ -algebra of subsets of Ω and P a measure defined on $\mathbf{A}$ for which $P(\Omega) = 1$. Let A be an arbitrary event in S , i.e., $A \in \mathbf{A}$, and let us suppose that putting $p = P(A)$ we have $0 < p < 1$. Let ξ be any random variable on S , i.e., a function defined on Ω which is measurable with respect to $\mathbf{A}$.

Let us put

$$h(x) = x \log_2 \frac{1}{x} + (1-x) \log_2 \frac{1}{1-x}, \quad (1)$$

where $\log_2$ denotes logarithm with base 2.

The amount of information contained in the value of ξ with respect to the event A will be denoted by $I(\xi, A)$, and is defined (see [2]) by the formula

$$I(\xi, A) = h(p) - H, \quad (2)$$

where

$$H = E\{h[P(A/\xi)]\}. \quad (3)$$

Here $P(A/\xi)$ denotes the conditional probability of the event A given the value of ξ , (see [1]) and $E(\dots)$ denotes the expectation of the random variable in the brackets. $h(p)$ can be interpreted as the amount of uncertainty concerning the event A , while $h[P(A/\xi)]$ is the amount of uncertainty concerning A after having observed the value ξ ; thus H is the average uncertainty concerning A after having observed ξ .

By other words, H is the *amount of missing information* concerning A after having observed ξ .

Suppose that we are interested in the event A having occurred or not, but are unable to observe A directly; we can observe only the value of ξ and from this indirect observation we want to decide whether A occurred or not. Any decision can be characterized by a function $d(\xi)$, which is

itself a random variable, with values 0 and 1 such that after observing ξ if $d(\xi) = 1$ we decide in favour of A while if $d(\xi) = 0$ we decide in favour of the opposite event $\bar{A}$. The error δ of a decision $d(\xi)$ is the probability of the decision being false, i.e.,

$$\delta = pP(d(\xi) = 0/A) + (1-p)P(d(\xi) = 1/\bar{A}). \quad (4)$$

We define the "standard decision" $D(\xi)$ as follows :

$$D(\xi) = \begin{cases} 1 & \text{if } P(A/\xi) > P(\bar{A}/\xi) \\ 0 & \text{if } P(A/\xi) < P(\bar{A}/\xi), \end{cases} \quad (5)$$

while in case $P(A/\xi) = P(\bar{A}/\xi)$ the value of $D(\xi)$ is determined at random so that with probability p we put $D(\xi) = 1$ and with probability $1 - p$ we put $D(\xi) = 0$. Thus the standard decision means, that we decide in favour of A or $\bar{A}$ according to which of them has the larger posterior probability. We denote the error of the standard decision by Δ ; thus

$$\Delta = pP(D(\xi) = 0/A) + (1-p)P(D(\xi) = 1/\bar{A}). \quad (6)$$

By reformulating the fundamental lemma of *Neyman and Pearson* for the present (Bayesian) case, we have shown (see [3]) that *no decision can have a smaller error than the standard decision*. It is easy to see that we have always $\Delta \leq 1/2$ because clearly

$$\Delta = \int_{P(A/\xi) \leq \frac{1}{2}} P(A/\xi) dP + \int_{P(\bar{A}/\xi) \leq \frac{1}{2}} P(\bar{A}/\xi) dP.$$

We have shown also (see [3]) that

$$\Delta \leq H, \quad (7)$$

i.e., the error of the standard decision cannot be larger than the amount of missing information, further (see [4]) that

$$H \leq h(\Delta). \quad (8)$$

Both (7) and (8) hold more generally in case we make a decision on the basis of observing the random variable ξ with respect to another random variable η .

(8) is a consequence of Jensen's inequality, and it is best possible in the sense that equality can stand in (8). For instance if $P(A) = \frac{1}{2}$ further ξ and A are independent, i.e., $P(A/\xi) \equiv \frac{1}{2}$, then $H = h(\frac{1}{2}) = 1$ and $\Delta = \frac{1}{2}$, thus $h(\Delta) = 1$ and therefore $H = h(\Delta)$.

In this section we shall give the following improvement of (7):

Theorem 1. *We have*

$$\Delta \leq \frac{H}{2}. \quad (9)$$

Remark. The inequality (9) is best possible in the sense that for the case when $P(A) = p = \frac{1}{2}$ and $P(A/\xi) \equiv \frac{1}{2}$ we have equality in (9).

Proof of Theorem 1. Let us put

$$g(\xi) = \begin{cases} P(A/\xi) & \text{if } P(A/\xi) \leq \frac{1}{2} \\ P(\bar{A}/\xi) & \text{if } P(A/\xi) > \frac{1}{2}. \end{cases} \quad (10)$$

As $h(x) = h(1-x)$ and $P(\bar{A}/\xi) = 1 - P(A/\xi)$ evidently

$$H = E(h(g(\xi))). \quad (11)$$

Now $g(\xi) \leq \frac{1}{2}$ further we have clearly $h(x) \geq 2x$ for $0 \leq x \leq \frac{1}{2}$. Thus if we denote by B the event $D(\xi) = 0$ we have

$$H \geq 2E(g(\xi)) = 2P(B)E(P(A/\xi)/B) + 2P(\bar{B})E(P(\bar{A}/\xi)/\bar{B}), \quad (12)$$

where $E(\dots/B)$ denotes conditional expectation under condition B .

Now by the definition of conditional probability (see [1]) we have

$$E(P(A/\xi)/B) = P(A/B),$$

and

$$E(P(\bar{A}/\xi)/\bar{B}) = P(\bar{A}/\bar{B}). \quad (13)$$

Thus we obtain

$$H \geq 2[P(AB) + P(\bar{A}\bar{B})]. \quad (14)$$

Now clearly

$$P(AB) + P(\bar{A}\bar{B}) = \Delta. \quad (15)$$

Thus (9) follows from (14) and (15).

2. A paradox and its explanation

Let us put $\eta = D(\xi)$ and compute the amount of information concerning the event A contained in η . Clearly if B denotes the event $\eta = 1$ then

$$I(\eta, A) = h(p) - [P(B)h(P(A/B)) + P(\bar{B})h(P(A/\bar{B}))]. \quad (16)$$

As η is a function of ξ , clearly

$$I(\eta, A) \leq I(\xi, A)$$

with equality standing only if $P(A/\xi)$ takes only two values; thus in general ξ contains more information on A than η . However the standard decision after having observed η is the same as after having observed ξ . In other words we arrive at the following paradox: while ξ contains in general more information on A than η , it is impossible to utilize this

extra information. But what is the value of information which cannot be used? This paradox seems to contradict the usual interpretation of the amount of information. However, a simple explanation of this paradox can be given. The information concerning A in the value of ξ , which is not contained in the value of η , can be utilized by making some additional observation of a third random variable. For instance, if α is the indicator of the event A (i.e. $\alpha = 1$ if A takes place and $\alpha = 0$ if $\bar{A}$ takes place), and $\zeta = \xi + \alpha$, then by observing both ξ and ζ , we get full information concerning the event A , because if $\zeta - \xi = 1$ then A certainly has happened while if $\zeta - \xi = 0$ then A did not happen.

However, if we observe only η and ζ , these two random variables do not give in general full information on the event A . Thus the latent extra information in the value of ξ concerning the event A can be made free by observing the auxiliary variable ζ .

REFERENCES

1. A. KOLMOGOROFF. *Grundbegriffe der Wahrscheinlichkeitsrechnung*, Springer, Berlin, (1933).
2. A. RÉNYI. On the amount of information concerning an unknown parameter in a sequence of observations, *Publ. Math. Inst. Hung. Acad. Sci.*, 9.A (1965), 617-624.
3. A. RÉNYI. On the amount of missing information and the Neyman-Pearson lemma. *Research papers in Statistics* (dedicated to J. Neyman), Wiley and Sons Ltd. (in print).
4. A. RÉNYI. On some basic problems of Statistics from the point of view of information theory, *Proceedings of the 5th Berkeley Symposium* (in print).

REMARKS ON THE POISSON PROCESS

by
A. RÉNYI

The inhomogeneous Poisson process on the real line is usually characterized as a stochastic additive set function $\xi(E)$ defined for each bounded Borel subset E of the real line such that

a) the random variable $\xi(E)$ has for each bounded Borel set E a Poisson distribution, i. e.

$$(1) \quad \mathbf{P}(\xi(E) = n) = \frac{[\lambda(E)]^n \cdot e^{-\lambda(E)}}{n!} \quad (n = 0, 1, \dots)$$

where $\lambda(E)$ is a nonatomic measure on the real line such that $\lambda(E)$ is finite for each finite interval E , and

b) if $E_1, E_2, \dots, E_n$ are mutually disjoint bounded Borel sets the random variables $\xi(E_1), \dots, \xi(E_n)$ are independent.

If we put $\xi_t = \xi([0, t])$ for $t > 0$, $\xi_t = -\xi([t, 0])$ for $t < 0$, this means that ξ_t is a process with independent increments such that $\xi_t - \xi_s$ has a Poisson distribution with mean value $\lambda(t) - \lambda(s)$ where $\lambda(t)$ is the λ -measure of the interval $[0, t]$ if $t > 0$ and $-\lambda(t)$ is the λ -measure of the interval $[t, 0]$ if $t < 0$. D. SZÁSZ (oral communication) asked the question whether there exists a point process for which a) holds but b) does not hold.

We shall show in this note that such a process does not exist, i. e. the usual supposition about independence in the above characterisation of the Poisson process is unnecessary; by other words supposition b) is a consequence of the supposition a).

More exactly we prove the following

THEOREM 1. *Let J denote the family of all subsets of the real line which can be obtained as the union of a finite number of disjoint finite intervals $[a, b)$ closed to the right and open to the left. Let $\xi(E)$ be an additive stochastic set function defined for each $E \in J$, i. e. such that if E_1 and E_2 are disjoint one has $\xi(E_1 + E_2) = \xi(E_1) + \xi(E_2)$. Suppose that for each $E \in J$ $\xi(E)$ has a Poisson distribution with mean value $\lambda(E)$ where $\lambda(E)$ is a nonatomic measure on the Borel subsets of the real line, which is finite for each $E \in J$. Then it follows that if $E_1, \dots, E_n$ are disjoint sets ($E_k \in J$) the random variables $\xi(E_1), \dots, \xi(E_n)$ are independent, i. e. $\xi(E)$ is a Poisson process.*

PROOF OF THEOREM 1. Let $A(E)$ denote the event $\xi(E) = 0$. If E is the union of the disjoint sets $E_j \in J$ ($j = 1, 2, \dots, n$) then¹ clearly $A(E) = A(E_1) \dots A(E_n)$ because $\xi(E) = \sum_{j=1}^n \xi(E_j)$ and thus $\xi(E) = 0$ iff $\xi(E_j) = 0$ for $j = 1, 2, \dots, n$.

¹ Here and in what follows the product of events denotes the joint occurrence of these events

But by supposition

$$(2) \quad \mathbf{P}(A(E)) = \mathbf{P}(\xi(E) = 0) = e^{-\lambda(E)} = \prod_{j=1}^n e^{-\lambda(E_j)} = \prod_{j=1}^n \mathbf{P}(A(E_j)).$$

Thus it follows that if the sets $E_1, \dots, E_n$ are disjoint, the events $A(E_1), \dots, A(E_n)$ are independent.

Now let $1_{A(E)}$ be the indicator of the event $A(E)$.

Let $E \in J$ and $F \in J$ be two disjoint sets. For any $\varepsilon > 0$ we can clearly decompose E into disjoint intervals E_i ($1 \leq i \leq n$) and F into disjoint intervals F_j ($1 \leq j \leq m$) such that

$$\max_i \lambda(E_i) < \varepsilon \quad \text{and} \quad \max_j \lambda(F_j) < \varepsilon.$$

Now evidently $\xi(E) \neq \sum_{i=1}^n 1_{A(E_i)}$ implies $\max_i \xi(E_i) \geq 2$ and $\xi(F) \neq \sum_{j=1}^m 1_{A(F_j)}$ implies $\max_j \xi(F_j) \geq 2$. On the other hand for any $B \in J$

$$(3) \quad \mathbf{P}(\xi(B) \geq 2) = \sum_{k=2}^{\infty} \frac{\lambda(B)^k \cdot e^{-\lambda(B)}}{k!} \leq \lambda^2(B).$$

Thus

$$(4a) \quad \mathbf{P}\left(\xi(E) \neq \sum_{i=1}^n 1_{A(E_i)}\right) \leq \sum_{i=1}^n \lambda^2(E_i) < \varepsilon \lambda(E)$$

and

$$(4b) \quad \mathbf{P}\left(\xi(F) \neq \sum_{j=1}^m 1_{A(F_j)}\right) \leq \sum_{j=1}^m \lambda^2(F_j) < \varepsilon \lambda(F).$$

This implies, as the sums $\sum_{i=1}^n 1_{A(E_i)}$ and $\sum_{j=1}^m 1_{A(F_j)}$ are independent that $\xi(E)$ and $\xi(F)$ are independent, too.

As a matter of fact it follows from (4a) and (4b) that for any n and m ($n, m = 0, 1, 2, \dots$)

$$(5) \quad |\mathbf{P}(\xi(E) = n, \xi(F) = m) - \mathbf{P}(\xi(E) = n) \cdot \mathbf{P}(\xi(F) = m)| \leq 2\varepsilon \lambda(E + F).$$

As $\varepsilon > 0$ can be chosen arbitrarily small, our statement follows. The independence of the variables $\xi(E_i)$ ($i = 1, 2, \dots, r$) with disjoint E_i and $r > 2$ is proved in exactly the same way. Thus our theorem is proved.

REMARK 1. Note that to prove the independence of $\xi(E_i)$ ($i = 1, 2, \dots, r$) for $E_i E_j = \emptyset$ if $i \neq j$ we have not used the full supposition that for each $E \in J$ $\xi(E)$ has a Poisson distribution, only that

$$(6a) \quad \mathbf{P}(\xi(E) = 0) = e^{-\lambda(E)}$$

and

$$(6b) \quad \mathbf{P}(\xi(E) \geq 2) = o(\lambda(E)) \quad \text{if} \quad \lambda(E) \rightarrow 0$$

uniformly in E .

Thus even these suppositions imply that the process $\xi(E)$ is a process of independent increments. It is easy to show however that this together with (6a) and (6b) implies that $\xi(E)$ has a Poisson distribution.

Thus the following theorem is true.

THEOREM 2. *Let J denote the family of all subsets of the real line which can be obtained as the union of a finite number of disjoint finite intervals $[a, b)$. Let $\xi(E)$ be an additive stochastic set function defined for $E \in J$, i. e. such that if $E_1 \in J$ and $E_2 \in J$ are disjoint one has $\xi(E_1 + E_2) = \xi(E_1) + \xi(E_2)$. Suppose that $\xi(E)$ is for each $E \in J$ a nonnegative integer valued random variable such that*

$$(7a) \quad \mathbf{P}(\xi(E) = 0) = e^{-\lambda(E)}$$

and

$$(7b) \quad \mathbf{P}(\xi(E) \geq 2) \leq \lambda(E) \cdot \delta(\lambda(E))$$

where $\delta(x)$ is an increasing positive function defined for $x > 0$ such that $\lim_{x \rightarrow 0} \delta(x) = 0$ and $\lambda(E)$ a nonatomic measure on J . Then it follows that $\xi(E)$ is a Poisson process, i. e. if E_i ($i = 1, 2, \dots, r$) are disjoint sets, $E_i \in J$ the random variables $\xi(E_i)$ ($i = 1, 2, \dots, r$) are independent, and (1) holds.

PROOF OF THEOREM 2. Put for $E \in J$

$$\varphi_E(u) = \mathbf{M}(e^{iu\xi(E)}) \quad (-\infty < u < +\infty)$$

then clearly

$$(8) \quad |\varphi_E(u)| \geq e^{-\lambda(E)} - (1 - e^{-\lambda(E)}) > 0$$

if $\lambda(E) < \log 2$. Thus if $E = \sum_{i=1}^r E_i$, where $E_i \in J$ and $E_i E_j = \emptyset$ if $i \neq j$, then if $\lambda(E_i) < \log 2$ we have (as it follows from the proof of Theorem 1 that the random variables $\xi(E_i)$ ($i = 1, 2, \dots, r$) are independent)

$$(9) \quad \varphi_E(u) = \prod_{i=1}^r \varphi_{E_i}(u) \neq 0$$

and therefore

$$(10) \quad \log \varphi_E(u) = \sum_{i=1}^r \log \varphi_{E_i}(u).$$

As however

$$(11) \quad \varphi_{E_i}(u) = e^{-\lambda(E_i)} + e^{iu}(1 - e^{-\lambda(E_i)}) + O(\lambda(E_i)\delta(\lambda(E_i)))$$

we get

$$(12) \quad \log \varphi_{E_i}(u) = \lambda(E_i)(e^{iu} - 1) + O(\lambda(E_i)(\lambda(E_i) + \delta(\lambda(E_i)))).$$

It follows that if $\lambda(E_i) < \varepsilon$ for $i = 1, 2, \dots, r$

$$(13) \quad \log \varphi_E(u) = \lambda(E)(e^{iu} - 1) + O(\varepsilon + \delta(\varepsilon))$$

that is, as $\varepsilon > 0$ can be chosen arbitrarily small,

$$(14) \quad \varphi_E(u) = e^{\lambda(E)(e^{iu} - 1)}$$

which implies that $\xi(E)$ has a Poisson distribution with mean $\lambda(E)$. Thus Theorem 2 follows from Theorem 1.

REMARK 2. The proof can be carried over without any change to the discussion of a Poisson process in more than one dimension or even in an abstract space. Thus we obtain the following

THEOREM 3. Let X be any space, J a family of subsets of X and $\lambda(E)$ a non-negative finite valued set function defined on J such that

- 1) if $E_1 \in J, E_2 \in J$ and $E_1 E_2 = \emptyset$, then $E_1 + E_2 \in J$,
- 2) If $E_1 \in J, E_2 \in J, E_1 E_2 = \emptyset$ then $\lambda(E_1 + E_2) = \lambda(E_1) + \lambda(E_2)$,
- 3) There is a constant α with $0 < \alpha < 1$ such that for every $E \in J$ with $\lambda(E) > 0$

there exists a subset F of E such that $F \in J, E - F \in J$ and $\alpha < \frac{\lambda(F)}{\lambda(E)} < 1 - \alpha$. Let us

suppose that a stochastic set function is defined on J i. e. to every $E \in J$ there corresponds a random variable $\xi(E)$ such that if $E_1 \in J, E_2 \in J$ and $E_1 E_2 = \emptyset$ we have $\xi(E_1 + E_2) = \xi(E_1) + \xi(E_2)$ and $\xi(E)$ has a Poisson distribution with mean value $\lambda(E)$.

Then the random variables $\xi(E_i)$ ($i = 1, 2, \dots, r$) are independent if the sets $E_i \in J$ ($i = 1, \dots, r$) are disjoint, i. e. $\xi(E)$ is a Poisson process.

Note that condition 3) is not quite the same as that λ is nonatomic, because we did not suppose that J is a σ -algebra of sets.

REMARK 3. The question arises whether the condition that the process should be one with independent increments can be deduced from other suppositions for other processes of independent increments, too.

The most interesting case is that of the Wiener process. For this process one has the following (almost trivial) analogue of Theorem 1.

THEOREM 4. Let ξ_t ($-\infty < t < +\infty$) be a stochastic process such that $\xi_t - \xi_s$ is normally distributed with mean 0 and variance $(t-s)$ for $s < t$. Suppose further that if the intervals $[s_j, t_j]$ ($j = 1, 2, \dots, r$) are disjoint, any linear combination

$\sum_{j=1}^r b_j(\xi_{t_j} - \xi_{s_j})$ of the increments $\xi_{t_j} - \xi_{s_j}$ with real coefficients b_j is normally distributed.

Then $\{\xi_t\}$ is the Wiener process, i. e. the random variables $\xi_{t_j} - \xi_{s_j}$ are independent if the intervals $[s_j, t_j]$ are disjoint.

PROOF OF THEOREM 4. Clearly putting for $I_k = [s_k, t_k]$ $\xi(I_k) = \xi_{t_k} - \xi_{s_k}$ ($k = 1, 2$) if I_1 and I_2 are adjacent intervals ($s_1 < t_1 = s_2 < t_2$) $\xi(I_1 + I_2) = \xi(I_1) + \xi(I_2)$ and thus

$$\mathbf{M}((\xi(I_1 + I_2))^2) = t_2 - s_1 = t_2 - s_2 + t_1 - s_1 = \mathbf{M}(\xi^2(I_1)) + \mathbf{M}(\xi^2(I_2))$$

and thus $\mathbf{M}(\xi(I_1)\xi(I_2)) = 0$, i. e. $\xi(I_1)$ and $\xi(I_2)$ are uncorrelated. Now let I_1 and I_2 be arbitrary disjoint intervals

$$I_1 = [s_1, t_1], I_2 = [s_2, t_2] \quad \text{where} \quad s_1 < t_1 < s_2 < t_2$$

and put $I_3 = [t_1, s_2]$. Then, taking into account that $\mathbf{M}(\xi(I_1)\xi(I_3))=0$ and $\mathbf{M}(\xi(I_3)\xi(I_2))=0$, we get $\mathbf{M}(\xi^2(I_1 + I_2 + I_3)) = t_2 - s_1 = \mathbf{M}(\xi^2(I_1)) + \mathbf{M}(\xi^2(I_2)) + \mathbf{M}(\xi^2(I_3)) + 2\mathbf{M}(\xi(I_1)\xi(I_2))$.

Thus

$$\mathbf{M}(\xi(I_1)\xi(I_2))=0.$$

(We have used here the following elementary geometrical fact: if a, b, c are vectors in the 3-dimensional Euclidean space for which c is orthogonal both to b and to $a+b$, then c is orthogonal to a , too.) Thus $\xi(I_1)$ and $\xi(I_2)$ are uncorrelated if I_1 and I_2 are arbitrary disjoint intervals.

It follows that if $I_1, I_2, \dots, I_r$ are disjoint intervals and I_j has length $|I_j|$, and $b_1, \dots, b_r$ are arbitrary real constants, then

$$\mathbf{M}\left(\left(\sum_{j=1}^r b_j \xi(I_j)\right)^2\right) = \sum_{j=1}^r b_j^2 |I_j|.$$

Thus

$$\mathbf{M}\left(e^{iu \sum_{j=1}^r b_j \xi(I_j)}\right) = e^{-\frac{1}{2}u^2 \sum_{j=1}^r b_j^2 |I_j|}$$

and thus for any real numbers $u_1, u_2, \dots, u_r$

$$\mathbf{M}\left(e^{i \sum_{j=1}^r u_j \xi(I_j)}\right) = \prod_{j=1}^r \mathbf{M}(e^{iu_j \xi(I_j)})$$

i. e. the $\xi(I_j)$ ($j=1, 2, \dots, r$) are independent i.e. ξ_t is the Wiener process.

REMARK 4. Returning to the Poisson process, the question arises whether if in Theorem 1 instead of the condition that $\xi(E)$ has a Poisson distribution if E is any finite union of intervals, one supposes only that $\xi(I)$ has a Poisson distribution if I is any interval, does this ensure that the process is a Poisson process? We can prove only that in this case $\xi(I_1)$ and $\xi(I_2)$ are uncorrelated if I_1 and I_2 are disjoint intervals. The proof of this is essentially the same as the first step of the proof of Theorem 4.

Remark added on August 22, 1966.

I have been informed by JAY GOLDMAN that the answer to the question in Remark 4 is: no. This has been shown by a counterexample by L. SHEPP; his example will be published in a forthcoming paper of J. GOLDMAN.

Remark added on March 15, 1967.

P. A. P. MORAN has obtained independently from L. SHEPP the same results. His paper will be published in this journal.

STATISTICS AND INFORMATION THEORY¹by
A. RÉNYI

§ 0. Introduction

In the present paper we deal with certain basic questions connected with the information-theoretic point of view on statistics. This paper is a continuation of the papers [1], [2], [3], [4], [5] of the author; most of the results of these previous papers are presented here in an improved (sharper or more general) form.

§ 1. On the Amount of Information in a Random Variable
Concerning Another

In this section we collect the basic definitions and well known results needed in what follows.

Let $S=(\Omega, \mathcal{A}, \mathbf{P})$ be a probability space, i. e. Ω an arbitrary nonempty set, $\mathcal{A}$ a σ -algebra of subsets of Ω and $\mathbf{P}$ a probability measure on $\mathcal{A}$. In what follows θ will always denote a discrete valued random variable in S , i. e., a function $\theta=\theta(\omega)$ defined for $\omega\in\Omega$, taking on only a finite number of different values $\theta_1, \theta_2, \dots, \theta_r$ ($r\geq 2$) for which the set (event) $H_k=\{\omega: \theta(\omega)=\theta_k\}$ belongs to $\mathcal{A}$ for $k=1, 2, \dots, r$. Here $\theta_1, \theta_2, \dots, \theta_r$ may be numbers, or any distinguishable symbols: their values will be in what follows irrelevant. We shall usually interpret θ as the parameter of a probability distribution and the event H_k as the *hypothesis that the true value of the parameter θ is equal to θ_k* ; we shall use the notation

$$(1.1) \quad p_k = \mathbf{P}(H_k) = \mathbf{P}(\theta = \theta_k) \quad (k=1, 2, \dots, r)$$

and call the distribution $(p_1, p_2, \dots, p_r)$ of θ (contrasting it with the conditional (or posterior) distribution of θ given certain observations, to be introduced later) the *prior distribution* of θ . The (unconditional) entropy of θ is defined by Shannon's formula ²

$$(1.2) \quad \mathbf{H}(\theta) = \sum_{k=1}^r p_k \log_2 \frac{1}{p_k}$$

where the numbers p_k ($k=1, 2, \dots, r$) are those defined by (1.1) $\mathbf{H}(\theta)$ will be interpreted as *the amount of missing information on θ when nothing else is known about θ except that its prior distribution is given.*

¹ This paper has been presented to the 1st European Meeting of Statisticians held in London, 5–10 September 1966.

² $\log_2 x$ denotes the logarithm with base 2 of the positive number x ; $0 \log_2 \frac{1}{0}$ always means 0.

Let now $\xi = \xi(\omega) = (\xi_1(\omega), \dots, \xi_n(\omega))$ be an n -dimensional vector valued random variable, i. e., an $\mathcal{A}$ -measurable function defined on Ω and with values in the Euclidean space E_n of dimension n . We shall interpret ξ as an *observed sample*. As ξ and θ are random variables on the same probability space, by observing ξ we usually get some information on θ (except when θ and ξ are independent). After having observed ξ we may consider the *conditional* (or *posterior*) *distribution*

$$(1.3) \quad p_k(\xi) = \mathbf{P}(H_k|\xi)$$

of H_k given the value of ξ . The conditional probability of an event $A \in \mathcal{A}$ given the observed value of ξ is as usual defined as follows: Let $\mathcal{A}_\xi$ denote the least σ -algebra of subsets of Ω on which ξ is measurable (i. e., the σ -algebra generated by ξ). By supposition $\mathcal{A}_\xi$ is a subalgebra of $\mathcal{A}$. The conditional probability $\mathbf{P}(A|\xi)$ of an event A , given the value of ξ , is defined as an $\mathcal{A}_\xi$ -measurable function (random variable) such that for every $B \in \mathcal{A}_\xi$, one has

$$(1.4) \quad \int_B \mathbf{P}(A|\xi) dP = \mathbf{P}(AB).$$

As well known, $\mathbf{P}(A|\xi)$ is by (1.4) uniquely defined up to a set of measure 0 and $\{\mathbf{P}(H_1|\xi), \dots, \mathbf{P}(H_r|\xi)\}$ is with probability one a probability distribution, i. e., $\mathbf{P}\left(\sum_{k=1}^r \mathbf{P}(H_k|\xi) = 1\right) = 1$. Let us consider now the entropy of the conditional (a posteriori) distribution of θ given ξ , i. e., the quantity

$$(1.5) \quad \mathbf{H}(\theta|\xi) = \sum_{k=1}^r p_k(\xi) \log_2 \frac{1}{p_k(\xi)}.$$

We interpret $\mathbf{H}(\theta|\xi)$ as *the amount of information concerning θ still missing after having observed the sample ξ* . Clearly $\mathbf{H}(\theta|\xi)$ itself is a random variable (which is not only $\mathcal{A}$ -measurable but also $\mathcal{A}_\xi$ -measurable); its expectation $\mathbf{E}(\mathbf{H}(\theta|\xi))$ is interpreted as *the average amount of information still missing about θ after having observed ξ* . We shall call this quantity for the sake of brevity when there is no danger of misunderstanding simply „the amount of missing information”, and denote it by $R(\xi, \theta)$; i. e., we put³

$$(1.6) \quad R(\theta, \xi) = \mathbf{E}(\mathbf{H}(\theta|\xi)).$$

The *amount of information* $I(\theta, \xi)$ in the observed sample ξ with respect to the (unknown) parameter θ is defined as the average decrease of the entropy of θ by observing ξ ; that is, we put

$$(1.7) \quad I(\theta, \xi) = \mathbf{H}(\theta) - R(\theta, \xi).$$

Evidently the conditional (posterior) distribution $\{p_1(\xi), \dots, p_r(\xi)\}$ of θ is identical with its prior distribution $\{p_1, \dots, p_r\}$ if and only if ξ and θ are independent. In this case $R(\theta, \xi) = \mathbf{H}(\theta)$, i. e., $I(\theta, \xi) = 0$, that is the observation of the sample ξ does not give us any information on θ . In every other case one has $R(\theta, \xi) < \mathbf{H}(\theta)$

³ Here and in what follows $\mathbf{E}(\eta)$ denotes the expectation of the random variable η .

and thus $I(\theta, \xi) > 0$. This can be shown by Jensen's inequality as follows. As the function $x \log_2 \frac{1}{x}$ is concave in $(0, 1)$ and by Jensen's inequality for any concave function $f(x)$ and any random variable η the values of which are lying in the domain of definition of $f(x)$ one has

$$(1.8) \quad \mathbf{E}(f(\eta)) \leq f(\mathbf{E}(\eta))$$

it follows

$$(1.9) \quad \begin{aligned} R(\theta, \xi) &= \sum_{k=1}^r \int_{\Omega} p_k(\xi) \log_2 \frac{1}{p_k(\xi)} dP \leq \\ &\leq \sum_{k=1}^r \left(\int_{\Omega} p_k(\xi) dP \right) \frac{1}{\left(\int_{\Omega} p_k(\xi) d\xi \right)} = H(\theta) \end{aligned}$$

because by (1.4)

$$(1.10) \quad \int_{\Omega} p_k(\xi) dP = \mathbf{P}(H_k) = p_k.$$

Evidently there is equality in (1.9) if and only if the distribution $\{p_1(\xi), \dots, p_r(\xi)\}$ is (with probability 1) identical to the distribution $\{p_1, \dots, p_r\}$, i. e., if ξ and θ are independent.

Let $g(x)$ ($x \in E_n$) be any k -dimensional vector valued Borel measurable function defined on the n -dimensional space E_n . We shall call the random variable $g(\xi)$ a *statistic*. If after observing ξ we consider the value of the statistic $g(\xi)$ only, and disregard every information (on θ) contained in the observation of ξ and not contained in $g(\xi)$, we usually lose some amount of information, i. e.,

$$(1.11) \quad I(g(\xi), \theta) \leq I(\xi, \theta).$$

The inequality (1.11) is clearly equivalent to

$$(1.12) \quad R(\xi, \theta) \leq R(g(\xi), \theta).$$

To prove (1.12) we need the following Lemma 1 which is an immediate consequence of the definition of conditional probability.

LEMMA 1. If $f(x)$ is any Borel measurable function and $A \in \mathcal{A}$ any event, we have

$$(1.13) \quad \mathbf{E}(f(g(\xi))\mathbf{P}(A|g(\xi))) = \mathbf{E}(f(g(\xi))\mathbf{P}(A|\xi)).$$

Using Lemma 1, we obtain

$$(1.14) \quad R(\theta, g(\xi)) - R(\theta, \xi) = \mathbf{E} \left(\sum_{k=1}^r \mathbf{P}(H_k|\xi) \log_2 \frac{\mathbf{P}(H_k|\xi)}{\mathbf{P}(H_k|g(\xi))} \right).$$

Now we need the following simple

LEMMA 2. If $\{q_1, q_2, \dots, q_r\}$ and $\{Q_1, Q_2, \dots, Q_r\}$ are arbitrary probability distributions consisting of the same number r of terms, we have

$$(1.15) \quad \sum_{k=1}^r q_k \log_2 \frac{q_k}{Q_k} \geq 0$$

with equality standing in (1.15) if and only if $q_k = Q_k$ for $k = 1, 2, \dots, r$.

Applying Lemma 2, we obtain from (1.14) that (1.12) holds and there is equality in (1.12) if and only if with probability 1, one has

$$(1.16) \quad \mathbf{P}(H_k|\xi) = \mathbf{P}(H_k|g(\xi)) \quad (k=1, 2, \dots, r).$$

If (1.16) holds (with probability 1) we call $g(\xi)$ a *sufficient function of ξ for θ* (or a *sufficient statistic*). Thus a function of the observations is called sufficient for a parameter if and only if it contains all information in the observation which is relevant to the parameter, in the sense that there is equality in (1.11).

Note that if (1.16) holds and the random vector ξ has the conditional density $\varphi_k(x)$ under condition H_k , and $g(\varphi)$ has the density $\psi_k(g(x))$, then

$$\varphi_k(x) = \psi_k(g(x))\chi(x)$$

where the function $\chi(x)$ does not depend on k ; as clearly $\varphi_k(x)$, $\psi_k(g(x))$ and $\chi(x)$ are all independent from the prior distribution $\{p_1, \dots, p_r\}$ of θ , it follows that our definition of sufficiency is equivalent with the usual definition of a sufficient statistic in case both definitions are applicable. An advantage of our definition is that it does not depend on the existence of densities; besides it has a clear information-theoretical meaning.

Before proceeding further we prove the following

THEOREM 1. *The conditional distribution $\Pi(\xi) = (p_1(\xi), \dots, p_r(\xi))$ of θ given ξ , considered as a statistic, is sufficient with respect to θ .*

To prove our theorem it is clearly enough to show that

$$(1.17) \quad p(H_k|\Pi(\xi)) = p_k(\xi) \quad (k=1, 2, \dots, r).$$

But (1.17) is evidently true as $p_k(\xi)$ is $\mathcal{A}_{\Pi(\xi)}$ -measurable ($p_k(\xi)$ being the k -th component of the vector $\Pi(\xi)$), we get $p_k(\xi)$ by projecting the vector $\Pi(\xi)$ to the x_k -axis.)

The statement of Theorem 1 can be expressed by saying that the *conditional distribution of θ given ξ contains all information relevant on θ which is present in the sample ξ .*

§ 2. A Bayesian Version of the Fundamental Lemma of Neyman and Pearson

If we have to make a *decision* concerning the parameter θ , on the basis of the observed value of the sample ξ , i. e., after observing ξ we have to select one of the possible values of θ , this decision can be described by a Borel measurable function $D(\xi)$ of ξ , the set of values of which is the set $\{\theta_1, \theta_2, \dots, \theta_r\}$ of possible values of θ . The *error e* of such a decision is simply the probability of the decision being false, that is

$$(2.1) \quad e = \mathbf{P}(D(\xi) \neq \theta).$$

We define the *standard decision* $\Delta(\xi)$ as follows: we decide always in favor of that hypothesis H_k (that value θ_k of θ) which has the largest conditional probability given the value of ξ ; in case there is more than one value k such that $p_k(\xi) = \max_{1 \leq j \leq r} p_j(\xi)$, we select in some way one among those values—say the least such value of k . If another rule is applied we call the corresponding decision a *variant of the standard decision*.

It is easy to see that it does not matter much which one of these values of k we choose (i. e., whether we use the standard decision or one of its variants) as the error of the decision is independent from this selection. As a matter of fact if ε denotes the *error of the standard decision*, we obtain by the definition (1. 4) of conditional probabilities

$$(2. 2) \quad \varepsilon = \mathbf{P}(\Delta(\xi) \neq \theta) = 1 - \mathbf{P}(\Delta(\xi) = \theta) = 1 - \mathbf{E}(\mathbf{P}(\theta = \Delta(\xi)|\xi)).$$

Clearly if we change the definition of the standard decision for some value of ξ from $\Delta(\xi) = \theta_{k_1}$ to $\Delta(\xi) = \theta_{k_2}$ where $p_{k_1}(\xi) = p_{k_2}(\xi)$, then ε remains unchanged, because $\mathbf{P}(\theta = \Delta(\xi)|\xi) = p_{\Delta(\xi)}(\xi)$ is by definition not affected by such a change.

Now let $D(\xi)$ be any other decision, and e its error. Then we get, similarly to (2. 2)

$$(2. 3) \quad e = 1 - \mathbf{E}(\mathbf{P}(\theta = D(\xi)|\xi)).$$

Thus we have

$$(2. 4) \quad e - \varepsilon = \mathbf{E}(\mathbf{P}(\theta = \Delta(\xi)|\xi) - \mathbf{P}(\theta = D(\xi)|\xi)).$$

The random variable, the expectation of which gives the difference $e - \varepsilon$, is clearly always non-negative, because for each value of ξ we have for some value of k (namely $k = D(\xi)$)

$$(2. 5) \quad \mathbf{P}(\theta = \Delta(\xi)|\xi) - \mathbf{P}(\theta = D(\xi)|\xi) = \max_{1 \leq j \leq r} p_j(\xi) - p_k(\xi) \geq 0.$$

Thus we have proved the following

THEOREM 2. *No decision can have a smaller error than the standard decision.*

Clearly if the decision $D(\xi)$ is such that $\mathbf{P}(\theta = D(\xi)|\xi) \neq \mathbf{P}(\theta = \Delta(\xi)|\xi)$ with positive probability, then $e > \varepsilon$. However, if $\mathbf{P}(\theta = D(\xi)|\xi) = \mathbf{P}(\theta = \Delta(\xi)|\xi)$ with probability 1, this means that the decision $D(\xi)$ differs from the decision $\Delta(\xi)$ only in that in case a tie presents itself, i. e., if the value of k for which $p_k(\xi)$ is maximal is not unique, the decision $D(\xi)$ prescribes another choice among those values k for which $p_k(\xi)$ is maximal as $\Delta(\xi)$; thus *except for variants of the standard decision every other decision has a definitely larger error than the standard decision* (or any of its variants).

Note that the difference between Theorem 2 and the usual form of the Neyman—Pearson lemma consists in that we have supposed that the parameter θ is a random variable, i. e. we have taken the Bayesian point of view. Thus we do not distinguish between errors of the first and second kind: only one sort of error is possible. A decision is namely either correct, or wrong, and the error of a decision is the probability of it being wrong. A formal difference of minor importance is that by using the general notion of a conditional probability we did not need any supposition concerning the existence of densities.

Note that it follows from Theorem 2 that the error of the standard decision is $\leq 1/2$ in the case $r=2$, because if $\bar{\Delta}$ means the decision which is the opposite of Δ , $\bar{\Delta}$ has the error $1 - \varepsilon$ and thus by Theorem 2, $\varepsilon \leq 1 - \varepsilon$.

As regards the standard decision $\Delta(\xi)$, we may compute the amount of information contained in the value of $\Delta(\xi)$ with respect to θ , i. e., the quantity $I(\Delta(\xi), \theta)$. Clearly one has $I(\Delta(\xi), \theta) \leq I(\xi, \theta)$ with strict inequality except when $\Delta(\xi)$ is a sufficient function of ξ concerning θ ; thus *even when the best possible decision is adopted some information is lost*. The explanation of this somewhat paradoxically

sounding statement is that usually the information on θ contained in the observed value of ξ is not enough to decide with certainty which is the value of the parameter, it only gives us a (conditional) probability distribution on the possible values. If, nevertheless, we insist on choosing one of the possible values and rejecting all the others, we naturally lose by this a certain amount of information.

§ 3. Estimating the Error of the Standard Decision by the Amount of Missing Information

We prove in this section the following ⁴

THEOREM 3. *Let ε denote the error of the standard decision and $R = R(\theta, \xi)$ the amount of missing information, then the following inequality holds*

$$(3.1) \quad \log_2 \frac{1}{1-\varepsilon} \leq R,$$

or expressed otherwise

$$(3.2) \quad \varepsilon \leq 1 - \frac{1}{2^R}.$$

PROOF OF THEOREM 3. Let us denote for the sake of brevity the event $\Delta(\xi) = \theta_j$ by A_j ($j = 1, 2, \dots$). Then we have clearly

$$(3.3) \quad R = \mathbf{E}(\mathbf{H}(\theta|\xi)) = \sum_{j=1}^r \mathbf{P}(A_j) \mathbf{E}(\mathbf{H}(\theta|\xi)|A_j).$$

(Here and in what follows $\mathbf{E}(\eta|B)$ denotes the conditional expectation of the random variable η with respect to the condition B , when B is an event such that $\mathbf{P}(B) > 0$.) Now by definition under condition A_j we have $p_k(\xi) \leq p_j(\xi)$ for $k = 1, 2, \dots, r$; in view of (1.5) we get that

$$(3.4) \quad R \geq \sum_{j=1}^r \mathbf{P}(A_j) \mathbf{E} \left(\log_2 \frac{1}{p_j(\xi)} \middle| A_j \right).$$

Applying now Jensen's inequality to the convex function $\log_2 \frac{1}{x}$ ($0 \leq x \leq 1$), it follows that

$$(3.5) \quad R \geq \sum_{j=1}^r \mathbf{P}(A_j) \log_2 \frac{1}{\mathbf{E}(p_j(\xi)|A_j)}.$$

Now it follows from (1.4) that

$$(3.6) \quad \mathbf{E}(p_j(\xi)|A_j) = \frac{\int \mathbf{P}(\theta = \theta_j|\xi) dP}{\mathbf{P}(A_j)} = \mathbf{P}(\Delta(\xi) = \theta_j|A_j).$$

⁴ In our previous paper [3] we have proved only the weaker estimate $\varepsilon \leq R$. Clearly (3.1) implies not only $\varepsilon \leq R$ but also $\frac{\varepsilon}{\ln 2} \leq R$.

Thus we obtain from (3.5)

$$(3.7) \quad R \cong \sum_{j=1}^r \mathbf{P}(A_j) \log_2 \frac{1}{\mathbf{P}(\Delta(\xi) = \theta | A_j)}.$$

We need now Jensen's inequality, in the form that if $f(x)$ is a convex function, $x_1, \dots, x_r$ any values in the domain of definition of $f(x)$ and $w_1, \dots, w_r$ non-negative numbers with sum equal to one, then

$$(3.8) \quad \sum_{j=1}^r w_j f(x_j) \cong f\left(\sum_{j=1}^r w_j x_j\right).$$

Applying (3.8) it follows from (3.7) that

$$(3.9) \quad R \cong \log_2 \frac{1}{\sum_{j=1}^r \mathbf{P}(A_j) \mathbf{P}(\Delta(\xi) = \theta | A_j)} = \log_2 \frac{1}{\mathbf{P}(\Delta(\xi) = \theta)} = \log_2 \frac{1}{1-\varepsilon}$$

and this proves (3.1).

In our previous paper [4] we have shown for the special case $r=2$ that the inequality $2\varepsilon \leq R$ holds; for this special case this is slightly better than (3.1). We reproduce here the proof of this inequality as it requires only a few lines. Let the possible values of θ be θ_0 and θ_1 , the corresponding hypotheses $\theta = \theta_0$ and $\theta = \theta_1$ shall be denoted by H_0 and H_1 respectively. Put

$$(3.10) \quad h(x) = x \log_2 \frac{1}{x} + (1-x) \log_2 \frac{1}{1-x}.$$

Then we have evidently $h(x) = h(1-x)$ and $h(x) \geq 2x$ for $0 \leq x \leq 1/2$. Let us put

$$(3.11) \quad p^*(\xi) = \begin{cases} p_0(\xi) & \text{if } p_0(\xi) \leq \frac{1}{2} \text{ i. e. if } \Delta(\xi) = \theta_1 \\ p_1(\xi) & \text{if } p_0(\xi) \geq \frac{1}{2} \text{ i. e. if } \Delta(\xi) = \theta_0. \end{cases}$$

Then we have clearly $p^*(\xi) \leq \frac{1}{2}$ further

$$(3.12) \quad R = \mathbf{E}(h(p^*(\xi))) \geq 2\mathbf{E}(p^*(\xi)).$$

Denoting the event $\Delta(\xi) = \theta_0$ by B_0 and the event $\Delta(\xi) = \theta_1$ by B_1 we obtain

$$(3.13) \quad R \geq 2 \left(\int_{B_1} p_0(\xi) dP + \int_{B_0} p_1(\xi) dP \right).$$

As by (1.4) we have

$$(3.14) \quad \int_{B_1} p_0(\xi) dP = \mathbf{P}(H_0 B_1) \quad \text{and} \quad \int_{B_0} p_1(\xi) dP = \mathbf{P}(H_1 B_0)$$

it follows that

$$(3.15) \quad R \geq 2(\mathbf{P}(H_0 B_1) + \mathbf{P}(H_1 B_0)) = 2\varepsilon,$$

which was to be proved.

Returning to the general case, we mention that one can also get an upper bound for the amount of missing information by means of the error of the standard decision. In this direction the following theorem is known (see [6] p. 35.).

THEOREM 4. *One has*

$$(3.16) \quad R \leq h(\varepsilon) + \varepsilon \log_2(r-1)$$

where $h(x)$ is defined by (3.10).

My thanks are due to G. KATONA, who called my attention to the fact that the estimation (3.16), proved first by R. M. FANO [7], is slightly sharper than a similar estimate which I have found previously.

§ 4. Conclusion

It follows from Theorems 3 and 4 that if we have an infinite sequence of observations $\xi_1, \xi_2, \dots, \xi_n, \dots$ each ξ_n being a random variable on the probability space S (it is not a restriction to suppose that each ξ_n is real valued), and $\xi^{(n)}$ denotes the sample $(\xi_1, \xi_2, \dots, \xi_n)$ further Δ_n the standard decision concerning the true value of θ taken on the basis of observing the sample $\xi^{(n)}$ and ε_n the error of the decision Δ_n , and if finally R_n denotes the average amount of information on θ still missing after having observed the sample $\xi^{(n)}$, then $\lim_{n \rightarrow \infty} \varepsilon_n = 0$ if and only if $\lim_{n \rightarrow \infty} R_n = 0$. This shows that to get in the limit all information on θ which is needed, is equivalent with having the possibility to make decisions on the true value of θ the probability of correctness of which is in the limit equal to 1. By other words the information-theoretical point of view is in accordance with the usual point of view of statistics.

REFERENCES

- [1] RÉNYI, A.: On the amount of information concerning an unknown parameter in a sequence of observations, *Magyar Tud. Akad. Mat. Kutató Int. Közl.* 9 (1964) 617—625.
- [2] RÉNYI, A.: On the amount of information in a frequency count, *35th Session of the International Statistical Institute*, Beograd, 1965, 1—8.
- [3] RÉNYI, A.: On the amount of missing information and the Neyman-Pearson lemma, *Festschrift for J. Neyman*, Wiley, London, 1966, 281—288.
- [4] RÉNYI, A.: On the amount of information in a random variable concerning an event, *Journal of Mathematical Sciences (Delhi)* 1 (1966) 30—33.
- [5] RÉNYI, A.: On some basic problems of statistics from the point of view of information theory. *Proceedings of the 5th Berkeley Symposium* (in print).
- [6] FEINSTEIN, A.: *Foundations of Information Theory*, McGraw-Hill, New York, 1958.
- [7] FANO, R. M.: *Statistical Theory of Communication*, MIT, Cambridge, Mass., 1954.

ON THE HEIGHT OF TREES

A. RÉNYI and G. SZEKERES¹

1. Introduction

In this note we shall deal with the enumeration of labelled trees of given order and given height over a selected point.

An undirected graph is called a tree if it is connected and contains no cycle. If we select any two vertices P and Q of a tree T , there is evidently a uniquely determined path in T leading from P to Q . We shall call the length of this path (i.e. the number of edges in the path) the distance of P and Q in T and denote it by $d_T(P, Q)$. If a vertex P is distinguished as the root of T , we define the height of T over P as the length of the longest path in T starting from P ; thus if $h_P(T)$ denotes the height of T over the root P , we have

$$(1.1) \quad h_P(T) = \max_{Q \in T} d_T(P, Q).$$

Let us consider the set $\mathcal{T}_n$ of all possible trees with n given labelled vertices $P_1, P_2, \dots, P_n$. According to a classical result of Cayley [1] if t_n denotes the number of elements of $\mathcal{T}_n$, we have

$$(1.2) \quad t_n = n^{n-2}$$

Let $t_n(k)$ denote the number of those trees $T \in \mathcal{T}_n$ for which $h_{P_1}(T) \leq k$. Clearly

$$(1.3) \quad t_1(0) = 1, \quad t_n(0) = 0 \quad \text{for } n > 1$$

and

$$(1.4) \quad t_n(k) = t_n \quad \text{for } k \geq n-1.$$

J. Riordan [2] has shown that the enumerator

$$(1.5) \quad G_k(x) = \sum_{n=1}^{\infty} \frac{t_n(k)}{(n-1)!} x^n \quad (k = 0, 1, \dots)$$

¹ Part of this work was done at the fifth Summer Research Institute of the Australian Mathematical Society in Canberra. The first author is greatly indebted to the Australian National University for its generous support of his visit to the Institute.

satisfies the recursion formula

$$(1.6) \quad G_{k+1}(x) = x \exp G_k(x) \quad (k = 0, 1, \dots)$$

with

$$(1.7) \quad G_0(x) = x;$$

the latter follows from (1.3) and (1.5).

From the recursion formula (1.6) one can determine $t_n(k)$ for any k and n ($0 \leq k \leq n-1$). For instance

$$(1.8) \quad G_1(x) = xe^x, \quad G_2(x) = xe^{xe^x}, \quad \text{etc.,}$$

and thus

$$(1.9) \quad t_n(1) = 1 \quad (n = 1, 2, \dots)$$

$$(1.10) \quad t_n(2) = \sum_{m=0}^{n-1} \binom{n-1}{m} m^{n-m-1} \quad (n = 1, 2, \dots)$$

and generally for $k \geq 1$

$$(1.11) \quad t_n(k) = \sum_{\substack{m_1 + \dots + m_k = n-1 \\ m_i \geq 0}} \frac{(n-1)!}{m_1! m_2! \dots m_k!} m_1^{m_1} m_2^{m_2} \dots m_k^{m_k} \quad (i = 1, 2, \dots, k).$$

In these formulae 0^0 always means 1.

In view of (1.2) and (1.4) one has

$$(1.12) \quad \lim_{k \rightarrow \infty} G_k(x) = \sum_{n=1}^{\infty} \frac{n^{n-2}}{(n-1)!} x^n$$

provided that the series on the right of (1.12) is convergent. But the series

$$(1.13) \quad y = \sum_{n=1}^{\infty} \frac{n^{n-2}}{(n-1)!} x^n$$

converges for $|x| \leq 1/e$ and represents the inverse function of

$$(1.14) \quad x = ye^{-y}.$$

This equation also follows from (1.6) and (1.12).

Riordan [2] obtained the formula (1.6) as a special case of a more general result on enumerators of trees. In § 2 we shall give direct proofs of (1.6) and (1.11).

In § 3 we shall investigate the asymptotic distribution of

$$(1.15) \quad d_n(k) = t_n(k) - t_n(k-1),$$

i.e. the number of trees $T \in \mathcal{T}_n$ having exact height k over P_1 . Let us

mention that if $D(T)$ denotes the diameter of T (i.e. the length of the longest path in T) one has evidently

$$(1.16) \quad \frac{1}{2}D(T) \leq \min_i h_{P_i}(T) \leq h_{P_i}(T) \leq \max_i h_{P_i}(T) \leq D(T).$$

Thus the study of the distribution of $h_{P_i}(T)$ for $T \in \mathcal{T}_n$ gives us also some information on the distribution of $D(T)$.

Our thanks are due to F. Harary and J. W. Moon for calling our attention to the paper [2] of Riordan.

2. Proof of the recursion formula

To prove (1.6) we start from the formula

$$(2.1) \quad t_n(k) = \sum_{p=1}^{n-1} \binom{n-1}{p} \sum_{m_1+\dots+m_p=n-1} \frac{(n-1-p)!}{(m_1-1)! \cdots (m_p-1)!} t_{m_1}(k-1) \cdots t_{m_p}(k-1).$$

(2.1) can be proved as follows: Let E denote the set of those points of $T \in \mathcal{T}_n$ which are directly connected (i.e. connected by an edge) with P_1 . If p is the number of elements of E then $1 \leq p \leq n-1$ and denoting these points by $Q_1, \dots, Q_p$, the points Q_i can be selected in $\binom{n-1}{p}$ ways. All the remaining $n-1-p$ points P_m ($P_m \neq Q_j$, $1 \leq j \leq p$; $P_m \neq P_1$) can be classified into p classes which are defined as follows: P_m lies in the j -th class ($j = 1, 2, \dots, p$) if the unique path from P_1 to P_m goes through Q_j . Clearly if the j -th class contains m_j-1 points, these points together with Q_j form a tree of order m_j and height $\leq k-1$ over the basic point Q_j . Thus (2.1) follows.

Multiplication of (2.1) by $x^n/(n-1)!$ and summation for $n = 1, 2, \dots$ leads immediately to (1.6). (1.11) can be deduced from (1.6) by using several times the power series of the exponential function. It can also be proved directly as follows:

Let $T \in \mathcal{T}_n$ be a tree the height of which over the basic point P_1 is $\leq k$. Then all points of T different from P_1 can be classified into k classes, the j -th class $\mathcal{C}_j$, consisting of those points whose distance from P_1 is equal to j ($1 \leq j \leq k$). Let m_j denote the number of points in the class $\mathcal{C}_j$, ($1 \leq j \leq k$); then

$$\sum_{j=1}^k m_j = n-1.$$

If the numbers m_j are fixed, the distribution of the $n-1$ points in the classes $\mathcal{C}_j$ can be carried out in $(n-1)!/m_1! \cdots m_k!$ ways. Now evidently each point in the class $\mathcal{C}_1$ is directly connected with P_1 , each point in $\mathcal{C}_2$ is directly connected with some point in $\mathcal{C}_1$ etc., each point in $\mathcal{C}_k$ is directly

connected with some point of $\mathcal{C}_{k-1}$. As the connections can be established in $m_1^{m_1} m_2^{m_2} \cdots m_{k-1}^{m_{k-1}}$ different ways and by choosing these connections the tree T is completely determined, (1.11) follows.

For $d_n(k) = t_n(k) - t_n(k-1)$ the proof of (1.11) gives

$$(2.2) \quad d_n(k) = \sum_{\substack{m_1 + \cdots + m_{k-1} = n-1 \\ m_i \geq 1}} \frac{(n-1)!}{m_1! \cdots m_{k-1}!} m_1^{m_1} m_2^{m_2} \cdots m_{k-1}^{m_{k-1}}, \\ (i = 1, \dots, k),$$

If $d_n(k, m)$ denotes the number of trees $T \in \mathcal{T}_n$ for which $h_{P_1}(T) = k$ and in which there are exactly m points connected with P_1 by an edge then (2.2) gives

$$(2.3) \quad d_n(k, m) = \frac{1}{m!} \sum_{\substack{m_1 + \cdots + m_{k-1} = n-1-m \\ m_i \geq 1}} \frac{(n-1)!}{m_1! \cdots m_{k-1}!} m_1^{m_1} \cdots m_{k-1}^{m_{k-1}}.$$

From here the following recursion formula can be deduced:

$$(2.4) \quad d_n(k, m) = \binom{n-1}{m} \sum_{p=1}^{n-1-m} m^p d_{n-m}(k-1, p).$$

Similarly if $t_n(k, m)$ is the number of those trees $T \in \mathcal{T}_n$ which have height $\leq k$ over P_1 and in which the number of points having distance k from P_1 equals m , then

$$(2.5) \quad t_n(k, m) = \frac{1}{m!} \sum_{m_1 + \cdots + m_{k-1} = n-1-m} \frac{(n-1)!}{m_1! \cdots m_{k-1}!} m_1^{m_1} \cdots m_{k-2}^{m_{k-2}} m_{k-1}^m,$$

and

$$(2.6) \quad t_n(k, m) = \binom{n-1}{m} \sum_{p=1}^{n-1-m} p^m t_{n-m}(k-1, p).$$

Thus putting

$$(2.7) \quad F_k(x, z) = \sum_{n=1}^{\infty} \sum_{m=0}^{n-1} \frac{t_n(k, m)}{(n-1)!} x^{n-m} z^m$$

we have the recursion formula

$$(2.8) \quad F_k(x, z) = F_{k-1}(x, xe^z)$$

with $F_0(x, z) = z$. We obtain

$$F_1(x, z) = xe^z, \quad F_2(x, z) = xe^{xe^z}, \text{ etc.,}$$

hence

$$(2.9) \quad F_{k+1}(x, z) = x \exp F_k(x, z)$$

further

$$(2.10) \quad F_k(x, x) = F_{k+1}(x, 0) = G_k(x).$$

3. The asymptotic distribution of $d_n(k)$

We consider now the asymptotic distribution of $d_n(k)$ when n and k are large. We shall make use of the generating function

$$(3.1) \quad G_k(x) - G_{k-1}(x) = \sum_{n=1}^{\infty} \frac{d_n(k)}{(n-1)!} x^n$$

where

$$(3.2) \quad G_0(x) = x, \quad G_k(x) = x \exp G_{k-1}(x) \quad (k = 1, 2, \dots)$$

by (1.5) and (1.15). From (3.2) it is seen that $G_k(z) - G_{k-1}(z)$ is an entire function and hence

$$(3.3) \quad \frac{d_n(k)}{(n-1)!} = \frac{1}{2\pi i} \int_{C+} \frac{G_k(z) - G_{k-1}(z)}{z^{n+1}} dz$$

where C is any circular path with centre 0. For the radius of C we shall take $r = e^{-1}$; this is the largest positive value of r for which the sequence $G_k(r)$, $k = 1, 2, \dots$ tends to a finite limit, namely $\lim_{k \rightarrow \infty} G_k(e^{-1}) = 1$. Moreover if k is of order $\sqrt{n}$ which is the case of principal interest then the point e^{-1} lies very close to a saddle point of the integrand.

As in (2.9), write for a fixed complex number ζ

$$(3.4) \quad F_0(\zeta, z) = z,$$

$$(3.5) \quad F_k(\zeta, z) = \zeta \exp F_{k-1}(\zeta, z) \quad (k = 1, 2, \dots).$$

Thus $F_k(\zeta, z)$ is the k -th iterate of

$$(3.6) \quad F(\zeta, z) = \zeta e^z \quad (\zeta \text{ fixed})$$

and

$$(3.7) \quad G_k(\zeta) = F_k(\zeta, \zeta) = F_{k+1}(\zeta, 0),$$

as in (2.10).

In the particular case of $\zeta = e^{-1}$, $z = 1$ is a fixed point with multiplier 1 of the function $F(e^{-1}, z) = e^{z-1}$; in fact $F(e^{-1}, 1) = 1$, $F'(e^{-1}, 1) = 1$.

The sequence

$$(3.8) \quad \gamma_k = F_k(e^{-1}, e^{-1}) = G_k(e^{-1}), \quad k = 0, 1, 2, \dots$$

satisfies

$$(3.9) \quad \gamma_k = \exp(\gamma_{k-1} - 1), \quad k = 1, 2, \dots$$

and has an asymptotic expansion

* $z = a$ is a fixed-point with multiplier μ of the function $F(z)$ if $F(a) = a$ and $F'(a) = \mu$. If $|\mu| < 1$, the fixed-point is called attractive. (Fatou [4], p. 186).

$$(3.10) \quad \gamma_k \cong 1 - \frac{2}{k} + \frac{2}{3} \frac{\log k}{k^2} + \frac{c}{k^2} + \dots \quad (k \rightarrow \infty)$$

where c is a certain constant (see e.g. [3], Lemma 3, p. 247). For all other values of ζ on the circle

$$\zeta = e^{-1+it}, \quad -\pi \leq t \leq \pi,$$

$F(\zeta, z)$ has an attractive fixed-point $\omega = u+iv$ with multiplier ω ($|\omega| < 1$), given by the equation

$$(3.11) \quad \omega = \zeta e^\omega = e^{-1+it+\omega}.$$

These fixed-points lie on the curve

$$(3.12) \quad u^2 + v^2 = e^{2(u-1)}, \quad u \leq 1$$

with

$$(3.13) \quad \tan(v+t) = v/u = u^{-1} (e^{2(u-1)} - u^2)^{\frac{1}{2}}.$$

Thus to each $\zeta = e^{-1+it}$ there corresponds a unique $\omega = \omega(\zeta) = u+iv$ on the curve (3.12). In the neighbourhood of $t = 0$, i.e. of $u = 1$, $v = 0$, the curve of fixed-points has a double point and satisfies an expansion

$$(3.14) \quad \begin{aligned} u &= 1 - \sqrt{t} + 0 \cdot t + at\sqrt{t} + \dots, \\ v &= \sqrt{t} - \frac{2}{3}t + bt\sqrt{t} + \dots \quad \text{if } t > 0 \\ &= -\sqrt{-t} - \frac{2}{3}t - bt\sqrt{-t} + \dots \quad \text{if } t < 0. \end{aligned}$$

The fixed-points ω on (3.12) are attractive for all z on the circle $|z| = e^{-1}$; in fact

$$(3.15) \quad |F(\zeta, z)| = |\zeta e^z| < 1$$

for all $|\zeta| = e^{-1}$, $\operatorname{Re} z < 1$ and the functions

$$F_k(\zeta, z), \quad |\zeta| = e^{-1}, \quad k = 0, 1, 2, \dots$$

form a normal family on the half plane $\operatorname{Re} z < 1$.

By a more refined argument one can show that if we set

$$(3.16) \quad D_k(\zeta) = G_k(\zeta) - \omega(\zeta)$$

then $D_k(\zeta)/\omega(\zeta)^k$ is uniformly bounded for all $\zeta = e^{-1+it}$, $-\pi \leq t \leq \pi$ and $k = 0, 1, 2, \dots$, i.e.

$$(3.17) \quad |D_k(\zeta)| < A|\omega(\zeta)|^k$$

for a suitable positive constant A . For we have

$$(3.18) \quad D_k(\zeta) = \omega(\zeta)[\exp D_{k-1}(\zeta) - 1], \quad k = 1, 2, \dots$$

by (3.2), (3.11) and (3.16), and the sequence behaves very nearly like the sequence D_k^* given by the recursion

$$(3.19) \quad D_k^* = \omega D_{k-1}^* / (1 - \frac{1}{2} D_{k-1}^*).$$

For this sequence the statement can be verified by direct calculation since

$$(3.20) \quad D_k^* = - \frac{2\omega^k}{1 + \omega + \dots + \omega^{k-1} - a}, \quad a = 1/D_0^*.$$

We omit details.

For $|t| < ((\log^2 k)/k)^2$ the sequence $G_k(\zeta)$, $k = 0, 1, 2, \dots$ has a uniform asymptotic expansion

$$(3.21) \quad G_k(e^{-1+it}) \cong 1 - \frac{2}{k} \tau \cot \tau + \frac{2}{3} \frac{\tau^2}{\sin^2 \tau} \frac{\log k}{k^2} \\ + \frac{1}{k^2} \left[c \frac{\tau^2}{\sin^2 \tau} + \frac{2}{3} \tau^2 \left(2 + \log \frac{\sin \tau}{\tau} \right) \right] + \dots$$

where

$$(3.22) \quad it = 2\tau^2/k^2$$

and c is the constant in (3.10). The expansion becomes (3.10) for $\tau = 0$ and can be verified formally by setting

$$(3.23) \quad G_k(e^{-1+it}) \cong 1 - \frac{\theta_1(\tau)}{k} + \theta_2(\tau) \frac{\log k}{k^2} + \frac{\theta_3(\tau)}{k^2} + \dots$$

and using (3.2).

We obtain (for fixed t) by (3.22)

$$G_{k+1}(e^{-1+it}) \cong 1 - \frac{\theta_1(\tau + \tau/k)}{k+1} + \theta_2(\tau + \tau/k) \frac{\log(k+1)}{(k+1)^2}$$

$$+ \theta_3(\tau + \tau/k) \frac{1}{(k+1)^2} + \dots$$

$$\cong 1 - \theta_1/k + \theta_1/k^2 - \theta_1/k^3 - \tau\theta_1'/k^2 \\ + \tau\theta_1'/k^3 - \tau^2\theta_1''/2k^3 + \theta_2 \log k/k^2 \\ - 2\theta_2 \log k/k^3 + \theta_2/k^3 + \tau\theta_2' \log k/k^3 \\ + \theta_3/k^2 - 2\theta_3/k^3 + \tau\theta_3'/k^3 + \dots,$$

$$\exp(G_k - 1 + 2\tau^2/k^2) \cong \exp \left[- \frac{\theta_1}{k} + \theta_2 \frac{\log k}{k^2} + \frac{\theta_3}{k^2} + \frac{2\tau^2}{k^2} + \dots \right]$$

$$\cong 1 - \theta_1/k + \theta_2 \log k/k^2 + (\theta_3 + 2\tau^2)/k^2 \\ + \frac{1}{2}\theta_1^2/k^2 - \theta_1\theta_2 \log k/k^3 - \theta_1\theta_3/k^3 \\ - 2\theta_1\tau^2/k^3 - \frac{1}{6}\theta_1^3/k^3 + \dots$$

where values of the function θ_i and their derivatives are taken at τ . These two expressions are equal by (3.2), hence comparing coefficients

$$(3.24) \quad \theta_1 - \tau\theta'_1 = \frac{1}{2}\theta_1^2 + 2\tau^2,$$

$$(3.25) \quad \tau\theta'_2 - 2\theta_2 = -\theta_1\theta_2,$$

$$(3.26) \quad -\theta_1 + \tau\theta'_1 - \frac{1}{2}\tau^2\theta''_1 + \theta_2 - 2\theta_3 + \tau\theta'_3 = -\theta_1\theta_3 - 2\tau^2\theta_1 - \frac{1}{6}\theta_1^3.$$

With the initial conditions $\theta_1(0) = 2$, $\theta_2(0) = \frac{2}{3}$, $\theta_3(0) = c$, obtained from (3.10), the equations (3.24)–(3.26) give

$$\theta_1(\tau) = 2\tau \cot \tau, \quad \theta_2(\tau) = \frac{2}{3} \frac{\tau^2}{\sin^2 \tau},$$

$$\theta_3(\tau) = c \frac{\tau^2}{\sin^2 \tau} + \frac{2}{3}\tau^2 \left(2 + \log \frac{\sin \tau}{\tau} \right), \quad \text{i.e. (3.21).}$$

Thus we only have to prove the existence of an expansion of the form (3.23). This can be achieved by a step by step method such as the one used in [3] for the proof of general expansions of the type (3.11); we omit details. Actually we only need the expansion in the weaker form

$$(3.27) \quad G_k(e^{-1+it}) = 1 - \frac{2}{k} \tau \cot \tau + O(k^{-1-2\delta})$$

for some $\delta > 0$ when $|t| \leq ((\log^2 k)/k)^2$.

We then get from (3.2), since

$$2\tau \cot \tau = O(k \sqrt{|t|}) = O(\log^2 k),$$

$$\begin{aligned} G_k(e^{-1+it}) - G_{k-1}(e^{-1+it}) &= \exp(-1+it+G_{k-1}) - G_{k-1} \\ &= it + \frac{1}{2}(G_{k-1}-1)^2 + O(k^{-3+\delta}) \\ &= 2\tau^2(1+\cot^2 \tau)/k^2 + O(k^{-2-\delta}), \end{aligned}$$

$$(3.28) \quad G_k(e^{-1+it}) - G_{k-1}(e^{-1+it}) = \frac{2}{k^2} \frac{\tau^2}{\sin^2 \tau} + O(k^{-2-\delta})$$

for $|t| \leq ((\log^2 k)/k)^2$.

Now from (3.17)

$$\begin{aligned} G_k(e^{-1+it}) - G_{k-1}(e^{-1+it}) &= D_k(e^{-1+it}) - D_{k-1}(e^{-1+it}) \\ &= O\left(\left(1 - \frac{\log^2 k}{k}\right)^k\right) = O(e^{-\log^2 k}) \end{aligned}$$

for $|t| \geq ((\log^2 k)/k)^2$, by (3.14), hence by (3.3) and (3.28)

$$(3.29) \quad \frac{d_n(k)}{(n-1)!} = \frac{1}{2\pi i} \frac{2e^n}{k^2} \left(\int_{|t| \leq ((\log^2 k)/k)^{1/2}} \frac{\tau^2}{\sin^2 \tau} e^{-n i t} i dt + O(k^{-2-\delta}) \right) \\ \cong \frac{1}{2\pi i} \frac{8e^n}{k^4} \int_{\Gamma} \frac{\tau^3}{\sin^2 \tau} e^{-\beta \tau^2} d\tau$$

by (3.22), where

$$(3.30) \quad \beta = 2n/k^2$$

and Γ is the path

$$\tau = (i-1)u, \quad -\frac{1}{2} \log^2 k \leq u \leq 0$$

$$\tau = (i+1)u, \quad 0 \leq u \leq \frac{1}{2} \log^2 k.$$

Hence

$$\frac{d_n(k)}{(n-1)!} \cong \frac{8e^n}{k^4} \sum_{p=1}^{\infty} \operatorname{res}_{\tau=p\pi} \left(\frac{\tau^3}{\sin^2 \tau} e^{-\beta \tau^2} \right).$$

By using Stirling's formula we obtain from here

$$(3.31) \quad p_n(k) = \frac{d_n(k)}{n^{n-2}} \cong 2 \left(\frac{2\pi}{n} \right)^{\frac{1}{2}} \beta^{\frac{1}{2}} \sum_{p=1}^{\infty} (2p^4 \pi^4 \beta - 3p^2 \pi^2) e^{-\beta \pi^2 p^2}$$

for large n and k where β is given by (3.30).

This is the required asymptotic probability distribution. Note that

$$\sum_{k=1}^{n-1} p_n(k) \sim 2 \left(\frac{2\pi}{n} \right)^{\frac{1}{2}} \int_0^{n-1} \beta^{\frac{1}{2}} \sum_{p=1}^{\infty} (2p^4 \pi^4 \beta - 3p^2 \pi^2) e^{-\beta \pi^2 p^2} dk \\ \cong 2\pi^{\frac{1}{2}} \int_0^{\infty} \sum_{p=1}^{\infty} \beta^{\frac{1}{2}} (-3p^2 \pi^2 + 2p^4 \pi^4 \beta) e^{-\beta \pi^2 p^2} d\beta \\ = 2\pi^{\frac{1}{2}} \lim_{\epsilon \rightarrow 0} \left[- \sum_{p=1}^{\infty} 2p^2 \pi^2 \beta^{\frac{1}{2}} e^{-\beta \pi^2 p^2} \right]_{\epsilon}^{\infty} \\ = \lim_{\beta \rightarrow 0} 4\pi^{\frac{1}{2}} \beta^{\frac{1}{2}} \sum_{p=1}^{\infty} p^2 e^{-\beta \pi^2 p^2} \\ = 4\pi^{\frac{1}{2}} \int_0^{\infty} u^2 e^{-u^2} du = 1,$$

as required.

The maximum of the distribution curve is reached when in (3.31), $(d/d\beta)p_n(k) = 0$, i.e.

$$\sum_{p=1}^{\infty} (9p^4 \pi^4 \beta^2 - 6p^2 \pi^2 \beta - 2p^6 \pi^6 \beta^3) e^{-\beta \pi^2 p^2} = 0.$$

Numerically $\beta(\max) = 0.373138525$ and

$$(3.32) \quad k(\max) = 2.31515436 \sqrt{n}.$$

4. Conclusion

The result of the previous section can be stated as follows:

Let $\mathcal{H}_n$ be the height over P_1 of a labelled random tree of order n i.e. of a tree selected at random from the set of n^{n-2} elements of $\mathcal{T}_n$ with uniform probability distribution. Then

$$(4.1) \quad \lim_{n \rightarrow \infty} P\left(\frac{\mathcal{H}_n}{\sqrt{2n}} < x\right) = H(x)$$

where

$$(4.2) \quad H(x) = 4x^{-3}\pi^{\frac{1}{2}} \sum_{p=1}^{\infty} p^{\frac{1}{2}} e^{-\pi^2 p^2 / x^2}.$$

This can be transformed (e.g. by means of Poisson's formula) to the form

$$(4.3) \quad H(x) = \sum_{v=-\infty}^{\infty} e^{-v^2 x^2} (1 - 2v^2 x^2)$$

whence

$$(4.4) \quad h(x) = H'(x) = 4x \sum_{v=1}^{\infty} v^3 (2v^2 x^2 - 3) e^{-v^2 x^2}.$$

From (4.4) we can calculate all moments of the distribution function $H(x)$:

$$(4.5) \quad \begin{aligned} M_s &= \int_0^{\infty} x^s h(x) dx \\ &= 2\Gamma(\tfrac{1}{2}s+1)(s-1)\zeta(s) \end{aligned} \quad (s > 1)$$

where $\zeta(s) = \sum_{m=1}^{\infty} 1/m^s$. In particular we obtain for M_1 , since

$$(4.6) \quad \begin{aligned} \lim_{s \rightarrow 1} (s-1)\zeta(s) &= 1, \\ M_1 &= \sqrt{\pi}. \end{aligned}$$

Hence the expectation value of $\mathcal{H}_n$ is

$$(4.7) \quad E(\mathcal{H}_n) \sim \sqrt{2n\pi} = 2.50663\sqrt{n}$$

and the variance is

$$(4.8) \quad D^2 = M_2 - M_1^2 = \frac{\pi(\pi-3)}{3}.$$

References

- [1] Cayley, A., 'A theorem on trees', *Quart. J. of Pure and Applied Math.* 23 (1889), 376-378.
- [2] Riordan, J., 'The enumeration of trees by height and diameter', *IBM Journal of Research and Development* 4 (1960), 473-478.

- [3] Szekeres, G., 'Regular iteration of real and complex functions', *Acta Math.* 100 (1958), 103–258.
 [4] Fatou, M. P., 'Sur les équations fonctionnelles', *Bull. Soc. Math. France* 47 (1919), 161–271.

163

NOTE

The diameter (the length of a maximal path) of a labelled tree and the height (the length of the maximal path from the root) of a rooted labelled tree are defined in [1]. Some formulas are given in [1] and [2]. The first asymptotic results concerning the height are due to Rényi and Szekeres (No: 286). The limit distribution function of the height is given, and it is proved that the mean value of the height of a random rooted tree of n vertices is $\sim \sqrt{2n\pi}$. Meir and Moon considered the problem of the distance of two given points. They give combinatorial formulas as well as the limit distribution of the distance of two fixed vertices in a random tree. The mean value is $\sqrt{\frac{1}{2}\pi n}(1 + o(1))$. The question of the diameter is still unsolved.

De Bruijn, Knuth and Rice [4] have investigated the so-called ordered rooted trees. This means that the branches of the trees are ordered in the plane, and two isomorphic (in graph sense) trees are different if this ordering is different. Some formulas and asymptotic results are given. E.g. the mean value of the height of a random ordered rooted tree is

$$\sqrt{\pi n} - 1/2 + o\left(\frac{\log n}{\sqrt{n}}\right).$$

In some applications it turned out that the total height of a tree is also important. The total height is simply the sum of the distances of the root. Riordan and Sloane [5] have results concerning the generating functions of the total height of random ordered and non-ordered rooted trees.

Moon has further papers of random trees. Let us consider a random rooted tree. Starting from its root we choose randomly an edge, and going along this edge at the endpoint we choose another (different) edge, . . . and so on. After a certain number λ of steps this process stops. The limit distribution of λ is determined [6]. E.g. the limit of the mean value is $2e - 1$. The proof uses a result of No. 163. In [7] the following is considered. The edges of a random tree are omitted randomly with probability $1/2$. What is the number of vertices in a component? The limit distribution is determined. The limit of the mean value is 4.

[9] solves the following problem. If we have a random rooted tree, how many times we have to omit a random edge from the component containing the root in order to isolate the root. A limb is a path from an endpoint to the first point with valency > 2 . [10] gives the limit distribution and the limit of the mean value of a limb in random trees.

A connected problem is treated in [8], concerning the mappings of finite sets. A result of No. 163 is used. [Gy. K.]

REFERENCES

- [1] Harary, F. and Prins, G.: The number of homeomorphically irreducible trees and other species. *Acta Math.*, **101** (1959), 141–162.
- [2] Riordan, J.: The enumeration of trees by height and diameter. *IBM Journ. of Research and Dev.*, **4** (1960), 473–478.
- [3] Méir, A. and Moon, J. W.: The distance between points in random trees. *J. Combinatorial Th.*, **8** (1970), 99–103.
- [4] De Bruijn, N. G., Knuth, D. E. and Rice, S. O.: *The average height of planted plane trees, Graph theory and computing*. Ed. by R. C. Read, Acad. Press, New York – London, 1972.
- [5] Riordan, J. and Sloane, N. J. A.: The enumeration of rooted trees by total height. *J. Austral. Math. Soc.*, **10** (1969), 278–282.
- [6] Moon, J. W.: Climbing random trees. *Aequationes Math.*, **5** (1970), 68–74.
- [7] Moon, J. W.: A problem on random trees. *J. Combinatorial Th.*, Ser. B, **10** (1971), 201–205.
- [8] Сачков, В. Н.: Отображения конечного множества с ограничениями на контуры и высоту. *Теория вероятностей*, **17** (1972), 679–694.
- [9] Meir, A. and Moon J. W.: Cutting down random trees. *J. Austral Math. Soc.*, **11** (1970), 313–324.
- [10] Moon, J. W.: The length of limbs of random trees. *Mathematika*, **18** (1971), 78–81.

287. *Symposium on probability methods in analysis*. Lectures delivered at a symposium at Loutraki, Greece, 22.5 - 4.6. 1966. Lecture Notes in Mathematics. 31. Springer, Berlin, 1967; pp. 280 - 286.

Remarks on the Poisson process.

A. Rényi

The (inhomogeneous) Poisson process on the real line is usually characterised as a stochastic additive set function $\{ (E) \}$ defined for each bounded Borel subset E of the real line such that

a) the random variable $\{ (E) \}$ has for each bounded Borel set E a Poisson distribution, i.e.

$$(1) \quad P(\{ (E) \} = n) = \frac{[\lambda(E)]^n \cdot e^{-\lambda(E)}}{n!} \quad (n = 0, 1, \dots)$$

where $\lambda(E)$ is a nonatomic measure on the real line such that $\lambda(E)$ is finite for each finite interval E , and

b) if $E_1, E_2, \dots, E_n$ are mutually disjoint bounded Borel sets the random variables $\{ (E_1) \}, \dots, \{ (E_n) \}$ are independent.

If we put $\{ t \} = \{ ([0, t]) \}$ for $t > 0$, this means that $\{ t \}$ is a process with independent increments such that $\{ t \} - \{ s \}$ has a Poisson distribution with mean value

$\lambda(t) - \lambda(s)$ where $\lambda(t)$ is the λ -measure of the interval $[0, t]$ if $t > 0$ and $-\lambda(t)$ is the λ -measure of the interval $[t, 0]$ if $t < 0$. D.Szász (oral communication) asked the question whether there exists a point process for which a) holds but b) does not hold.

We shall show in this note that such a process does not exist, i.e. the usual supposition about independence in the above characterisation of the Poisson process is unnecessary, as it follows from the Poissonity of the distribution of $\{ (E) \}$; in other words we prove that the supposition b) is a consequence of the supposition a).

More exactly we prove the following

Theorem 1.

Let $\mathcal{I}$ denote the family of all subsets of the real line which can be obtained as the union of a finite number of disjoint finite intervals $[a, b)$ closed to the right and open to the left. Let $\{ (E) \}$ be an additive stochastic set function defined for each $E \in \mathcal{I}$, i.e. such that if E_1 and E_2 are disjoint one has $\{ (E_1 + E_2) \} = \{ (E_1) \} + \{ (E_2) \}$

Suppose that for each $E \in \mathcal{F}$ $\xi(E)$ has a Poisson distribution with mean value $\lambda(E)$ where $\lambda(E)$ is a nonatomic measure on the Borel subsets of the real line, which is finite for each $E \in \mathcal{F}$. Then it follows that if $E_1, \dots, E_n$ are disjoint sets ($E_k \in \mathcal{F}$) the random variables $\xi(E_1), \dots, \xi(E_n)$ are independent, i.e. $\xi(E)$ is a Poisson process.

Proof of theorem 1. Let $A(E)$ denote the event $\xi(E) = 0$. If E is the union of the disjoint sets $E_j \in \mathcal{F}$ ($j = 1, 2, \dots, n$) then (*) clearly $A(E) = A(E_1) \dots A(E_n)$ because $\xi(E) = \sum_{j=1}^n \xi(E_j)$ and thus $\xi(E) = 0$ iff $\xi(E_j) = 0$ for $j = 1, 2, \dots, n$. But by supposition

$$(2) \quad P(A(E)) = P(\xi(E) = 0) = e^{-\lambda(E)} = \prod_{j=1}^n e^{-\lambda(E_j)} = \prod_{j=1}^n P(A(E_j))$$

Thus it follows that if the sets $E_1, \dots, E_n$ are disjoint, the events $A(E_1), \dots, A(E_n)$ are independent.

Now let $1_A(E)$ be the indicator of the event $A(E)$. Let $E \in \mathcal{F}$ and $F \in \mathcal{F}$ be two disjoint sets. For any $\varepsilon > 0$ we can clearly decompose E into disjoint intervals E_i ($1 \leq i \leq n$) and F into disjoint intervals such that

$$\max_i \lambda(E_i) < \varepsilon \quad \text{and} \quad \max_j \lambda(F_j) < \varepsilon$$

Now evidently $\xi(E) \neq \sum_{i=1}^n 1_{A(E_i)}$ implies $\max_i \xi(E_i) \geq 2$

$$\text{and } \xi(F) \neq \sum_{j=1}^m 1_{A(F_j)} \text{ implies}$$

$$\max_j \xi(F_j) \geq 2.$$

On the other hand for any $B \in \mathcal{F}$

$$(3) \quad P(\xi(B) \geq 2) = \sum_{k=2}^{\infty} \frac{\lambda(B)^k e^{-\lambda(B)}}{k!} \leq \lambda^2(B)$$

Thus

$$(4a) \quad P(\xi(E) \neq \sum_{i=1}^n 1_{A(E_i)}) \leq \sum_{i=1}^n \lambda^2(E_i) < \varepsilon \lambda(E)$$

(*) Here and in what follows the product of events denotes the joint occurrence of these events.

and

$$(4b) \quad P(\{F\} \neq \sum_{j=1}^m 1_{A(F_j)}) \leq \sum_{j=1}^m \lambda^2(F_j) < \varepsilon \lambda(F)$$

This implies, as the sums

$$\sum_{i=1}^n 1_{A(E_i)} \quad \text{and} \quad \sum_{j=1}^m 1_{A(F_j)}$$

are independent, that $\{E\}$ and $\{F\}$ are independent too.

As a matter of fact it follows from (4a) and (4b) that for any n and m ($n, m = 0, 1, 2, \dots$)

$$(5) \quad \left| P(\{E\} = n, \{F\} = m) - P(\{E\} = n) P(\{F\} = m) \right| \leq 2 \varepsilon \lambda(E + F).$$

As $\varepsilon > 0$ can be chosen arbitrarily small, our statement follows. The independence of the variables $\{E_i\}$ ($i = 1, 2, \dots, r$) with disjoint E_i and $r > 2$ is proved in exactly the same way. Thus our theorem is proved.

Remark 1. Note that to prove the independence of $\{E_i\}$ ($i = 1, 2, \dots, r$) for $E_i E_j = \emptyset$ if $i \neq j$ we have not used the full supposition that for each $E \in \mathcal{F}$ $\{E\}$ has a Poisson distribution, only that

$$(6a) \quad P(\{E\} = 0) = e^{-\lambda(E)}$$

$$\text{and } (6b) \quad P(\{E\} \geq 2) = o(\lambda(E)) \quad \text{if } \lambda(E) \rightarrow 0$$

uniformly in E .

Thus even these suppositions imply that the process $\{E\}$ is a process of independent increments. It is easy to show however that this together with (6a) and (6b) implies that $\{E\}$ has a Poisson distribution.

Thus the following theorem is true.

Theorem 2.

Let $\mathcal{F}$ denote the family of all subsets of the real line which can be obtained as the union of a finite number of disjoint finite intervals $[a, b]$. Let $\{E\}$ be an additive stochastic set function defined for $E \in \mathcal{F}$, i.e. such that if $E_1 \in \mathcal{F}$ and $E_2 \in \mathcal{F}$ are disjoint one has $\{E_1 + E_2\} = \{E_1\} + \{E_2\}$. Suppose that $\{E\}$ is for each

$E \in \mathcal{F}$ a non-negative integer valued random variable such that

$$(7a) \quad P(f(E) = 0) = e^{-\lambda(E)} \quad \text{and}$$

$$(7b) \quad P(f(E) \geq 2) \leq \lambda(E) \delta(\lambda(E))$$

where $\delta(x)$ is an increasing positive function defined for $x > 0$ such that $\lim_{x \rightarrow 0} \delta(x) = 0$ and $\lambda(E)$ a nonatomic measure on $\mathcal{F}$. Then it follows that $f(E)$ is a Poisson process, i.e. if E_i ($i=1,2, \dots, r$) are disjoint sets, $E_i \in \mathcal{F}$ the random variables $f(E_i)$ ($i = 1,2, \dots, r$) are independent, and (1) holds.

Proof of theorem 2. Put for $E \in \mathcal{F}$

$$\varphi_E(u) = M(e^{iu} f(E)) \quad (-\infty < u < +\infty) \quad \text{then clearly}$$

$$(8) \quad |\varphi_E(u)| \geq e^{-\lambda(E)} - |u| (1 - e^{-\lambda(E)}) > 0 \quad \text{if}$$

$$|u| < \frac{1}{e^{\lambda(E)} - 1}$$

Thus if

$$E = \sum_{i=1}^r E_i, \quad \text{where } E_i \in \mathcal{F} \text{ and } E_i E_j = \emptyset \text{ if } i \neq j, \text{ then for}$$

$$|u| < \frac{1}{e^{\lambda(E)} - 1} \quad \text{we have}$$

$$(9) \quad \varphi_E(u) = \prod_{i=1}^r \varphi_{E_i}(u) \neq 0 \quad \text{and therefore}$$

$$(10) \quad \log \varphi_E(u) = \sum_{i=1}^r \log \varphi_{E_i}(u). \quad \text{As however}$$

$$(11) \quad \varphi_{E_i}(u) = e^{-\lambda(E_i)} + e^{iu} (1 - e^{-\lambda(E_i)}) + O(\lambda(E_i) \delta(\lambda(E_i))) \quad \text{we get}$$

$$(12) \quad \log \varphi_{E_i}(u) = \lambda(E_i)(e^{iu} - 1) + O(\lambda(E_i)(\lambda(E_i) + \delta(\lambda(E_i))))$$

It follows that if $\lambda(E_i) < \varepsilon$ for $i = 1,2, \dots, r$

$$(13) \quad \log \varphi_E(u) = \lambda(E)(e^{iu} - 1) + O(\varepsilon + \delta(\varepsilon))$$

that is, as $\varepsilon > 0$ can be chosen arbitrarily small,

$$(14) \quad \varphi_E(u) = e^{\lambda(E)} (e^{iu} - 1)$$

which implies that $\xi(E)$ has a Poisson distribution with mean $\lambda(E)$. Thus theorem 2 follows from theorem 1.

Remark 2. The proof can be carried over without any change to the discussion of a Poisson process in more than one dimension or even in an abstract space. Thus we obtain the following

Theorem 3.

Let X be any space, $\mathcal{F}$ a family of subsets of X and $\lambda(E)$ a non-negative finite valued set function defined on $\mathcal{F}$, such that

- 1) if $E_1 \in \mathcal{F}$, $E_2 \in \mathcal{F}$ and $E_1 E_2 = \emptyset$, then $E_1 + E_2 \in \mathcal{F}$
- 2) $E_1 \in \mathcal{F}$, $E_2 \in \mathcal{F}$, $E_1 E_2 = \emptyset$ then $\lambda(E_1 + E_2) = \lambda(E_1) + \lambda(E_2)$
- 3) There is a constant α with $0 < \alpha < 1$ such that for every $E \in \mathcal{F}$ with $\lambda(E) > 0$ there exists a subset F of E such that $F \in \mathcal{F}$, $E - F \in \mathcal{F}$ and

$$\alpha < \frac{\lambda(F)}{\lambda(E)} < 1 - \alpha$$

Let us suppose a stochastic set function is defined on $\mathcal{F}$, i.e. to every $E \in \mathcal{F}$ there corresponds a random variable $\xi(E)$ such that if $E_1 \in \mathcal{F}$, $E_2 \in \mathcal{F}$ and $E_1 E_2 = \emptyset$ we have $\xi(E_1 + E_2) = \xi(E_1) + \xi(E_2)$ and $\xi(E)$ has a Poisson distribution with mean value $\lambda(E)$. Then the random variables $\xi(E_i)$ ($i=1,2,\dots, r$) are independent if the sets $E_i \in \mathcal{F}$ ($i = 1,2, \dots, r$) are disjoint, i.e. $\xi(E)$ is Poisson-process.

Note that condition 3) is not quite the same as that λ is nonatomic, because we did not suppose that $\mathcal{F}$ is a σ -algebra of sets.

Remark 3. The question arises whether the condition that the process should be one with independent increments can be deduced from other suppositions for other processes of independent increments too.

The most interesting case is that of the Wiener process; for this process one has the following (almost trivial) analogue of theorem 1.

Theorem 4.

Let $\{t\}$ ($-\infty < t < +\infty$) be a stochastic process such that $\{t\} - \{s\}$ is normally distributed with mean 0 and variance $c(t - s)$ ($c > 0$) for $s < t$. Suppose further that if the intervals $[s_j, t_j)$ ($j = 1, 2, \dots, r$) are disjoint, any linear combination

$\sum_{j=1}^r b_j (\{t_j\} - \{s_j\})$ of the increments $\{t_j\} - \{s_j\}$ with real coefficients b_j is normally distributed. Then $\{\{t\}\}$ is the Wiener process, i.e. the random variables $\{t_j\} - \{s_j\}$ are independent if the intervals $[s_j, t_j)$ are disjoint.

Proof of theorem 4. Clearly putting for $I_k = [s_k, t_k)$ $\{I_k\} = \{t_k\} - \{s_k\}$ ($k=1, 2$) if I_1 and I_2 are adjacent intervals ($s_1 < t_1 = s_2 < t_2$) $\{I_1 + I_2\} = \{I_1\} + \{I_2\}$ and thus

$$\begin{aligned} M(\{\{I_1 + I_2\}\}^2) &= t_2 - s_1 = t_2 - s_2 + t_1 - s_1 = \\ &= M(\{I_1\}^2) + M(\{I_2\}^2) \end{aligned}$$

and thus $M(\{I_1\}\{I_2\}) = 0$, i.e. $\{I_1\}$ and $\{I_2\}$ are uncorrelated. Now let I_1 and I_2 be arbitrary disjoint intervals

$$I_1 = [s_1, t_1), \quad I_2 = [s_2, t_2) \quad \text{where} \quad s_1 < t_1 < s_2 < t_2$$

and put $I_3 = [t_1, s_2)$. Then, taking into account that

$$\begin{aligned} M(\{I_1\}\{I_3\}) &= 0 \quad \text{and} \quad M(\{I_3\}\{I_2\}) = 0, \quad \text{we get} \\ M(\{I_1 + I_2 + I_3\}^2) &= t_2 - s_1 = M(\{I_1\}^2) + M(\{I_2\}^2) + M(\{I_3\}^2) + \\ &\quad + 2M(\{I_1\}\{I_2\}) \end{aligned}$$

Thus $M(\{I_1\}\{I_2\}) = 0$

(We have used here the following elementary geometrical fact: if a, b, c are vectors in the 3-dimensional Euclidean space for which c is orthogonal both to b and to $a + b$, then c is orthogonal to a too.)

Thus $\{I_1\}$ and $\{I_2\}$ are uncorrelated if I_1 and I_2 are arbitrary disjoint intervals.

It follows that if $I_1, I_2, \dots, I_r$ are disjoint intervals and I_j has length $|I_j|$, and $b_1, \dots, b_r$ are arbitrary real constants then

$$M\left(\sum_{j=1}^r b_j f(I_j)\right)^2 = \sum_{j=1}^r b_j^2 c(I_j)$$

Thus

$$M\left(e^{iu \sum_{j=1}^r b_j f(I_j)}\right) = e^{-\frac{1}{2} u^2 \sum_{j=1}^r b_j^2 c(I_j)}$$

and thus for any real numbers $u_1, u_2, \dots, u_r$

$$M\left(e^{i \sum_{j=1}^r u_j f(I_j)}\right) = \prod_{j=1}^r M\left(e^{iu_j f(I_j)}\right)$$

i. e. the $f(I_j)$ ($j = 1, 2, \dots, r$) are independent, i. e. f_t is the Wiener-process.
(Note that it would have been sufficient to suppose that

$$\sum_{j=1}^r b_j f(I_j) \text{ is normally distributed for } \sum_{j=1}^r b_j^2 = 1.)$$

Remark 4. Returning to the Poisson-process, the question arises, whether if in theorem 1 instead of the condition that $f(E)$ has a Poisson distribution if E is any finite union of intervals, one supposes only that $f(I)$ has a Poisson distribution if I is any interval, does this still ensure that the process is a Poisson process? It is easy to show that in this case $f(I_1)$ and $f(I_2)$ are uncorrelated if I_1 and I_2 are disjoint intervals. The proof of this is essentially the same as the first step of the proof of theorem 4.

Remark added on August 22, 1966:

I have been informed by Jay Goldman, that the answer to the question in Remark 4 is: no. This has been shown by a counterexample by L. Shepp; this example will be published in a forthcoming paper of J. Goldman.

39, 50, 69

NOTE

1. A significant part of the characterization theorems of Poisson processes can be obtained from the theory of stochastic processes of independent increments. This theory was developed by Ito [4] who used many ideas of Lévy. The

fundamental importance of Poisson processes makes it reasonable to work out the theory of the Poisson processes independently of the theory of processes of independent increments.

In 1933 Khintchine proved the following

Theorem 1 (Khintchine [8]). *If a stationary point process has independent increments and — using the notations of No. 39 — we have*

$$(1) \quad 1 - W_0(t) = \lambda t + o(t) \quad (t \rightarrow 0)$$

and

$$(2) \quad 1 - W_0(t) - W_1(t) = o(t) \quad (t \rightarrow 0)$$

then the process is a Poisson process with parameter λ .

In No. 39 the authors noticed that $W_0(t)$ satisfies the Cauchy functional equation hence they could omit condition (1). Developing on this technique Rényi No. 50 gave a characterization of non-stationary point processes with independent increments assuming their stochastic continuity.

This research was continued in 1953–54 by Polish probabilists, who understood the Poisson process as a stochastic set function (Marczewski [13], Ryll-Nardzewski [23]). Later on stochastic set functions and also Poisson processes in an abstract space were investigated by Prékopa [18], [19], [20], [21]. A representation theorem for random measures with independent increments was obtained by Kingman [11].

In his famous paper Khintchine [9] collected various methods for proving the characterization theorem of No. 39, § 1. (A problem for those who favourize the method of characteristic functions: Is it possible to prove the mentioned characterization theorem by using characteristic functionals?!) He also described the point processes of independent increments without the condition of stochastic continuity (Khintchine [10]). We remark that Khintchine certainly did not know the above mentioned results of Hungarian and Polish mathematicians because he did not give references to them only to Redheffer [22], who had obtained the representation of stationary point processes with independent increments.

2. Let P be a point process on the real line (i.e. a probability measure on the space of realizations) and denote by $\nu(A)$ the number of points contained in the set A . The well-known definition of the Poisson process requires the fulfilment of two conditions:

I. For disjoint intervals $I_1, \dots, I_n$ the random variables $\nu(I_1), \dots, \nu(I_n)$ are independent ($n = 1, 2, \dots$).

P. For any interval I

$$P\{\nu(I) = k\} = \frac{[\lambda(I)]^k}{k!} e^{-\lambda(I)} \quad (k = 0, 1, 2, \dots)$$

where λ is a nonatomic measure on the Borel sets and is finite for bounded intervals.

In 1965 D. Szász posed the question (oral communication to Rényi), whether it was true that the only condition P characterizes the Poisson process. In 1967–68 Shepp (see Goldman [2]), Moran [15] and Lee [12] independently proved that this was not true. They gave examples of point processes fulfilling P but not I. At the same time Rényi posed and answered the question in a different way. In No. 228 he substituted condition P with a stronger one.

P^* . For any finite union E of finite intervals

$$P\{v(E) = k\} = \frac{[\lambda(E)]^k}{k!} e^{-\lambda(E)} \quad (k = 0, 1, \dots)$$

where λ is as in P and proved that P^* is sufficient to characterize the Poisson process, i.e. I is a consequence of P^* .

Rényi's theorem can be formulated also as follows, if P is a point process and Π is a Poisson process and

$$(3) \quad P\{v(E) = k\} = \Pi\{v(E) = k\} \quad (E \in \mathfrak{R})$$

where $\mathfrak{R}$ is the ring of finite unions of finite intervals then

$$(4) \quad P \equiv \Pi.$$

This form of Rényi's theorem led to interesting generalizations. Mönch [16] proved that if instead of Π we have any point process without *multiple* points then (3) is always sufficient to ensure (4) (Mönch's result is formulated for point processes in a *Polish space*). Kallenberg [6] proved a sharper result than Mönch's one and he and Grandell [3] obtained similar theorems for random measures and stochastic processes (see also Kallenberg [7]).

Rényi's theorem is strong in the sense that it would not be enough to require (3) only for the unions of a bounded number of finite intervals. This comes from an example of Szász [25], who constructed a non-Poisson process satisfying P and also

I_N . For disjoint intervals $I_1, \dots, I_n$ the random variables $v(I_1), \dots, v(I_n)$ are independent ($n = 1, 2, \dots, N$).

Recently similar type of counterexamples were obtained by Oakes [17] and for a large class of Markov processes (including the Poisson process) by Balkema [1].

3. The solution of the telephone-problem given in § 2 of No. 45, § 2 of No. 50 and in No. 69 is connected with secondary stochastic processes generated by a Poisson process. Such processes were treated later by Ryll-Nardzewski [24], Takács [26] and Prékopa [21].

4. Mine and Ohno [14] applied a result of No. 39 in queueing theory and Jagers [5] Theorem 1 of No. 284 to a theoretical problem of point processes. (D. SZ.)

REFERENCES

- [1] Balkema, A. A.: *Stochastic processes with the n -dimensional marginal distributions of Markov-processes*. Manuscript, (1973).
- [2] Goldman, J. R.: Stochastic point processes: limit theorems. *Annals Math. Statist.*, **38** (1967), 771–779.
- [3] Grandell, J.: Part of a manuscript. (1973).
- [4] Ito, K.: On stochastic processes. *Jap. J. Math.*, **18** (1942), 261–301.
- [5] Jagers, P.: On Palm probabilities. *Z. Wahrscheinlichkeitstheorie*, **26** (1973), 17–32.
- [6] Kallenberg, O.: Characterization and convergence of random measures and point processes. *Z. Wahrscheinlichkeitstheorie*, **27** (1973), 9–21.
- [7] Kallenberg, O.: Characterization of continuous random processes and signed measures. *Studia Sci. Math. Hung.*, **8** (1973) 473–477.
- [8] Khintchine, A.: *Asymptotische Gesetze der Wahrscheinlichkeitsrechnung*. Berlin, (1933).
- [9] Khintchine, A.: Mathematical methods in the theory of queues (in Russian). *Trudi Math. Inst. Steklov.*, **49** (1955).

- [10] Khintchine, A.: Flows of random events without interaction. *Teorija Veroyatnostei i Prim.*, 1 (1956), 3–17.
- [11] Kingman, J. F. C.: Completely random measures. *Pacific J. Math.*, 21 (1967), 59–78.
- [12] Lee, P. M.: Some examples of infinitely divisible processes. *Studia Sci. Math. Hung.*, 3 (1964), 219–224.
- [13] Marczewski, E.: Remarks on the Poisson stochastic process. II. *Studia Math.*, 13 (1953), 130–136.
- [14] Mine, H. and Ohno, K.: Traffic light queues as a generalization to queueing theory. *J. Appl. Prob.*, 8 (1971), 480–493.
- [15] Moran, P. A. P.: A non-Markovian quasi-Poisson process. *Studia Sci. Math. Hung.*, 2 (1967), 425–429.
- [16] Mönch, G.: Verallgemeinerung eines Satzes von A. Rényi. *Studia Sci. Math. Hung.*, 6 (1971), 81–90.
- [17] Oakes, D.: A k -fold quasi-Poisson process. *Colloquia Math. Soc. János Bolyai*, 9. European Meeting of Stat. (1972).
- [18] Prékopa, A.: On stochastic set functions I. *Acta Math. Acad. Sci. Hung.*, 7 (1956), 215–263.
- [19] Prékopa, A.: On stochastic set functions II. *Acta Math. Acad. Sci. Hung.*, 8 (1957), 337–374.
- [20] Prékopa, A.: On stochastic set functions III. *Acta Math. Acad. Sci. Hung.*, 8 (1957), 375–400.
- [21] Prékopa, A.: On secondary processes generated by a random point distribution of Poisson type. *Annales Univ. Sci. Budapestensis*, 1 (1958), 153–170.
- [22] Redheffer, R. M.: A note on the Poisson law. *Math. Magazine*, 26 (1953), 185–188.
- [23] Ryll-Nardzewski, C.: On the non-homogeneous Poisson process I. *Studia Math.*, 14 (1953), 124–128.
- [24] Ryll-Nardzewski, C.: Remarks on the Poisson stochastic process III. *Studia Math.*, 14 (1954), 314–318.
- [25] Szász, D.: Once more on the Poisson process. *Studia Sci. Math. Hung.*, 5 (1970), 441–444.
- [26] Takács, L.: On secondary stochastic processes generated by a multidimensional Poisson process. *Publ. Math. Inst. Hung. Acad. Sci.*, 2 (1957), 71–80.

288. *Proceedings of the Fifth Berkeley symposium on mathematical statistics and probability*. Held at the Statistical Laboratory, University of California, June 21–July 18, 1965 and December 27, 1965–January 7, 1966. Vol. I. University of California Press, Berkeley and Los Angeles, 1967; pp. 531–543.

ON SOME BASIC PROBLEMS OF STATISTICS FROM THE POINT OF VIEW OF INFORMATION THEORY

ALFRÉD RÉNYI

MATHEMATICAL INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCES

1. Introduction

Many problems of mathematical statistics consist in that one has to extract from certain observations the information which is needed. In other words, one has to separate the relevant information from the irrelevant. For instance, it is a generally accepted view that if for a parameter there exists a sufficient statistic, its sufficiency means that it contains all the information which is present in the sample and is relevant for determining the parameter. Although this is generally admitted, it is not usual to go a step further and ask: *how much information is contained in a statistic (sufficient or not) concerning a parameter?* (According to the author's knowledge, the first to consider this question was D. V. Lindley [1].) In view of the success of information theory in other fields (especially in the theory of information-transmission), which success was achieved by attributing a numerical measure to amounts of information, this question is a very natural one. It seems to the author that the reason why this question is usually not asked in current statistical practice is that a meaningful answer to this question can be given only if one accepts the Bayesian point of view; that is, if one considers the unknown parameter as a random variable and attributes to it a prior distribution. As a matter of fact, the amount of information in a random variable concerning another random variable is a well-defined concept of information theory, whereas the amount of information in a random variable concerning a constant is always zero. The amount of information in a random variable ξ concerning another random variable θ is equal to the average decrease of uncertainty (entropy) concerning θ which results if ξ is observed. In order to measure this decrease of uncertainty, our prior knowledge about θ has to be taken into account.

If we have some prior knowledge about θ , this causes no difficulty. If we have no prior knowledge about θ , except that we know the set of its possible values, from the point of view of information theory it seems to be natural to attribute to θ that prior distribution on the admissible set of values which has the largest entropy, that is which corresponds to maximal uncertainty. Even if the parameter is in reality a constant, if its value is unknown to us, I do not find any logical fault in attributing to θ a prior distribution, if this is needed to compare

different statistics and to choose that which is the best for our purposes. Usually the choice depends only weakly on the prior distribution.

In this paper we do not want to go into the philosophical aspects of the question—however interesting they may be—as our aim is to deal with certain purely mathematical problems which arise when one tries to apply the concepts of information theory to the mentioned statistical problems.

The problem which will be discussed in what follows is: *how can one decide whether or not a certain sequence of observations contains all the information which is needed* (for example, to find the true value of the parameter)? In general, if a statistician is confronted with a concrete problem, his first task is to decide whether or not the required information is fully present. If the answer is positive, then the second step consists in trying to find an appropriate decision procedure, for instance one which is optimal in some respect. However, if the answer to the first question is negative, then it is futile to take the second step, as even the “best” decision procedure will not yield the required information. In this case the statistician has to look for some other source of information, that is, make some other observations.

In the present paper we shall discuss from this point of view the following problem. Let us be given an infinite sequence $\{\xi_n\}$, ($n = 1, 2, \dots$) of observations. We suppose that the distributions of the random variables ξ_n , ($n = 1, 2, \dots$) depend on a parameter θ , whose set of possible values is *finite*. We suppose further that for each fixed value of θ the random variables ξ_n , ($n = 1, 2, \dots$) are independent, but in general do not have the same distribution. We shall be especially interested in the case where the amount of information on θ contained in the observation ξ_n decreases when n increases. Such problems are often encountered. Let us imagine for instance that an event $\mathcal{E}$ happened at time $t = 0$, and ξ_n is the value of some quantity connected with the aftereffects of this event measured by some instrument at time $t = n$. Usually as time passes, the aftereffects of the event $\mathcal{E}$ become weaker and weaker, and thus as n increases, ξ_n gives gradually less and less information on the event $\mathcal{E}$.

In section 2 we shall consider the amount of information on θ which is still missing after having observed the values $\xi_1, \xi_2, \dots, \xi_n$ and compare it with the error of the “standard” decision, consisting in deciding always in favor of the hypothesis which has the largest posterior probability.

In section 3 we give an upper bound for the amount of missing information (theorem 2) and give a necessary and sufficient condition for the convergence to 0 of this quantity for n tending to $+\infty$.

In section 4 we shall discuss some special cases, some of which have been discussed in previous papers of the author (see [2], [3], [4]), and also others which are presented here for the first time. In section 5 we compare some of our results with a theorem of S. Kakutani [5].

For the sake of brevity we deal in detail only with the case where θ may have only two values. The generalization to the case when the set of possible values of θ is an arbitrary *finite* set is quite straightforward and presents no difficulty. It

should be added, however, that our results cannot be generalized immediately to the case when the set of possible values of θ is infinite. This case presents some peculiar difficulties. We hope to return to this question in another paper.

2. An inequality between the amount of missing information and the error of the standard decision

Let $\{\xi_n\}$, ($n = 1, 2, \dots$) be a sequence of random variables. Let us suppose that the distribution of ξ_n depends on a parameter θ , which may take on two different values θ_0 and θ_1 . We suppose that the random variables ξ_n are independent under the condition $\theta = \theta_0$, as well as under the condition $\theta = \theta_1$. We suppose further (this restriction is made only to simplify notations) that all the distributions in question are absolutely continuous. Let $f_n(x)$ and $g_n(x)$ denote the density functions of ξ_n under the conditions $\theta = \theta_0$ and $\theta = \theta_1$, respectively. As regards θ we suppose that it is a random variable, taking on the values θ_0 and θ_1 with the corresponding positive probabilities W_0 and W_1 , ($W_0 + W_1 = 1$).

These suppositions can be formulated as follows. Let $[\Omega, \mathcal{G}, P] = S$ be a probability space. Let us be given a partition of Ω into two $\mathcal{G}$ -measurable sets Ω_0 and $\Omega_1 = \Omega - \Omega_0$, with $P(\Omega_0) = W_0$, $P(\Omega_1) = W_1 = 1 - W_0$. Let S_0 and S_1 denote the probability spaces $S_0 = [\Omega, \mathcal{G}, P_0]$ and $S_1 = [\Omega, \mathcal{G}, P_1]$ where $P_0(A) = (P(A\Omega_0)/P(\Omega_0))$ and $P_1(A) = (P(A\Omega_1)/P(\Omega_1))$ for $A \in \mathcal{G}$. Let $\xi_n = \xi_n(\omega)$, ($\omega \in \Omega$), ($n = 1, 2, \dots$) be a sequence of $\mathcal{G}$ -measurable real functions. Then we can consider the ξ_n as random variables on the probability space S as well as on the probability spaces S_0 and S_1 . We suppose that the random variables ξ_n are independent on S_0 as well as on S_1 . Note that on the probability space S the random variables ξ_n are usually not independent.

Let us suppose now that we observe the values of all the variables ξ_n , and we want to decide on this basis whether $\theta = \theta_0$ or $\theta = \theta_1$. In other words, we suppose that the sequence of values $\xi_n(\omega^*)$, ($n = 1, 2, \dots$) is given for a single unknown $\omega^* \in \Omega$, and want to decide, whether $\omega^* \in \Omega_0$ or $\omega^* \in \Omega_1$. We especially want to find out under what conditions on the density functions $f_n(x)$ and $g_n(x)$ can a correct decision be made for almost all $\omega^* \in \Omega$ (with respect to the measure P)?

Let us denote by ζ_n the random n -dimensional vector with components $(\xi_1, \xi_2, \dots, \xi_n)$. Let I_n denote the amount of information contained in ζ_n concerning θ . Then we have

$$(2.1) \quad I_n = H(\theta) - E(H(\theta|\zeta_n)),$$

where

$$(2.2) \quad H(\theta) = W_0 \log \frac{1}{W_0} + W_1 \log \frac{1}{W_1}$$

is the entropy of the random variable θ , and $H(\theta|\zeta_n)$ is the conditional entropy of θ given ζ_n , that is

$$(2.3) \quad H(\theta|\xi_n) = P(\theta = \theta_0|\xi_n) \log \frac{1}{P(\theta = \theta_0|\xi_n)} \\ + P(\theta = \theta_1|\xi_n) \log \frac{1}{P(\theta = \theta_1|\xi_n)},$$

and $E(H(\theta|\xi_n))$ denotes the expectation of the random variable $H(\theta|\xi_n)$. Here and in what follows $\log$ always denotes logarithm with base 2.

According to our supposition and the Bayes' theorem, one has

$$(2.4) \quad P(\theta = \theta_0|\xi_n) = \frac{W_0 f_1(\xi_1) f_2(\xi_2) \cdots f_n(\xi_n)}{W_0 f_1(\xi_1) \cdots f_n(\xi_n) + W_1 g_1(\xi_1) \cdots g_n(\xi_n)}$$

and similarly,

$$(2.5) \quad P(\theta = \theta_1|\xi_n) = \frac{W_1 g_1(\xi_1) g_2(\xi_2) \cdots g_n(\xi_n)}{W_0 f_1(\xi_1) \cdots f_n(\xi_n) + W_1 g_1(\xi_1) \cdots g_n(\xi_n)}.$$

For the sake of brevity, we introduce the notations $x^{(n)} = (x_1, \dots, x_n)$, $\varphi_n(x^{(n)}) = f_1(x_1) \cdots f_n(x_n)$, and $\psi_n(x^{(n)}) = g_1(x_1) \cdots g_n(x_n)$.

With these notations, letting $\chi_n(x^{(n)}) = W_0 \varphi_n(x^{(n)}) + W_1 \psi_n(x^{(n)})$ we have

$$(2.6) \quad E(H(\theta|\xi_n)) \\ = \int_{X_n} \left[W_0 \varphi_n(x^{(n)}) \log \frac{\chi_n(x^{(n)})}{W_0 \varphi_n(x^{(n)})} + W_1 \psi_n(x^{(n)}) \log \frac{\chi_n(x^{(n)})}{W_1 \psi_n(x^{(n)})} \right] dx^{(n)}$$

where X_n is the n -dimensional Euclidean space and $dx^{(n)}$ stands for $dx_1 dx_2 \cdots dx_n$.

The quantity $E(H(\theta|\xi_n))$ may be interpreted as the amount of missing information on θ after observing ξ_n .

It is easy to see that I_n is nondecreasing for $n = 1, 2, \dots$ and $I_n \leq H(\theta)$. Thus $\lim_{n \rightarrow +\infty} I_n = I^*$ always exists. If $I^* = H(\theta)$, we shall say that the sequence of observations $\{\xi_n\}$, ($n = 1, 2, \dots$) gives us full information on θ , whereas in the case $I^* < H(\theta)$ we shall say that the observations $\{\xi_n\}$ do not give full information on θ .

Clearly, the most natural decision after having observed ξ_n is to accept θ_0 if $P(\theta_0|\xi_n) > P(\theta_1|\xi_n)$ and to accept θ_1 if $P(\theta_1|\xi_n) > P(\theta_0|\xi_n)$, and if $P(\theta_0|\xi_n) = P(\theta_1|\xi_n)$ to make a random choice between θ_0 and θ_1 with probabilities W_0 and W_1 . We shall call this the *standard decision*. Let us define the random variable $\Delta_n = \Delta_n(\xi_n)$ as follows:

$$(2.7) \quad \Delta_n = \begin{cases} \theta_0 & \text{if the standard decision means acceptance of } \theta_0, \\ \theta_1 & \text{if the standard decision means acceptance of } \theta_1. \end{cases}$$

The error ϵ_n of the standard decision after taking n observations is defined as the probability of the standard decision being false. We have clearly

$$(2.8) \quad \epsilon_n = P(\Delta_n \neq \theta) = W_0 P(\Delta_n = \theta_1 | \theta = \theta_0) + W_1 P(\Delta_n = \theta_0 | \theta = \theta_1),$$

where $P(A|B)$ denotes the conditional probability of the event A under condition B . Obviously, $\Delta_n = \theta_0$ if $(\varphi_n(\xi_n)/\psi_n(\xi_n)) > (W_1/W_0)$ and $\Delta_n = \theta_1$ if $(\varphi_n(\xi_n)/\psi_n(\xi_n)) < (W_1/W_0)$. Thus

$$(2.9) \quad \epsilon_n = W_0 \int_{A_n} \varphi_n(x^{(n)}) dx^{(n)} + W_1 \int_{B_n} \psi_n(x^{(n)}) dx^{(n)}$$

where

$$(2.10) \quad A_n = \left\{ \frac{\psi_n(x^{(n)})}{\varphi_n(x^{(n)})} \geq \frac{W_0}{W_1} \right\} \quad \text{and} \quad B_n = \left\{ \frac{\psi_n(x^{(n)})}{\varphi_n(x^{(n)})} < \frac{W_0}{W_1} \right\}.$$

It is easy to prove the following.

THEOREM 1. *One has*

$$(2.11) \quad \frac{\epsilon_n}{2} \leq H(\theta) - I_n \leq h(\epsilon_n)$$

where

$$(2.12) \quad h(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}, \quad (0 \leq p \leq 1).$$

PROOF OF THEOREM 1. One has clearly

$$(2.13) \quad E(H(\theta|\xi_n)) = W_0 E(H(\theta|\xi_n)|\theta = \theta_0) + W_1 E(H(\theta|\xi_n)|\theta = \theta_1);$$

$E(\eta|B)$ denotes the conditional expectation of η under condition B . Now evidently

$$(2.14) \quad W_1 E(H(\theta|\xi_n)|\theta = \theta_1) \geq \int_{A_n} \frac{\varphi_n(x^{(n)}) W_0}{\chi_n(x^{(n)})} \log \left(1 + \frac{W_1 \psi_n(x^{(n)})}{W_0 \varphi_n(x^{(n)})} \right) W_1 \psi_n(x^{(n)}) dx^{(n)}$$

and thus, as on the set defined by $(\psi_n(x^{(n)})/\varphi_n(x^{(n)})) \geq (W_0/W_1)$ one has $(W_1 \psi_n(x^{(n)})/\varphi_n(x^{(n)})) \geq \frac{1}{2}$, it follows that

$$(2.15) \quad W_1 E(H(\theta|\xi_n)|\theta = \theta_1) \geq \frac{1}{2} \int_{A_n} W_0 \varphi_n(x^{(n)}) dx^{(n)} = \frac{W_0}{2} P(\Delta = \theta_1|\theta = \theta_0).$$

Similarly we obtain

$$(2.16) \quad W_0 E(H(\theta|\xi_n)|\theta = \theta_0) \geq \frac{W_1}{2} P(\Delta = \theta_0|\theta = \theta_1).$$

Thus it follows that

$$(2.17) \quad E(H(\theta|\xi_n)) \geq \frac{\epsilon_n}{2}.$$

This proves the lower inequality in (2.11).

This proof was given earlier in [2]; it is reproduced here for the convenience of the reader. To prove the upper inequality in (2.11) we apply the following integral form of Jensen's inequality:

$$(2.18) \quad \frac{\int_A h(a(x))k(x) dx}{\int_A k(x) dx} \leq h\left(\frac{\int_A a(x)k(x) dx}{\int_A k(x) dx}\right),$$

valid for every nonnegative function $k(x)$ and every concave function $h(x)$; we apply (2.18) to the concave function $h(x)$ defined by (2.12) and the domain A in X_n defined by $(\varphi_n(x^{(n)})W_0/\psi_n(x^{(n)})W_1) \geq 1$ and for the complementary domain $\bar{A}$. Thus we obtain

$$(2.19) \quad E(H(\theta|\xi_n)) \leq \alpha h(p) + \beta h(q)$$

where

$$(2.20) \quad \alpha = \int_A \chi_n(x^{(n)}) dx^{(n)}, \quad \beta = \int_{\bar{A}} \chi_n(x^{(n)}) dx^{(n)} = 1 - \alpha,$$

$$p = \frac{W_1 \int_A \psi_n(x^{(n)}) dx^{(n)}}{\alpha} \quad \text{and} \quad q = \frac{W_0 \int_{\bar{A}} \varphi_n(x^{(n)}) dx^{(n)}}{\beta}.$$

Again applying Jensen's inequality in the form

$$(2.21) \quad \alpha h(p) + \beta h(q) \leq h(\alpha p + \beta q),$$

valid for any concave function h and for $\alpha \geq 0$, $\beta \geq 0$, $\alpha + \beta = 1$, since $\alpha p + \beta q = \epsilon_n$, it follows that

$$(2.22) \quad E(H(\theta|\zeta_n)) \leq h(\epsilon_n) = \epsilon_n \log \frac{1}{\epsilon_n} + (1 - \epsilon_n) \log \frac{1}{1 - \epsilon_n}.$$

Thus theorem 1 is proved.

We obtain easily from theorem 1 the following corollary.

COROLLARY. *The error of the standard decision tends to zero for $n \rightarrow \infty$ if and only if the amount of missing information tends to zero, that is, $\lim_{n \rightarrow +\infty} \epsilon_n = 0$ if and only if $\lim_{n \rightarrow \infty} I_n = H(\theta)$.*

It should be added that by a slight modification of the usual proof of the Neyman-Pearson fundamental lemma one can prove (see [3]) that the error of any decision function is at least as large as that of the standard decision. Thus if $\lim_{n \rightarrow \infty} I_n < H(\theta)$, that is, if the amount of information in the first n observations does not tend to the total amount of information needed, then there cannot exist a decision procedure whose error tends to zero, whereas if $\lim_{n \rightarrow \infty} I_n = H(\theta)$, there certainly exists such a procedure, namely the standard decision.

3. An upper bound for the amount of missing information and a criterion for obtaining full information

We prove now the following theorem.

THEOREM 2. *Let us write*

$$(3.1) \quad \lambda_k = \int_{-\infty}^{+\infty} \sqrt{f_k(x)g_k(x)} dx, \quad (k = 1, 2, \dots).$$

Then the following inequality holds:

$$(3.2) \quad 0 \leq H(\theta) - I_n \leq B \sqrt{W_0 W_1} \prod_{k=1}^n \lambda_k$$

where $B > 0$ is an absolute constant.

PROOF OF THEOREM 2. The function $(h(x)/\sqrt{x})$ where $h(x)$ is defined by (2.12) is clearly continuous in the closed interval $0 \leq x \leq 1$. Let

$$(3.3) \quad C = \max_{0 \leq x \leq 1} \frac{h(x)}{\sqrt{x}}$$

Since $h(x) = h(1 - x)$, we also have

$$(3.4) \quad C = \max_{0 \leq x \leq 1} \frac{h(x)}{\sqrt{1-x}}.$$

It follows that

$$(3.5) \quad H(\theta|\xi_n) \leq C\sqrt{P(\theta = \theta_1|\xi_n)}$$

and also that

$$(3.6) \quad H(\theta|\xi_n) \leq C\sqrt{P(\theta = \theta_0|\xi_n)}.$$

Thus we have, in view of (2.4) and (2.5),

$$(3.7) \quad H(\theta|\xi_n) \leq C \sqrt{\frac{W_0}{W_1}} \prod_{k=1}^n \sqrt{\frac{f_k(\xi_k)}{g_k(\xi_k)}}$$

and

$$(3.8) \quad H(\theta|\xi_n) \leq C \sqrt{\frac{W_1}{W_0}} \prod_{k=1}^n \sqrt{\frac{g_k(\xi_k)}{f_k(\xi_k)}}.$$

From (3.8) we obtain

$$(3.9) \quad W_0 E(H(\theta|\xi_n)|\theta = \theta_0) \leq C\sqrt{W_0 W_1} \prod_{k=1}^n \lambda_k,$$

and from (3.7) we obtain

$$(3.10) \quad W_1 E(H(\theta|\xi_n)|\theta = \theta_1) \leq C\sqrt{W_0 W_1} \prod_{k=1}^n \lambda_k.$$

Adding (3.9) and (3.10) we get

$$(3.11) \quad E(H(\theta|\xi_n)) \leq 2C\sqrt{W_0 W_1} \prod_{k=1}^n \lambda_k,$$

which proves theorem 2 with $B = 2C$.

Note that according to the Cauchy-Schwarz inequality, $0 \leq \lambda_k \leq 1$ and $\lambda_k = 1$ if and only if $f_k(x) = g_k(x)$ almost everywhere. Further, $\lambda_k = 0$ if and only if the intersection of the sets on which $f_k(x) > 0$ and $g_k(x) > 0$ is of Lebesgue measure zero. In this case, of course, the observation of ξ_k alone is sufficient with probability 1 to decide whether $\theta = \theta_0$ or $\theta = \theta_1$.

We shall now prove the following.

THEOREM 3. *One has*

$$(3.12) \quad \prod_{k=1}^n \lambda_k \leq \sqrt{\frac{\epsilon_n}{W_0 W_1}}$$

where λ_k is defined by (3.1), and ϵ_n is the error of the standard decision.

PROOF OF THEOREM 3. Clearly,

$$(3.13) \quad \prod_{k=1}^n \lambda_k = \int_{X_n} \sqrt{\varphi_n(x^{(n)})\psi_n(x^{(n)})} dx^{(n)}.$$

Let us denote again by A the subset of X_n on which $(W_0\varphi_n(x^{(n)})/W_1\psi_n(x^{(n)})) \geq 1$ and put $\bar{A} = X_n - A$. Taking into account that φ_n is a density function, the Cauchy-Schwarz inequality gives

$$(3.14) \quad \int_A \sqrt{\varphi_n(x^{(n)})\psi_n(x^{(n)})} dx^{(n)} \leq \left(\int_A \psi_n(x^{(n)}) dx^{(n)} \right)^{1/2}.$$

Similarly we obtain

$$(3.15) \quad \int_A \sqrt{\varphi_n(x^{(n)})\psi_n(x^{(n)})} dx^{(n)} \leq \left(\int_A \varphi_n(x^{(n)}) dx^{(n)} \right)^{1/2}.$$

Thus using again the Cauchy inequality we obtain

$$(3.16) \quad \prod_{k=1}^n \lambda_k \leq \left(\frac{1}{W_0} + \frac{1}{W_1} \right)^{1/2} \sqrt{\epsilon_n} = \sqrt{\frac{\epsilon_n}{W_0 W_1}}.$$

This proves theorem 3.

Now we can prove the following theorem.

THEOREM 4. *If $\lambda_k > 0$ for $k = 1, 2, \dots$, the sequence of observations ξ_n ($n = 1, 2, \dots$) contains full information on θ if and only if the series*

$$(3.17) \quad \sum_{k=1}^{\infty} (1 - \lambda_k)$$

is divergent.

As regards the connection of theorem 4 with a theorem of Kakutani, see section 4.)

PROOF OF THEOREM 4. Since $1 - x \leq e^{-x}$, if the series $\sum_{k=1}^{\infty} (1 - \lambda_k)$ is divergent, one has $\lim_{n \rightarrow \infty} \prod_{k=1}^n \lambda_k = 0$, and thus by theorem 2 it follows that

$$(3.18) \quad \lim_{n \rightarrow +\infty} I_n = H(\theta).$$

This proves the "if" part of the theorem. On the other hand, using the inequality $1 - x \geq e^{-(x/(1-x))}$, ($0 \leq x \leq 1$), we obtain

$$(3.19) \quad \prod_{k=1}^n \lambda_k \geq \exp \left\{ - \sum_{k=1}^n \left(\frac{1 - \lambda_k}{\lambda_k} \right) \right\}.$$

Now if $\sum_{k=1}^{\infty} (1 - \lambda_k)$ is convergent, then $\lim_{k \rightarrow \infty} \lambda_k = 1$, and since by assumption $\lambda_k > 0$ for $k = 1, 2, \dots$, it follows that the sequence λ_k has a positive lower bound: $\lambda_k \geq c > 0$ for $k = 1, 2, \dots$. It follows that the series $\sum_{k=1}^{\infty} (1 - \lambda_k/\lambda_k)$ is also convergent, and thus $\prod_{k=1}^n \lambda_k$ has a positive lower bound. By theorem 3 this implies that ϵ_n has a positive lower bound. Therefore, by theorem 1 the sequence $H(\theta) - I_n$ has a positive lower bound too. This proves the "only if" part of theorem 4.

THEOREM 5. *A sequence of statistics $\alpha_n = \alpha_n(\xi_1, \dots, \xi_n)$ converging in probability to the true value of the parameter (real-valued) can exist only if the sequence ξ_n ($n = 1, 2, \dots$) contains full information with respect to θ , that is if (3.18) holds. Conversely if (3.18) holds, there exists a sequence of statistics α_n which converges with probability 1 to θ .*

PROOF OF THEOREM 5. If $\lim_{n \rightarrow \infty} P(|\alpha_n - \theta| > \epsilon) = 0$ for every $\epsilon > 0$, then we can construct the following decision function:

$$(3.20) \quad \begin{cases} \text{if } |\alpha_n - \theta_1| < |\alpha_n - \theta_0|, & \text{accept } \theta_1; \\ \text{if } |\alpha_n - \theta_0| < |\alpha_n - \theta_1|, & \text{accept } \theta_0; \\ \text{if } |\alpha_n - \theta_0| = |\alpha_n - \theta_1|, & \text{choose at random between } \theta_0 \text{ and} \\ & \theta_1 \text{ with probabilities } W_0 \text{ and } W_1. \end{cases}$$

Let us suppose that $\theta_0 < \theta_1$. Clearly,

$$(3.21) \quad P(|\alpha_n - \theta_0| \leq |\alpha_n - \theta_1| | \theta = \theta_1) = P\left(\alpha_n \leq \frac{\theta_0 + \theta_1}{2} | \theta = \theta_1\right),$$

and thus by assumption,

$$(3.22) \quad \lim_{n \rightarrow \infty} P(|\alpha_n - \theta_0| \leq |\alpha_n - \theta_1| | \theta = \theta_1) = 0.$$

Similarly,

$$(3.23) \quad \lim_{n \rightarrow \infty} P(|\alpha_n - \theta_1| \leq |\alpha_n - \theta_0| | \theta = \theta_0) = 0.$$

Thus the error of the decision in question tends to zero for $n \rightarrow \infty$. A fortiori, the error of the standard decision tends to zero which implies by theorem 1 that (3.18) holds. This proves the "only if" part of theorem 5. Conversely, if (3.18) holds and θ_0 and θ_1 are different real numbers, let us choose a sequence n_r such that the series $\sum_{r=1}^{\infty} \epsilon_{n_r}$ is convergent. Then by the Borel-Cantelli lemma the standard decisions Δ_{n_r} tend with probability 1 to θ . More exactly, $\Delta_{n_r} = \theta$ for all but a finite number of values of r . Now if we put $\alpha_n = \Delta_{n_r}$ for $n_r \leq n < n_{r+1}$, then the sequence of statistics $\alpha_n = \alpha_n(\xi_1, \dots, \xi_n)$ tends with probability 1 to θ .

If the variables ξ_n have a discrete distribution, all our results remain valid; only the quantity λ_k has to be defined accordingly. If ξ_n can take the values $a_1, \dots, a_l, \dots$ and if

$$(3.24) \quad P(\xi_k = a_l | \theta = \theta_0) = p_{k,l},$$

whereas

$$(3.25) \quad P(\xi_k = a_l | \theta = \theta_1) = q_{k,l},$$

write

$$(3.26) \quad \lambda_k = \sum_{l=1}^{\infty} \sqrt{p_{k,l} q_{k,l}}.$$

All our results remain valid for this case.

4. Some examples

EXAMPLE 1. Let us suppose that $f_k(x) = f(x)$ and $g_k(x) = g(x)$, ($k = 1, 2, \dots$); that is, the random variables ξ_k are identically distributed under condition $\theta = \theta_i$, ($i = 1, 2$). Suppose further that

$$(4.1) \quad 1 > \lambda = \int_{-\infty}^{+\infty} \sqrt{f(x)g(x)} dx > 0.$$

Then it follows from theorem 2 that

$$(4.2) \quad H(\theta) - I_n \leq B\sqrt{W_0 W_1} \lambda^n,$$

and thus the missing information tends exponentially to zero for $n \rightarrow \infty$. This question was treated in [2] and [3]. In [4] we have been concerned with the

special case where the random variables ξ_n take only the values 0 and 1, and where one has

$$(4.3) \quad P(\xi_n = 1 | \theta = \theta_j) = p_j, \quad P(\xi_n = 0 | \theta = \theta_j) = q_j = 1 - p_j$$

for $j = 1, 2$. We have shown that the smallest value of λ for which (4.2) holds is $\lambda = 2^{-d(p_1, p_2)}$ where

$$(4.4) \quad d(p_1, p_2) = \rho \log \frac{\rho}{p_1} + (1 - \rho) \log \frac{1 - \rho}{1 - p_1} = \rho \log \frac{\rho}{p_2} + (1 - \rho) \log \frac{1 - \rho}{1 - p_2}$$

with

$$(4.5) \quad \rho = \frac{\log(q_1/q_2)}{\log(p_2 q_1 / p_1 q_2)}.$$

In the special case where $p_1 = q_2 = p$, $q_1 = p_2 = q = 1 - p$, one has simply $\lambda = 2\sqrt{pq}$.

EXAMPLE 2. Let ξ_n be normally distributed with variance S_n^2 and with mean $m = m_0$ or $m = m_1 \neq m_0$ according to whether $\theta = \theta_0$ or $\theta = \theta_1$. We want to find the true value of m . Clearly

$$(4.6) \quad \lambda_k = \exp \left(-\frac{(m_0 - m_1)^2}{8S_k^2} \right).$$

It follows that we have full information on m if and only if the series $\sum_{k=1}^{\infty} (1/S_k^2)$ is divergent. Note that the statistic

$$(4.7) \quad \eta_n = \frac{\sum_{k=1}^n (\xi_k/S_k^2)}{\sum_{k=1}^n (1/S_k^2)},$$

being the unbiased linear estimate of m with the least variance, is normally distributed with mean m and variance $(\sum_{k=1}^n (1/S_k^2))^{-1}$. If $\sum_{k=1}^{\infty} (1/S_k^2) = +\infty$, then η_n converges in probability to m and a suitably chosen subsequence η_{n_r} , such that $\sum_{r=1}^{\infty} (\sum_{k=1}^{n_r} (1/S_k^2))^{-1} < \infty$, converges with probability 1 to m .

EXAMPLE 3. Let an urn contain $a + b$ balls ($a > 0$, $b > 0$, $a \neq b$) of which either a are red and b white, or conversely, b are red and a white. Suppose that both cases have the prior probability $\frac{1}{2}$. We draw a ball from the urn, notice its color and put it back, and add, independently of the color of the ball drawn, $c_1 \geq 1$ red balls. After mixing the balls we draw again a ball, notice its color and put it back, adding $c_2 \geq 1$ red balls.

Let us continue this process indefinitely so that after the n -th step $c_n \geq 1$ new red balls are added. Can we determine with probability 1 the original composition of the urn?

Let us put $\xi_n = 1$ if the ball drawn at the n -th step is white and $\xi_n = 0$ if it is red. Let θ denote the number of white balls contained originally in the urn; thus $\theta_0 = b$ and $\theta_1 = a$. In this case

$$(4.8) \quad p_{k,1} = P(\xi_k = 1 | \theta = \theta_0) = \frac{b}{a + b + \sum_{i=1}^{k-1} c_i}$$

and

$$(4.9) \quad q_{k,1} = P(\xi_k = 1 | \theta = \theta_1) = \frac{a}{a + b + \sum_{i=1}^{k-1} c_i}.$$

Putting $N_k = a + b + \sum_{i=1}^{k-1} c_i$, one has

$$(4.10) \quad \lambda_k = \frac{\sqrt{ab}}{N_k} + \sqrt{\left(1 - \frac{a}{N_k}\right) \left(1 - \frac{b}{N_k}\right)},$$

and thus

$$(4.11) \quad \lambda_k = 1 - \frac{\frac{a+b}{2} - \sqrt{ab}}{N_k} + O\left(\frac{1}{N_k^2}\right).$$

Therefore, $\sum_{k=1}^{\infty} (1 - \lambda_k)$ is divergent or convergent according to whether $\sum_{k=1}^{\infty} (1/N_k)$ is divergent or convergent. Thus $\sum_{k=1}^{\infty} (1/N_k) = +\infty$, for example if $c_n = 1$ for $n = 1, 2, \dots$, one can find out the original composition of the urn with probability 1, whereas if $\sum_{k=1}^{\infty} (1/N_k) < \infty$ (for instance if $(c_n = n)$ this is impossible.

EXAMPLE 4. Suppose that ξ_n has under the condition that $\theta = \theta_i$ a Poisson distribution with mean value $\alpha_i \delta_n$, ($i = 1, 2$) where $\alpha_1 > 0$, $\alpha_2 > 0$, $\alpha_1 \neq \alpha_2$ and $\delta_n > 0$, $\lim_{n \rightarrow \infty} \delta_n = 0$. In this case

$$(4.12) \quad \lambda_k = \exp \left(- \left(\frac{\alpha_1 + \alpha_2}{2} - \sqrt{\alpha_1 \alpha_2} \right) \delta_k \right).$$

Clearly, $\sum_{k=1}^{\infty} (1 - \lambda_k)$ is divergent if and only if $\sum_{k=1}^{\infty} \delta_k$ is divergent. Thus, for instance, if $\delta_k = (\gamma/k)$, ($k = 1, 2, \dots$; $\gamma > 0$), it is possible to decide with probability 1 whether $\theta = \theta_1$ or $\theta = \theta_2$, but if $\delta_k = (\gamma/k^2)$, this is not possible.

EXAMPLE 5. Let ξ_n have a binomial distribution of fixed order N and parameter $\delta_n \theta_i$ under the condition that $\theta = \theta_i$, ($i = 0, 1$) where $\theta_0 > 0$, $\theta_1 > 0$, $\theta_0 \neq \theta_1$. Then we can easily see that the observations ξ_n , ($n = 1, 2, \dots$) contain full information on θ if and only if $\sum_{k=1}^{\infty} \delta_n = +\infty$.

EXAMPLE 6. Let η_n have the density function $f(x)$ where $f(x)$ is everywhere positive and has a continuous derivative such that $\int_{-\infty}^{+\infty} (f'(v)/f(v)) dv < +\infty$. Suppose that $\xi_n = m_0 + c_n \eta_n$ if $\theta = \theta_0$ and $\xi_n = m_1 + c_n \eta_n$ if $\theta = \theta_1$ where $m_0 \neq m_1$ and $c_n \rightarrow \infty$. Writing $d = m_1 - m_0$, we have

$$(4.13) \quad 1 - \lambda_k = \frac{1}{2} \int_{-\infty}^{+\infty} \left(\sqrt{f\left(u + \frac{d}{c_n}\right)} - \sqrt{f(u)} \right)^2 du.$$

Write $p(u) = \sqrt{f(u)}$; then we have

$$(4.14) \quad 1 - \lambda_k = \frac{1}{2} \int_{-\infty}^{+\infty} \left(\int_u^{u+(d/c_n)} p'(v) dv \right)^2 du.$$

Thus

$$(4.15) \quad 1 - \lambda_k \leq \frac{d^2}{8c_k^2} \int_{-\infty}^{+\infty} \frac{f'(v)^2}{f(v)} dv.$$

It follows that if the series $\sum_{k=1}^{\infty} (1/c_k^2) < +\infty$, then $\sum_{k=1}^{\infty} 1 - \lambda_k < +\infty$, and we do not get full information on θ .

On the other hand, the divergence of the series $\sum (1/c_k^2)$ ensures that the sequence of observations $\{\xi_n\}$ does contain full information on θ . As a matter of fact, since $p'(x)$ is continuous, there exists an interval (a, b) in which $p'(x)$ does not change sign and $|p'(x)| \geq \delta > 0$. Letting $h_n = d/c_n$, it follows that

$$(4.16) \quad 1 - \lambda_n \geq \delta^2(b - a - h_n)h_n^2.$$

Thus if $\sum_{n=1}^{\infty} (1/c_n^2) = +\infty$, then $\sum_{n=1}^{\infty} (1 - \lambda_n) = +\infty$.

5. Further remarks

S. Kakutani [5] has proved the following.

THEOREM K. *Let $(\Omega_n, \mathcal{G}_n)$ be measurable spaces ($n = 1, 2, \dots$). Let Ω be the product space $\prod_{n=1}^{\infty} \Omega_n$. Let μ_n and ν_n be two equivalent probability measures on Ω_n , and let μ and ν denote the product measures $\mu = \prod_{n=1}^{\infty} \mu_n$ and $\nu = \prod_{n=1}^{\infty} \nu_n$ on Ω . Then the measures μ and ν are either equivalent or orthogonal according to whether the infinite product $\prod_{n=1}^{\infty} \rho(\mu_n, \nu_n)$ is convergent or divergent. Here $\rho(\mu_n, \nu_n)$ denotes the Hellinger distance of the measures μ_n and ν_n ; that is, if m is any measure such that μ_n and ν_n are both absolutely continuous with respect to m ,*

$$(5.1) \quad \rho(\mu_n, \nu_n) = \int_{\Omega_n} \sqrt{\frac{d\mu_n}{dm} \cdot \frac{d\nu_n}{dm}} dm$$

where $(d\mu_n/dm)$ and $(d\nu_n/dm)$ are Radon-Nikodym derivatives.

(The value of ρ is clearly independent of the choice of m .)

Obviously our results are closely connected with the above mentioned theorem of S. Kakutani. (My thanks are due to Professor K. Jacobs for calling my attention to this fact.)

As a matter of fact, according to Kakutani's theorem, if μ_n and ν_n denote the measures with density $f_n(x)$ and $g_n(x)$ with respect to the Lebesgue measure on the real line, then according to whether $\theta = \theta_0$ or $\theta = \theta_1$, one obtains in the sequence-space $x = (\xi_1, \xi_2, \dots, \xi_n, \dots)$ the product measure μ or ν . Further, our λ_k is equal to the Hellinger distance ρ_k of μ_k and ν_k . It follows that $\mu \sim \nu$ or $\mu \perp \nu$ according to whether $\prod_{k=1}^{\infty} \lambda_k > 0$ or $\prod_{k=1}^{\infty} \lambda_k = 0$.

If $\prod_{k=1}^{\infty} \lambda_k = 0$, that is, if $\mu \perp \nu$, then there exists a measurable set A in X such that $\mu(A) = 1$ and $\nu(A) = 0$. In this case given the infinite sequence $\{\xi_n\}$ one can clearly decide with probability 1 whether $\theta = \theta_0$ or $\theta = \theta_1$: if the infinite sequence $(\xi_1, \dots, \xi_n, \dots) \in A$ we decide for $\theta = \theta_0$, and in the opposite case for $\theta = \theta_1$. Now one can obviously find a sequence of sets A_n such that A_n is a cylinder set of X , its base belonging to the finite product set $\prod_{k=1}^n \Omega_k$, such that $\mu(A_n) \rightarrow 1$ and $\nu(A_n) \rightarrow 0$ for $n \rightarrow +\infty$. Thus if after observing $\xi_1, \dots, \xi_n$ we decide for θ_0 or θ_1 according to whether or not the point $(\xi_1, \dots, \xi_n)$ belongs to the base of A_n , the error of our decision tends to 0 for $n \rightarrow \infty$.

Conversely, it is easy to see that such a sequence of sets cannot exist if $\mu \sim \nu$.

Thus, in view of the corollary of theorem 1, theorem 4 can be deduced from theorem K. Note, however, that our direct approach is not only more elementary than this one via Kakutani's theorem, it also gives somewhat more, as it shows not only that $\epsilon_n \rightarrow 0$ if and only if $\lim_{n \rightarrow \infty} \prod_{k=1}^n \lambda_k = 0$, but also gives estimates between these quantities for finite values of n .

REFERENCES

- [1] D. V. LINDLEY, "On a measure of the information provided by an experiment," *Ann. Math. Statist.*, Vol. 27 (1956), pp. 986-1005.
- [2] A. RÉNYI, "On the amount of information concerning an unknown parameter in a sequence of observations," *Publ. Math. Inst. Hungar. Acad. Sci.*, Vol. 9 (1964), pp. 617-624.
- [3] ———, "On the amount of missing information and the Neyman-Pearson lemma," *Festschrift for J. Neyman*, Wiley, 1966, pp. 281-288.
- [4] ———, "On the amount of information in a frequency-count," *The 35th Session of the International Statistical Institute at Beograd*, 1965, pp. 1-8.
- [5] S. KAKUTANI, "On equivalence of infinite product measures," *Ann. of Math.*, Vol. 49 (1948), pp. 214-226.

231, 236, 265, 266, 267, 285, 305, 328

ON SOME PROBLEMS IN THEORY
OF ORDER STATISTICS

A. RÉNYI

SUMMARY

In 1953 the author has published a paper [1] concerning the ratio of the empirical and the theoretical distribution function of a sample. Since that time a great number of results have been obtained in this field. The present paper contains a review of these developments and gives new simple proofs for certain theorems. Some unsolved problems are also mentioned and some remarks are made on applications of the results in question.

§ 1. INTRODUCTION

Let $\{\xi_1, \dots, \xi_n\}$ be a sample of n independent observations from a population; by other words let $\xi_1, \dots, \xi_n$ be n independent random variables with the same distribution function $F(x)$. Let us denote by $F_n(x)$ the empirical distribution function of the sample $\{\xi_1, \dots, \xi_n\}$, i.e. put

$$(1.1) \quad F_n(x) = \frac{1}{n} \sum_{\substack{\xi_k \leq x \\ 1 \leq k \leq n}} 1.$$

Let $\xi_1^* \leq \xi_2^* \leq \dots \leq \xi_n^*$ be the order statistics of the sample $\{\xi_1, \dots, \xi_n\}$, i.e. let $\xi_1^*, \dots, \xi_n^*$ be the elements of the sample $\{\xi_1, \dots, \xi_n\}$ arranged into a nondecreasing sequence.

Clearly

$$(1.2) \quad F_n(x) = \begin{cases} 0 & \text{if } x \leq \xi_1^* \\ \frac{k}{n} & \text{if } \xi_k^* < x \leq \xi_{k+1}^* \quad (k = 1, 2, \dots, n-1) \\ 1 & \text{if } \xi_n^* < x. \end{cases}$$

Thus $F_n(x)$ is for each x a random variable. According to Glivenko's theorem [2] $\sup_x |F_n(x) - F(x)|$ tends with probability 1 to 0 for $n \rightarrow +\infty$; according to the theorems of N. V. Smirnov [3] and A. N. Kolmogorov [4] if $F(x)$ is continuous

$$(1.3) \quad \lim_{n \rightarrow +\infty} P(\sqrt{n} \cdot \sup_x (F_n(x) - F(x)) < y) = \begin{cases} 1 - e^{-2y^2} & \text{if } y > 0 \\ 0 & \text{if } y \leq 0 \end{cases}$$

and

$$(1.4) \quad \lim_{n \rightarrow +\infty} P(\sqrt{n} \cdot \sup_x |F_n(x) - F(x)| < y) = \begin{cases} \sum_{k=-\infty}^{+\infty} (-1)^k e^{-2k^2 y^2} & \text{if } y < 0 \\ 0 & \text{if } y \leq 0. \end{cases}$$

The fact that $F_n(x)$ approaches $F(x)$ if $n \rightarrow +\infty$ can be expressed by studying the ratio $\frac{F_n(x)}{F(x)}$ too. However, while of course $\frac{F_n(x)}{F(x)}$ tends to 1 with probability 1 if $n \rightarrow +\infty$, for each x for which $F(x) > 0$, this does not hold uniformly in x ; as a matter of fact one has for each n if $F(x)$ is continuous

$$(1.5) \quad P\left(\sup_{0 < F(x)} \frac{F_n(x)}{F(x)} > 1 + \varepsilon\right) = \frac{1}{1 + \varepsilon} \quad \text{if } \varepsilon \geq 0.$$

(1.5) is due to Daniels [22] rediscovered by H. Robbins [23] and Chang Li Chien [5] (Chapman [6]) and Dempster [24] A new proof of (1.5) will be given in § 2.

It follows, however, from Glivenko's theorem that $\frac{F_n(x)}{F(x)}$ tends to 1 uniformly in x with probability 1 if we consider only those values of x for which $F(x) \geq a > 0$, where a is a fixed positive number not depending on n . Moreover it has been shown in [1] that the following analogues of Kolmogorov's and Smirnov's results are valid if $F(x)$ is any continuous distribution function:

$$(1.6) \quad \lim_{n \rightarrow +\infty} P\left(\sqrt{n} \cdot \sup_{a \leq F(x)} \frac{(F_n(x) - F(x))}{F(x)} < y\right) = \begin{cases} \sqrt{\frac{2}{\pi}} \int_0^{y\sqrt{\frac{a}{1-a}}} e^{-\frac{t^2}{2}} dt & \text{if } y > 0 \\ 0 & \text{if } y \leq 0 \end{cases}$$

$$(1.7) \quad \lim_{n \rightarrow +\infty} P\left(\sqrt{n} \cdot \sup_{a \leq F(x)} \frac{|F_n(x) - F(x)|}{F(x)} < y\right) = \begin{cases} \frac{4}{\pi} \sum_{k=0}^{\infty} (-1)^k \frac{e^{-\frac{(2k+1)^2 \pi^2 (1-a)}{8y^2 a}}}{2k+1} & \text{if } y > 0 \\ 0 & \text{if } y \leq 0. \end{cases}$$

In [1] still more general results have been given, corresponding to the case when only those values of k are considered for which $a \leq F(x) \leq b$ where $0 < a < b < 1$.

These results were obtained by a method based on the following observations.

Lemma 1. The random variables ξ_k^* can be represented in the form

$$(1.8) \quad \xi_k^* = F^{-1}\left(\exp\left(-\sum_{j=0}^{n-k} \frac{\delta_j}{n-j}\right)\right) \quad (k = 1, 2, \dots, n)$$

where $\delta_0, \delta_1, \dots, \delta_{n-1}$ are independent random variables with the same exponential distribution, with mean 1, i.e. $P(\delta_j < x) = 1 - e^{-x}$ if $x \geq 0$. (As regards further developments of this method see [7] and [16]).

Another simple but useful fact (see e.g. [8]) is the following.

Lemma 2. Putting $\eta_k = F(\xi_k)$, the random variables $\eta_1, \dots, \eta_n$ are uniformly distributed in the interval $(0, 1)$, and putting $\eta_k^* = F(\xi_k^*)$, under condition $\eta_{k+1}^* = c$ ($0 < c < 1$) the random variables $\frac{\eta_1^*}{c}, \dots, \frac{\eta_k^*}{c}$ are distributed

as the order statistics of a sample of size k and the random variables $\frac{\eta_{k+2}^* - c}{1 - c}$,
 $\dots, \frac{\eta_n^* - c}{1 - c}$ are distributed as the order statistics of a sample of size $n - k - 1$
from a distribution uniform in the interval $(0, 1)$.

§ 2. EXACT DISTRIBUTIONS

We start by giving a new simple proof for (1.5). Clearly if $\eta_1^* > 0$ (which holds with probability 1)

$$(2.1) \quad \sup_{0 < F(x)} \frac{F_n(x)}{F(x)} = \text{Max}_{1 \leq k \leq n} \frac{k}{n \eta_k^*} = \left(\text{Min}_{1 \leq k \leq n} \frac{n \eta_k^*}{k} \right)^{-1}.$$

Thus putting

$$(2.2) \quad G_n(t) = P \left(\sup_{0 < F(x)} \frac{F_n(x)}{F(x)} < \frac{1}{t} \right) \quad (t > 0)$$

one has

$$(2.3) \quad G_n(t) = P \left(\text{Min}_{1 \leq k \leq n} \frac{n \eta_k^*}{k} > t \right).$$

In view of Lemma 2 and taking into account that the density function of η_n^* is equal to ny^{n-1} for $0 < y < 1$, we obtain the following recursion formula:

$$(2.4) \quad G_n(t) = \int_t^1 G_{n-1} \left(\frac{(n-1)t}{ny} \right) ny^{n-1} dy.$$

Now evidently

$$(2.5) \quad G_1(t) = P(\eta_1 > t) = 1 - t \quad (0 \leq t \leq 1),$$

and using (2.4) the formula

$$(2.6) \quad G_n(t) = 1 - t \quad \text{for } n = 1, 2, \dots$$

follows by induction.

Clearly $\inf_{F(x) > 0} \frac{F_n(x)}{F(x)} = 0$ with probability 1; however the quantity $\inf_{F_n(x) > 0} \frac{F_n(x)}{F(x)}$ has (see [5]) a nontrivial limit distribution if $n \rightarrow \infty$, namely

$$(2.7) \quad \lim_{n \rightarrow +\infty} P \left(\inf_{F_n(x) > 0} \frac{F_n(x)}{F(x)} < \frac{1}{t} \right) = e^{-t} + \sum_{k=1}^{\infty} \frac{(k-1)^{k-1} (te^{-t})^k}{k!} \quad \text{if } t > 0.$$

A new proof of (2.7) will be given below.

Clearly (with probability 1)

$$(2.8) \quad \inf_{F_n(x) > 0} \frac{F_n(x)}{F(x)} = \min_{1 \leq k \leq n-1} \frac{k}{n \cdot \eta_{k+1}^*} = \left(\max_{1 \leq k \leq n-1} \frac{n \cdot \eta_{k+1}^*}{k} \right)^{-1}$$

Thus (2.7) can also be written in the form

$$(2.9) \quad \lim_{n \rightarrow +\infty} P \left(\max_{1 \leq k \leq n-1} \frac{n \cdot \eta_{k+1}^*}{k} > t \right) = e^{-t} + \sum_{k=1}^{\infty} \frac{(k-1)^{k-1} (te^{-t})^k}{k!} \text{ if } t > 0.$$

It is easy to show by the *Bürman—Lagrange* formula for the power series expansion of the inverse function (see [19]) that

$$(2.10) \quad e^{-t} + \sum_{k=1}^{\infty} \frac{(k-1)^{k-1}}{k!} (te^{-t})^k = 1 \text{ if } 0 \leq t \leq 1.$$

The reformulation (2.9) of (2.7) raises the question: what is the limit distribution of $\max_{1 \leq k \leq n} \frac{n \eta_k^*}{k}$ for $n \rightarrow +\infty$? This question is answered by the following counterpart of (2.7):

Theorem 1.

$$(2.11) \quad \begin{aligned} \lim_{n \rightarrow \infty} P \left(\sup_{0 \leq x \leq 1} \frac{F(x)}{F_n(x) + \frac{1}{n}} > t \right) &= \lim_{n \rightarrow \infty} P \left(\inf_{0 \leq x \leq 1} \frac{F_n(x) + \frac{1}{n}}{F(x)} < \frac{1}{t} \right) = \\ &= \lim_{n \rightarrow +\infty} P \left(\max_{1 \leq k \leq n} \frac{n \eta_k^*}{k} > t \right) = \sum_{k=0}^{\infty} \frac{t^k e^{-(k+1)t} (k+1)^{k-1}}{k!} \text{ if } t \geq 0. \end{aligned}$$

Note that one has (see [19])

$$(2.12) \quad \sum_{k=0}^{\infty} \frac{t^k e^{-(k+1)t} (k+1)^{k-1}}{k!} = 1 \text{ if } 0 \leq t \leq 1.$$

The exact distribution of

$$\sup_{v \leq F(x)} \frac{F_n(x)}{F(x)} \quad \text{and} \quad \inf_{a \leq F(x)} \frac{F_n(x)}{F(x)}$$

has been computed by Goro Ishi [9], by evaluating many-dimensional integrals. A simpler proof of these formulae was given by N. V. Smirnov [10], based on the combinatorial proof of the following lemma (compare also [15]).

Lemma 3.

If $0 < p < 1$ and $n \geq 2$

$$(2.13) \quad P \left(\eta_k^* \leq p + \frac{(k-1)(1-p)}{n-1} \text{ for } 1 \leq k \leq n-1 \right) = p \left(1 + \frac{1-p}{n-1} \right)^{-1}.$$

We shall give a new proof for Lemma 3. Let us put

$$(2.14) \quad P(p) = P \left(\eta_k^* \leq p + \frac{(k-1)(1-p)}{n-1} \text{ for } 1 \leq k \leq n-1 \right).$$

By Lemma 2 and taking into account that the density function of η_1^* is equal to $n(1-y)^{n-1}$ for $0 < y < 1$, we get the recursion formula

$$(2.15) \quad P_n(p) = \int_0^p n(1-y)^{n-1} P_{n-1} \left(\frac{p-y + \frac{1-p}{n-1}}{1-y} \right) dy.$$

As evidently $P_2(p) = P(\eta_1^* < p) = p(1 + (1-p))$,

$$(2.16) \quad P_n(p) = p \left(1 + \frac{1-p}{n-1} \right)^{-1}$$

follows from (2.15) by induction.

Using Lemma 2 and Lemma 3 we can deduce, following Smirnov, immediately

Lemma 4. Putting

$$(2.17) \quad P_{n,s}(a, b) = P(\eta_k^* \leq a + (k-1)b \text{ for } 1 \leq k \leq s, \eta_{s+1}^* > a + sb)$$

one has

$$(2.18) \quad P_{n,s}(a, b) = \binom{n}{s} a(a+sb)^{s-1} (1-a-sb)^{n-s}$$

for $s = 0, 1, \dots, n$; $a > 0$, $b > 0$, $a + sb < 1$.

Corollary: Abel's identity

$$\sum_{s=0}^n \binom{n}{s} a(a+sb)^{s-1} (1-a-sb)^{n-s} = 1.$$

Now we can turn to the proof of (2.11) and (2.9). Clearly

$$P \left(\max_{1 \leq k \leq n} \frac{n \eta_k^*}{k} > t \right) = \sum_{s=0}^{n-1} P \left(\eta_k^* \leq \frac{kt}{n} \text{ for } 1 \leq k \leq s, \eta_{s+1}^* > \frac{(s+1)t}{n} \right).$$

Thus from Lemma 4

$$(2.19) \quad P \left(\max_{1 \leq k \leq n} \frac{n \eta_k^*}{k} > t \right) = \sum_{s=0}^{n-1} \binom{n}{s} \left(\frac{t}{n} \right)^s (s+1)^{s-1} \left(1 - \frac{(s+1)t}{n} \right)^{n-s}$$

By passing to the limit $n \rightarrow +\infty$, (2.11) follows immediately.

Similarly one has

$$\begin{aligned} P \left(n \max_{1 \leq k \leq n-1} \frac{\eta_{k+1}^*}{k} > t \right) &= \left(1 - \frac{t}{n} \right)^n + \\ &+ \int_0^{\frac{t}{n}} n(1-y)^{n-1} \left[\sum_{s=0}^{n-2} P_{n-1,s} \left(\frac{\frac{t}{n}-y}{1-y}, \frac{t}{n(1-y)} \right) \right] dy. \end{aligned}$$

Thus it follows, by passing to the limit $n \rightarrow +\infty$, that

$$\begin{aligned} \lim_{n \rightarrow \infty} P \left(\max_{1 \leq k \leq 1-n} \frac{n \eta_{k+1}^*}{k} > t \right) &= e^{-t} + \sum_{s=0}^{\infty} \frac{e^{-(s+1)t}}{s!} \int_0^t (t-u) [(s+1)t-u]^{-1} du = \\ &= e^{-t} + \sum_{k=1}^{\infty} \frac{(te^{-t})^k (k-1)^{k-1}}{k!} \end{aligned}$$

which proves (2.9).

The distribution of $\sup_{F(x) > 0} \frac{|F_n(x) - F(x)|}{F(x)}$ could also be obtained by this method.

§ 3. VARIOUS GENERALIZATIONS

It is well known that the Kolmogorov—Smirnov theorems can be generalized for two samples. The corresponding result for the case of one-sided relative deviation has been proved by Wang Shou-Jen [11], and for the two-sided deviation by M. Csörgő [12]. In all these results it has been supposed that the distribution function $F(x)$ is continuous; the Kolmogorov—Smirnov theorems as well as of the theorems (1.6) and (1.7) of the author have been extended for the case of discontinuous $F(x)$ by P. Schmid [13] and H. Carnal [14].

M. Csörgő has given [21] a series of variants new proof and generalizations of theorems (1.6) and (1.7). In his paper [17] he has remarked that if one replaces the ratio $\frac{F_n(x) - F(x)}{F(x)}$ by $\frac{F_n(x) - F(x)}{F_n(x)}$, the limit distributions (1.6) and (1.7) remain unchanged.

As regards (1.6), this can be shown very easily by the remark that

$$P \left(\sqrt{n} \cdot \sup_{a \leq F_n(x)} \frac{(F_n(x) - F(x))}{F_n(x)} < y \right) = P \left(\sqrt{n} \cdot \sup_{a \leq F_n(x)} \frac{(F_n(x) - F(x))}{F(x)} < \frac{y}{1 - \frac{y}{\sqrt{n}}} \right),$$

and asymptotically one can replace the condition $a \leq F_n(x)$ by $a \leq F(x)$. The modification of (1.7) can be reduced similarly to (1.7).

In other papers ([18] and [20]) M. Csörgő deals with the following generalization: Let us consider r independent samples of sizes $n_1, \dots, n_r$ respectively, from the same population with the continuous distribution function $F(x)$ and let $F_{n_1}(x), \dots, F_{n_r}(x)$ be their empirical distribution functions. He considers

the distribution of $\sup_{a < F(x)} \frac{\left(\prod_{j=1}^r F_{n_j}(x) - F^r(x) \right)}{F^r(x)}$. He obtains that multiplying this quantity by $\sqrt{N}$ where $\frac{1}{N} = \sum_{j=1}^r \frac{1}{n_j}$, if $n_1, \dots, n_r$ tend to infinity so that the positive and finite limits $\lim_{n_j} \frac{n_1}{n_j} = \varrho_j$ exist, ($j = 2, \dots, r$) this quantity has again the limit distribution function (1.6).

§ 4. SOME FURTHER REMARKS

The main reason — as pointed out in [1] — for using tests based on the ratio $\frac{F_n(x)}{F(x)}$ instead of the difference $F_n(x) - F(x)$, is that these tests deal with

the relative error instead of the absolute error, which corresponds better to the general principles of numerical analysis. It remains however an open question to compare the powers of the corresponding tests. Another reason for using tests based on $\sup_{a \leq F(x) \leq b} \frac{|F_n(x) - F(x)|}{F(x)}$ may be that the sample considered is truncated, i.e. the exact values of the small (or large) elements of the sample are not available. As pointed out by Ishii, this is usually the case in life-testing.

As regards the quantity $\sup_x \frac{\left(\prod_{j=1}^r F_{n_j}(x) - F^r(x) \right)}{F^r(x)}$ considered by Csörgő, the question arises, whether it is not more advantageous to unite the r samples into a single sample? The author's guess is that this increases usually the power of the test; nevertheless it may be advantageous not to unite the samples if the size of the united sample would be very large, e.g. when testing a procedure for generating random numbers with a prescribed distribution.*

As a matter of fact, the number of pairwise comparisons needed to rearrange a set of rn numbers into an increasing sequence is larger than the number of pairwise comparisons needed to rearrange into increasing sequences r given sequences of n numbers each.

REFERENCES

- [1] Rényi, A.: On the theory of order statistics. *Acta Math. Acad. Sci. Hung.*, **4** (1953), 191—231.
- [2] Glivenko, V. I.: Sulla determinazione empirica delle leggi di probabilità. *Giornale Ist. Ital. Attuari*, **4** (1933), 92—99.
- [3] Smirnov, N. V.: Über die Verteilung des allgemeinen Gliedes in der Variationsreihe. *Metron*, **12** (1935), 59—81.
- [4] Kolmogoroff, A. N.: Sulle determinazione empirica di una legge di distribuzione. *Giorn. Ist. Ital. Attuari*, **4** (1933), 83—91.
- [5] Chang Li Chien: On the ratio of an empirical distribution function to the theoretical distribution function (in Chinese with English summary). *Acta Math. Sinica*, **5** (1955), 347—368.
- [6] Chappman, P. G.: On a limiting distribution due to Rényi. *Ann. Math. Stat.*, **29** (1958), 1282.
- [7] Rao, M. M.: Theory of Order Statistics. *Math. Annalen*, **147** (1962), 298—312.
- [8] Hajós, G. and Rényi, A.: Elementary proofs of some basic facts concerning order statistics. *Acta Math. Acad. Sci. Hung.*, **5** (1954), 1—6.
- [9] Goro Ishii: On the exact probabilities of Rényi's tests. *Ann. Inst. Statist. Math.*, **11** (1959), 17—24.
- [10] Smirnov, N. V.: The probability of large values of one-sided non-parametric tests of goodness of fit (in Russian). *Trudy Mat. Inst. Steklov*, **64** (1961), 185—210.
- [11] Wang Shou-Jen: On the limiting distribution of the ratio of two empirical distributions (in Chinese with English summary). *Acta Math. Sinica*, **5** (1955), 253—267.

* The attention of the author to this problem was called by A. Békéssy.

- [12] Csörgő, M.: Some Smirnov type theorems of probability theory. *Annals of Math. Stat.*, **36** (1965), 1113—1119.
- [13] Schmidt, P.: On the Kolmogorov and Smirnov limit theorems for discontinuous distribution functions. *Ann. Math. Stat.*, **29** (1958) 1011—1027.
- [14] Carnal, H.: Sur les théorèmes de Kolmogoroff et Smirnov dans le cas d'une distribution discontinue. *Comm. Math. Helv.*, **37** (1962), 19—35.
- [15] Nef, W.: Über die Differenz zwischen theoretischer und empirischer Verteilungsfunktion. *Z. Wahrscheinlichkeitstheorie*, **3** (1964), 154—162.
- [16] Blom, G.: Statistical estimates and transformed betavariates. Wiley, New York, 1958.
- [17] Csörgő, M.: Some Rényi-type limit theorems for empirical distribution functions. *Ann. Math. Stat.*, **36** (1965), 322—326.
- [18] Csörgő, M.: K -sample analogues of Rényi's Kolmogorov—Smirnov-type theorems. *Bull. Amer. Math. Soc.*, **71** (1965), 616—618.
- [19] Pólya, G. and Szegő, G.: Aufgaben und Lehrsätze aus der Analysis, Springer, Berlin, 1925, Vol. I. 125.
- [20] Csörgő, M.: Some k -sample Kolmogorov—Smirnov—Rényi type theorems for empirical distribution functions. *Acta Math. Acad. Sci. Hung.*, **17** (1966), 325—334.
- [21] Csörgő, M.: A new proof of some results of Rényi and the asymptotic distribution of the range of his Kolmogorov—Smirnov type random variables. *Canadian Journ. Math.*, **19** (1967), 550—558.
- [22] Daniels, H. E.: The statistical theory of the strength of bundles of threads. *Proc. Roy. Soc.*, **A183**, 412—416.
- [23] Robbins, H.: A one-sided confidence interval for an unknown distribution function. *AMS*, **25** (1954), 409.
- [24] Dempster, A. P.: *AMS*, **30** (1959), 593—596.

84, 85, 86, **246**

NOTE

Article No.84 is interesting and significant mainly in two respects: a) a powerful method is elaborated in it for the derivation of limiting distribution laws in connection with order statistics, b) new statistics are introduced for one-sample goodness of fit criteria, the limiting distributions of which are derived by means of the method a). Extending the Markov-chain property of the ordered sample-elements due to Kolmogorov to an additive Markov property, this is what is utilized. — A great interest and a quick influence was the reaction to the work: Wang Shou Yen determined the limiting distribution of the corresponding two-sample statistics in 1955, the limiting distributions if the common distribution function of the underlying variables are non-continuous were determined by Schmid [30], exact distributions were found by Ishii Goro in [21], the critical values for the test statistic was published by J. Janko in [22] and later by Bolshew and Smirnov [4]. The method mentioned above under a) was fruitfully utilized, i.e. by Rossberg and Krem. Analogous statistics to the relative deviation were considered by Vincze [33] and Csörgő. Csörgő has given a peculiar interest to the statistics introduced by Rényi and considered them in a series of papers (see [10]—[16]) given new proofs, exact distributions, alterations, etc. Rényi-type statistics were introduced and considered — given exact distributions and tables for critical values — by Z. W. Birnbaum and B. P. Lientz [2]. — A not at all complete list of further papers considering Rényi's mentioned results are embodied also in the references.

In No. 246 he summarized the literature connected with his article No. 84 appearing in the meantime. (I. V.)

REFERENCES

- [1] Birnbaum, Z. W. and Liehtz, B. P.: Exact distributions for some Rényi-type statistics. *Zastos. Mat.*, **10** (1969), 179–192.
- [2] Birnbaum, Z. W. and Liehtz, B. P.: Tables of critical values of some Rényi-type statistics for finite sample sizes. *J. Amer. Statist. Ass.*, **64** (1969), 870–877.
- [3] Blom, G.: *Statistical estimates and transformed beta-variables*. Almqvist and Wiksell, Stockholm, 1958.
- [4] Bolshev, L. N. and Smirnov, N. V.: *Tablitsi matematicheskoy statistiki. Izdatelstva "NAUKA"*. Moscow, 1965.
- [5] Book, S. A.: Large deviation probabilities for weighted sums. *Ann. Math. Statist.*, **43** (1972), 1221–1234.
- [6] Csáki, E. and Tusnády, G.: On the number of intersections and the ballot-theorem. *Periodica Mathematica Hungarica*, **2** (1972), 5–13.
- [7] Chapman, P. G.: On a limiting distribution due to Rényi. *Ann. Math. Statist.*, **29** (1958), 1282.
- [8] Chapman, P. G.: A comparative study of several one-sided goodness-of-fit tests. *Ann. Math. Statist.*, **29** (1958), 655–674.
- [9] Chernoff, H., Gastwirth, J. L. and Johns, M. V., Jr.: Asymptotic distribution of linear combinations of functions of order statistics with applications to estimation. *Ann. Math. Statist.*, **38** (1967), 52–72.
- [10] Csörgő, M.: On some Kolmogorov–Smirnov–Rényi type theorems of probability theory. *Unpublished doctoral dissertation*. McGill University, Montreal (1963).
- [11] Csörgő, M.: Some Rényi type limit theorems for empirical distribution functions. *Ann. Math. Statist.*, **36** (1965), 322–326.
- [12] Csörgő, M.: Some Smirnov type theorems of probability theory. *Ann. Math. Stat.*, **36** (1965), 1113–1119.
- [13] Csörgő, M.: Exact probability distribution functions of some Rényi-type statistics. *Proc. Amer. Math. Soc.*, **16** (1965), 1158–1166.
- [14] Csörgő, M.: Some k -sample Kolmogorov–Smirnov–Rényi type theorems for empirical distribution functions. *Acta Math. Acad. Sci. Hung.*, **17** (1966), 325–334.
- [15] Csörgő, M.: A new proof of some results of Rényi and the asymptotic distribution of the range of his Kolmogorov–Smirnov type random variables. *Can. J. Math.*, **19** (1967), 550–558.
- [16] Csörgő, M. and Seshadri, V.: Characterizing the Gaussian and Exponential Laws via Mappings onto the Unit Interval. *Z. Wahrscheinlichkeitstheorie verw. Geb.*, **18** (1971), 333–339.
- [17] Eicker, F.: On the probability that a sample distribution function lies below a line segment. *Ann. Math. Stat.*, **41** (1970), 2075–2092.
- [18] Fisz, M.: *Probability theory and mathematical statistics*. Wiley & Sons, New York.
- [19] Galambos, J.: Characterization of certain populations by independence of order statistics. *J. Appl. Prob.*, **9** (1972), 224–230.
- [20] Hájek, J. and Sidák, Z.: *Theory of rank tests*. Academia, Prague 1967.
- [21] Ishii Goro: On the exact probabilities of Rényi's test. *Ann. Inst. Stat. Math. Tokyo*, **11** (1959), 17 ff.
- [22] Janko, J.: *Statisticky tabulky*. Ces-Slov. Akad. Ved. Praga, 1958.
- [23] Krem, A.: On the independence in the limit of extreme and central order statistics. *Publ. Math. Inst. Hung. Acad. Sci.*, **8** (1963), 469–474.
- [24] Preschán, F. and Pyke, R.: Tests for monotone failure rate. *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability*. Berkeley and Los Angeles, University of California Press, 1967, **3**, 293–312.
- [25] Rao, M. M.: Theory of order statistics. *Math. Annalen*, **147** (1962), 298–312.
- [26] Rossberg, H.-J.: Über das asymptotische Verhalten der Rand- und Zentralglieder einer Variationsreihe. *Publ. Math. Inst. Hung. Acad. Sci.*, **8** (1963), 463–468.
- [27] Rossberg, H.-J.: Characterization of distribution functions by the independence of certain functions of order statistics. *Sankhya*, **34** (1972), 111–120.
- [28] Sahler, W.: A survey on distribution-free statistics based on differences between distribution functions. *Metrika*, **13** (1968), 149–169.
- [29] Schnetterser, L.: *Einführung in die mathematische Statistik*. 2nd ed. Springer Verlag, Wien 1966.

- [30] Schmid, P.: On the Kolmogorov and Smirnov limit theorems for discontinuous distribution functions. *Ann. Math. Stat.*, **29** (1958), 1011—1027.
- [31] Shanti S. Gupta and Panchapakesan, S.: On order statistics and some applications of combinatorial methods in statistics. *A Survey on Combinatorial Theory*. Ed.: J. N. Srivastava et al. North-Holland Publishing Company, 1973.
- [32] Stiegler, S. M.: Linear functions of order statistics. *Ann. Math. Stat.*, **40** (1969), 770—788.
- [33] Vincze, I.: Einige zweidimensionale Verteilungs- und Grenzübergangssätze in der Theorie der geordneten Stichproben. *Publ. Math. Inst. Hung. Acad. Sci.*, **2** (1957), 183—209.
- [34] Wang Shou Jen: On the limiting distribution of the ratio of two empirical distributions (Chinese with English summary). *Acta Math. Sinica*, **5** (1955), 253—267.
- [35] Weiss, L.: On Asymptotic sampling theory for distributions approaching the uniform distribution. *Z. Wahrscheinlichkeitstheorie und verw. Geb.*, **4** (1965), 217—221.

Zufällige konvexe Polygone in einem Ringgebiet

A. RÉNYI und R. SULANKE

1. Einleitung

Sei K ein nicht ausgearteter, beschränkter, konvexer Bereich der euklidischen Ebene und B ein beliebiger, im Innern von K enthaltener konvexer Bereich. Wir wählen n zufällige Geraden $g_1, \dots, g_n$, die den Bereich K , aber nicht den Bereich B treffen. Die g_i seien unabhängig; ihre Verteilung sei durch das euklidische invariante Geradenmaß μ mit der Dichte dg definiert (W. BLASCHKE [1], § 2). Durch H_i bezeichnen wir die von g_i bestimmte abgeschlossene Halbebene, die B enthält. Dann ist

$$(1.1) \quad \Pi_n = \bigcap_{i=1}^n H_i$$

ein durch die g_i eindeutig bestimmtes, zufälliges konvexes Polygon, das B enthält. Durch X_n bezeichnen wir die Anzahl der Ecken von Π_n . Wir wollen das asymptotische Verhalten der mathematischen Erwartung der Eckenanzahl X_n unter verschiedenen Voraussetzungen für B bestimmen.

In § 2 stellen wir die Formeln für die zu untersuchenden Wahrscheinlichkeiten auf und leiten einige einfache, in den §§ 3–5 anzuwendende Abschätzungen her. Ferner zeigen wir, daß die Wahrscheinlichkeit dafür, daß Π_n nicht geschlossen ist, ebenso wie die Wahrscheinlichkeit dafür, daß Π_n nicht in K enthalten ist, von der Ordnung $O(\gamma^n)$ ($0 < \gamma < 1$), gegen Null geht. In § 3 betrachten wir den Fall, daß B in einem Punkt ausartet, und beweisen $E(X_n) \rightarrow \frac{\pi^2}{2}$ für $n \rightarrow +\infty$. In dem Fall, daß B einen glatten Rand beschränkter Krümmung hat, gilt $E(X_n) \sim \text{konst. } n^{1/3}$ (Satz 4, § 4); wenn schließlich B ein konvexes r -Eck ist ($r \geq 2$; $r = 2$ bedeutet, daß B in eine Strecke ausartet), ergibt sich $E(X_n) \sim \frac{2}{3} r \log n$ (Satz 5, § 5). Die Größenordnung, in der $E(X_n)$ in den letzten beiden Fällen mit n gegen Unendlich geht, stimmt also mit den entsprechenden Größenordnungen für den Fall der Eckpunkte der konvexen Hülle von n in B zufällig gewählten Punkten überein (A. RÉNYI, R. SULANKE [2]).

Herrn L. BERG möchten wir für einige Hinweise zu den Berechnungen in § 5 herzlich danken.

Das Resultat von § 3 kann folgendermaßen interpretiert werden: Wir betrachten ein System von n zufälligen linearen Ungleichungen $a_k x + b_k y \leq c_k$ ($k = 1, 2, \dots, n$). Das Wort „zufällig“ bedeute, daß die Verteilung der voneinander unabhängigen Geraden $a_k x + b_k y = c_k$, die alle den Bereich K treffen sollen, durch das invariante Geradenmaß bestimmt ist und der Punkt $B(x=0, y=0) \in K$ allen Ungleichungen genügt. Sei X_n die kleinste Zahl mit der folgenden Eigenschaft: Es gibt X_n aus den n Ungleichungen derart, daß jeder Punkt (x, y) , der

diesen X_n Ungleichungen genügt, sogar alle n Ungleichungen erfüllt. Unser Ergebnis besagt, daß für $n \rightarrow \infty$ der Erwartungswert der minimalen Anzahl X_n der „kritischen“ Ungleichungen gegen $\pi^2/2$ strebt. Also kann man erwarten, daß man bei der Lösung einer Aufgabe der Linearprogrammierung mit zwei Unbekannten und einer beliebig großen Anzahl linearer Ungleichungen mit zufälligen Daten im Mittel nur eine ziemlich kleine Anzahl von Schritten nach einem der bekannten Verfahren benötigt. So ergibt sich naturgemäß das Problem, die analoge Aufgabe für eine beliebige Anzahl von Unbekannten (also für den Durchschnitt von zufälligen Halbräumen eines k -dimensionalen Raumes, $k=3, 4, \dots$) zu behandeln. Diese Aufgabe hat unlängst Herr WOLFGANG M. SCHMIDT gelöst, indem er bewies, daß die mittlere minimale Anzahl der „kritischen“ Ungleichungen auch im k -dimensionalen Fall ($k=3, 4, \dots$) gegen einen endlichen, nur von k abhängigen Grenzwert λ_k strebt; sein Beweis ergibt aber nur die Existenz der Zahlen λ_k und nicht deren genauen Wert. Aus dem Satz von Herrn WOLFGANG M. SCHMIDT folgt für den von uns betrachteten zweidimensionalen Fall die Existenz der Grenzverteilung von X_n . Auf die explizite Bestimmung dieser Grenzverteilung hoffen wir in einer anderen Arbeit zurückzukommen.

2. Grundformeln und einfache Abschätzungen

Sei $S_{ij} = g_i \cap g_j$ ($i \neq j$). Der Punkt S_{ij} existiert mit Wahrscheinlichkeit 1. Setzen wir $\varepsilon_{ij} = 1$, wenn S_{ij} Eckpunkt von Π_n ist, und $\varepsilon_{ij} = 0$ sonst, so gilt

$$(2.1) \quad X_n = \sum_{1 \leq i < j \leq n} \varepsilon_{ij}.$$

Sei $W(n)$ die Wahrscheinlichkeit dafür, daß S_{12} Eckpunkt von Π_n ist. Aus Symmetriegründen ergibt sich für die mathematische Erwartung

$$(2.2) \quad E(X_n) = \binom{n}{2} W(n).$$

Wir wollen zunächst eine allgemeine Formel für $W(n)$ herleiten. Der Punkt $S = S_{12}$ ist Eckpunkt von Π_n genau dann, wenn keine der Geraden $g_3, \dots, g_n$ die konvexe Hülle B_S von $B \cup S$ trifft. Sei l der Umfang von K , b der von B und l_S der von B_S . Nach der Croftonschen Formel für konvexe Bereiche (W. BLASCHKE [1], § 3, (60))

$$(2.3) \quad \int_{g \cap K \neq \emptyset} dg = l$$

ergibt sich im Falle $S \in K$

$$(2.4) \quad P(g_3 \cap B_S = \emptyset) = \frac{l - l_S}{l - b}.$$

Wir zerlegen $W(n)$ in die beiden Wahrscheinlichkeiten

$$(2.5) \quad W(n) = W_1(n) + W_2(n),$$

$$(2.6) \quad W_1(n) = P(S \text{ Ecke von } \Pi_n, S \in K),$$

$$(2.7) \quad W_2(n) = P(S \text{ Ecke von } \Pi_n, S \notin K).$$

Es gilt

$$(2.8) \quad W_1(n) = \frac{1}{(l-b)^n} \iint_{g_1 \cap g_2 \cap K \neq \emptyset, (g_1 \cup g_2) \cap B = \emptyset} (l - l_S)^{n-2} dg_1 dg_2.$$

Für $W_2(n)$ geben wir eine Abschätzung an, aus der folgen wird, daß $W_2(n)$ gegen-

über $W_1(n)$ zu vernachlässigen ist. Bezeichnet μ das Geradenmaß, so ergibt sich

$$(2.9) \quad W_2(n) = \frac{1}{(l-b)^n} \iint_D f(S)^{n-2} dg_1 dg_2$$

mit $f(S) = \mu(g: g \cap B_S = \emptyset, g \cap K \neq \emptyset)$. Integriert wird über den Bereich D aller Geradenpaare g_1, g_2 mit $g_1 \cap K \neq \emptyset, g_2 \cap K \neq \emptyset, g_1 \cap g_2 \cap K = \emptyset, (g_1 \cup g_2) \cap B = \emptyset$. Um $f(S)$ abzuschätzen, wählen wir einen Randpunkt R von K , der in B_S liegt; dann gilt $B_R \subset B_S$ und folglich

$$(2.10) \quad f(S) \leq f(R) = l - l_R = (l - b) - (l_R - b).$$

Indem wir von B_R durch eine geeignete Stützgerade an den in B_R liegenden Randbogen B ein gleichschenkliges Dreieck abschneiden (Abb. 1), ergibt sich

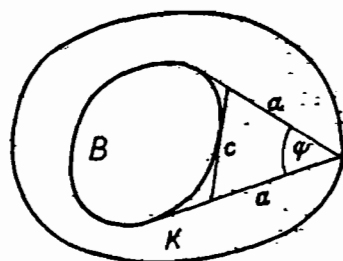


Abb. 1

$$(2.11) \quad l_R - b \geq 2a - c = 2a \left(1 - \sin \frac{\varphi}{2}\right).$$

Bezeichnet r den Abstand der Ränder von B und K , so gilt offenbar $a \geq r > 0$; ferner haben wir, wenn φ der Winkel ist, in dem man B von einem Randpunkt von K aus sieht, $0 \leq \varphi \leq \varphi_0 < \pi$; denn B liegt ganz im Innern von K . Somit gilt

$$(2.12) \quad l - b \geq l_R - b \geq 2r \left(1 - \sin \frac{\varphi_0}{2}\right) = \varepsilon > 0.$$

Aus (2.10) und (2.12) folgt

$$(2.13) \quad \frac{f(S)}{l-b} \leq \frac{l-b-\varepsilon}{l-b} = \gamma \quad \text{mit} \quad 0 < \gamma < 1,$$

wobei γ nur von B und K abhängt. Wir erhalten

$$(2.14) \quad W_2(n) \leq \frac{\gamma^{n-2}}{(l-b)^2} \iint_{\substack{g_1 \cap K \neq \emptyset, g_2 \cap K \neq \emptyset \\ g_1 \cap g_2 \cap K = \emptyset}} dg_1 dg_2.$$

Nach einer Formel von CROFTON (W. BLASCHKE, [1], § 7) ergibt sich für das Integral (2.14)

$$(2.15) \quad \iint dg_1 dg_2 = l^2 - 2\pi F$$

wobei F der Flächeninhalt von K ist. Es folgt

$$(2.16) \quad W_2(n) = O(\gamma^n) \quad \text{mit} \quad 0 < \gamma < 1.$$

Wenn der Bereich B in einem Punkt ausartet, erhält man (2.16) durch eine noch einfachere Abschätzung. Dieselben Überlegungen zeigen allgemein, daß der Anteil der Geradenpaare g_1, g_2 deren Schnittpunkt S außerhalb einer festen konvexen Umgebung U von B liegt, von der Größenordnung $O(\gamma^n)$ ist, wobei γ mit $0 < \gamma < 1$ natürlich von der Umgebung U abhängt.

Satz 1. Sei B ein (möglicherweise ausgearteter) konvexer Bereich und K eine konvexe Umgebung von B . Die Wahrscheinlichkeit dafür, daß eine Ecke von Π_n

außerhalb K liegt, genügt der Beziehung

$$(2.17) \quad P(\text{Ecke von } \Pi_n \notin K) = O(\gamma^n) \quad (0 < \gamma < 1)$$

wobei γ eine von K und B abhängige Konstante ist.

Es bleibt also (2.8) auszuwerten. Hierzu führen wir nach W. BLASCHKE [1], § 6, (89) die Substitution

$$(2.18) \quad dg_1 dg_2 = |\sin(\varphi_1 - \varphi_2)| d\varphi_1 d\varphi_2 dS$$

aus; hierbei sind φ_1, φ_2 die Winkel von g_1 bzw. g_2 mit einer festen Richtung und dS die Dichte des Schnittpunktes $S = g_1 \cap g_2$. Wegen

$$(2.19) \quad \int_0^\alpha \int_0^\alpha |\sin(\varphi_1 - \varphi_2)| d\varphi_1 d\varphi_2 = 2(\alpha - \sin \alpha)$$

erhalten wir, weil über $\varphi_1 \leq \varphi_1, \varphi_2 \leq \varphi_2$ zu integrieren ist,

$$(2.20) \quad W_1(n) = \frac{2}{(l-b)^2} \int_{S \in K \setminus B} \left(1 - \frac{l_S - b}{l-b}\right)^{n-2} (\alpha(S) - \sin \alpha(S)) dS;$$

hierbei ist $\alpha = \varphi_2 - \varphi_1 = \pi - \omega$ und $\omega(S)$ ist der Winkel, unter dem man B von S aus sieht (Abb. 2). Die Auswertung dieses Integrals unter verschiedenen Voraussetzungen über B erfolgt in den §§ 3–5.

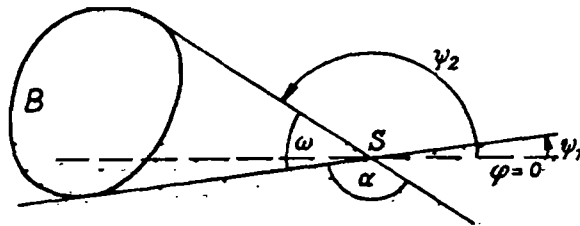


Abb. 2

Zuerst untersuchen wir noch die Wahrscheinlichkeit dafür, daß Π_n nicht geschlossen ist. Es ist ja denkbar, daß das Polygon Π_n auch für größere n nicht den Bereich B umschließt, d.h. nicht beschränkt ist. Das wird besonders dann eintreten, wenn B nur an einer Seite dem Rand von K sehr nahe kommt. Natürlich geht die Wahrscheinlichkeit dafür, daß Π_n nicht geschlossen ist, für $n \rightarrow +\infty$ gegen Null. Wir wollen die Größenordnung dieser Konvergenz abschätzen.

Seien φ_i die Winkel der von B weg gerichteten Normalen von g_i mit einer festen Richtung. Durch ψ_i bezeichnen wir die geordnete Stichprobe der φ_i , d.h. die ψ_i sind gleich den φ_i , der Größe nach geordnet: $0 \leq \psi_1 \leq \psi_2 \leq \dots \leq \psi_n < 2\pi$. Sei $\delta_i = \psi_i - \psi_{i-1}$ ($i = 1, \dots, n$), wobei $\psi_0 = \psi_n - 2\pi$ gesetzt werde. Das Polygon ist genau dann nicht geschlossen, wenn einer der Winkel $\delta_i \geq \pi$ ist. Zunächst haben wir also die Verteilungsfunktion des Winkels φ unter der Bedingung $g \cap K \neq \emptyset, g \cap B = \emptyset$ zu berechnen. Ist $p_0(\varphi)$ die Stützfunktion von B und $p_1(\varphi)$ die von K , so folgt für $0 \leq x \leq 2\pi$

$$(2.21) \quad P(\varphi \leq x) = \frac{1}{l-b} \int_0^x \int_{p_0(\varphi)}^{p_1(\varphi)} dp d\varphi = \frac{1}{l-b} \int_0^x (p_1(\varphi) - p_0(\varphi)) d\varphi.$$

Hieraus ergibt sich: Ist $p_1(\varphi) - p_0(\varphi) = r$ konstant, d.h. K der äußere Parallelbereich im Abstand r von B , so ist φ auf dem Einheitskreis gleichverteilt und es

gilt

$$(2.22) \quad l - b = 2\pi r$$

In diesem Fall ist die Dichte von φ

$$(2.23) \quad f(\varphi) = \frac{p_1(\varphi) - p_0(\varphi)}{l - b}$$

konstant gleich $\frac{1}{2\pi}$; die Wahrscheinlichkeit dafür, daß $\delta_i \geq \pi$ ist, ist gleich der Wahrscheinlichkeit dafür, daß $n-1$ Winkel $\psi_1, \dots, \psi_{i-1}, \psi_{i+1}, \dots, \psi_n$ zwischen ψ_i und $\psi_i + \pi$ liegen, also gleich $2^{-(n-1)}$. Da alle Möglichkeiten $\delta_i \geq \pi$ sich gegenseitig ausschließen und gleich wahrscheinlich sind, ergibt sich (vgl. [3])

$$(2.24) \quad P(\Pi_n \text{ nicht geschlossen}) = \frac{n}{2^{n-1}}$$

(falls K Parallelbereich von B ist).

Im allgemeinen Fall gilt wieder

$$(2.25) \quad P(\Pi_n \text{ nicht geschlossen}) = n \int_0^{2\pi} f(\varphi) \left(\int_{\varphi}^{\varphi+\pi} f(\Theta) d\Theta \right)^{n-1} d\varphi.$$

Nun ist offenbar

$$(2.26) \quad f(\varphi) = \frac{p_1(\varphi) - p_0(\varphi)}{l - b} \geq c > 0$$

also

$$(2.27) \quad \int_{\varphi}^{\varphi+\pi} f(\Theta) d\Theta \leq 1 - \pi c$$

wobei

$$(2.28) \quad \pi c < \int_0^{2\pi} f(\Theta) d\Theta = 1$$

gilt. Aus (2.25) und (2.27) folgt

Satz 2. Ist K ein Parallelbereich von B , so gilt für die Wahrscheinlichkeit, daß Π_n nicht geschlossen ist, die Beziehung (2.24). Ist B enthalten im Innern von K , so ergibt sich für diese Wahrscheinlichkeit im allgemeinen Fall

$$(2.29) \quad P(\Pi_n \text{ nicht geschlossen}) \leq n \gamma^{n-1}$$

wobei γ ($0 < \gamma < 1$) eine von B und K abhängende Konstante ist.

3. Zufällige Polygone um einen Punkt

Sei $B = O \in K$ ein fester Punkt. Dann ist $b = 0$ und $l_S = 2|OS|$ gleich der doppelt zu zählenden Länge der Strecke OS . Aus (2.8) folgt

$$(3.1) \quad W_1(n) = \frac{1}{l^2} \int \int_{g_1 \cap g_2 \cap K \neq \emptyset} \left(1 - \frac{2|OS|}{l} \right)^{n-2} dg_1 dg_2.$$

Die Bedingung $g_i \cap O = \emptyset$ braucht nicht beachtet zu werden, weil die Menge aller Geraden durch einen Punkt das Maß Null hat. Aus (2.20) ergibt sich, weil in unserem Fall $\alpha = \pi$ ist:

$$(3.2) \quad W_1(n) = \frac{2\pi}{l^2} \int_{S \in K} \left(1 - \frac{2|OS|}{l} \right)^{n-2} dS.$$

Sei $0 < r < l/2$, r fest. Dann gilt offenbar

$$(3.3) \quad \frac{2\pi}{l^2} \int_{\substack{S \in K \\ |OS| > r}} \left(1 - \frac{2|OS|}{l}\right)^{n-2} dS = O(\alpha^n), \quad 0 < \alpha < 1,$$

wobei $\alpha = 1 - (2r)/l$ zu setzen ist. Bezeichnet K_r den Kreis vom Radius r um O , $K_r \subset K$, so folgt

$$(3.4) \quad W_1(n) = \frac{2\pi}{l^2} \int_{S \in K_r} \left(1 - \frac{2|OS|}{l}\right)^{n-2} dS + O(\alpha^n)$$

mit $0 < \alpha < 1$. Für Polarkoordinaten ϱ , Θ gilt $dS = \varrho d\varrho d\Theta$ und es ergibt sich durch eine einfache Rechnung

$$(3.5) \quad E(X_n) = \frac{n(n-1)}{2} W(n) = \frac{\pi^2}{2} + O(\gamma^n) \quad \text{mit} \quad 0 < \gamma < 1.$$

Satz 3. Die mathematische Erwartung der Anzahl X_n der Ecken eines zufälligen konvexen Polygons Π_n um einen Punkt O einer konvexen Menge K genügt der Beziehung (3.5).

4. Ringgebiet um einen glatten Bereich

Über B setzen wir nun voraus, daß die Randkurve konvex und genügend oft stetig differenzierbar ist. Unter dieser Voraussetzung ist die Formel (2.20) auszuwerten. Um die Größen $\alpha(S)$ und $l_S - b$ abzuschätzen, wählen wir zunächst geeignete Koordinaten t, s . Auf dem Rand $\mathcal{B}$ von B führen wir die Bogenlänge s als Parameter ein. Wir orientieren $\mathcal{B}$ entgegengesetzt zum Uhrzeigersinn. Sei $x = f(s)$, $y = g(s)$ die Gleichung von $\mathcal{B}$, $t = \{f'(s), g'(s)\}$ der Tangentialvektor und $n = \{g', -f'\}$ der äußere Normalvektor; die Striche bedeuten die Ableitung nach s . Es gilt dann $[n, t] = 1$ für die Determinante von n, t . Die Normalen

$$(4.1) \quad x = f(s) + tg'(s), \quad y = g(s) - tf'(s)$$

bedecken ein Gebiet, welches das Komplement von B in seinem Innern enthält, schlicht, so daß (4.1) eine in diesem Gebiet umkehrbar eindeutige Koordinatentransformation definiert. Die Funktionaldeterminante dieser Transformation ist

$$(4.2) \quad \frac{\partial(x, y)}{\partial(t, s)} = 1 + tk(s) > 0 \quad \text{für} \quad t > -\frac{1}{k(s)};$$

hierbei bezeichnet $k(s) \geq 0$ die Krümmung von $\mathcal{B}$ im Punkte S . Für dS folgt

$$(4.3) \quad dS = (1 + tk(s)) dt ds.$$

Wir betrachten nun einen festen Punkt Y_0 von $\mathcal{B}$, etwa $s_0 = 0$, und ziehen von einem äußeren Punkt S auf der Normalen durch Y_0 die Tangenten an $\mathcal{B}$, die $\mathcal{B}$ in den Punkten $Y(\sigma_\alpha)$, $\alpha = 1, 2$, berühren mögen (Abb. 3). Um Näherungsausdrücke für die Größen σ_α und $\tau_\alpha = |Y_\alpha S|$ als Funktionen von t zu berechnen, stellen wir die Kurve $\mathcal{B}$ in bezug

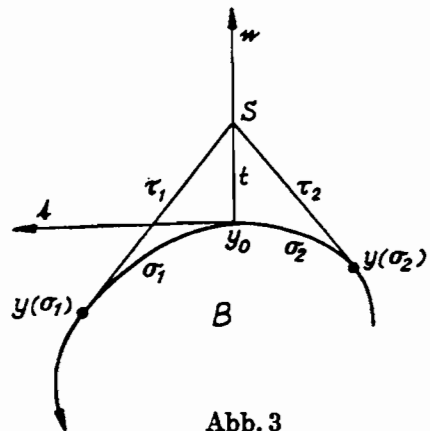


Abb. 3

auf das begleitende Zweibein n, t im Punkte Y_0 dar:

$$(4.4) \quad \begin{aligned} \xi(s) = & t \left(s - \frac{k^2}{3!} s^3 - \frac{3kk'}{4!} s^4 + O(s^5) \right) \\ & - n \left(\frac{k}{2!} s^2 + \frac{k'}{3!} s^3 + (k'' - k^3) \frac{s^4}{4!} + O(s^5) \right). \end{aligned}$$

Für den Schnittpunkt S der Tangente an $\mathcal{B}$ im Punkte $Y(\sigma_\alpha)$ mit der Normale durch Y_0 haben wir die Beziehung

$$(4.5) \quad \xi(\sigma) + \tau \xi'(\sigma) = t n$$

auszuwerten. Setzen wir für τ eine Entwicklung

$$(4.6) \quad \tau = A\sigma + B\sigma^2 + C\sigma^3 + D\sigma^4 + O(\sigma^5)$$

an und gehen damit in (4.5) ein, so erhalten wir nach Zerlegung in die Komponenten bezüglich t, n zwei skalare Gleichungen. Aus der t -Komponente folgt

$$(4.7) \quad \tau = -\sigma - \frac{k^2}{3} \sigma^3 - \frac{3}{8} k k' \sigma^4 + O(\sigma^5).$$

Durch Koeffizientenvergleich der n -Komponente erhält man unter Berücksichtigung von (4.7):

$$(4.8) \quad t = \frac{k}{2} \sigma^2 + \frac{k'}{3} \sigma^3 + (3k'' + 5k^3) \frac{\sigma^4}{4!} + O(\sigma^5).$$

Setzen wir nun $t = u^2$, so ergibt sich für einen zu (4.6) analogen Ansatz von $\sigma = \sigma(u)$ aus (4.8):

$$(4.9) \quad \sigma_{1,2}(u) = \pm \sqrt{\frac{2}{k}} u - \frac{2k'}{3k^2} u^2 \pm \frac{1}{3} \sqrt{\frac{k}{2}} \left(\frac{10}{3} \frac{k'^2}{k^4} - \frac{3}{2} \frac{k''}{k^3} - \frac{5}{2} \right) u^3 + O(u^4).$$

Diese Entwicklung macht die Voraussetzung $k > 0$ für $\mathcal{B}$ notwendig; der Rand von B darf also keinen Streckpunkt und erst recht keine Strecke enthalten. Die beiden Vorzeichen entsprechen den zwei Tangenten von S an $\mathcal{B}$. Nun können wir das Integral (2.20) unter Berücksichtigung von (4.3) auswerten. Unter Beachtung der Vorzeichen für die berechneten Längen (Abb. 3) gilt nach (4.7)

$$(4.10) \quad l_S - b = (\tau_2 + \sigma_2) - (\tau_1 + \sigma_1) = \frac{k^2}{3} (\sigma_1^3 - \sigma_2^3) + \frac{3}{8} k k' (\sigma_1^4 - \sigma_2^4) + O(\sigma^5).$$

Wegen (4.9) erhalten wir

$$(4.11) \quad l_S - b = \frac{4}{3} \sqrt{2k} u^3 + O(u^5).$$

Für $\alpha - \sin \alpha$ ergibt sich wegen

$$(4.12) \quad \alpha(s, t) = \int_{\sigma_1}^{\sigma_2} k(\sigma) d\sigma$$

unter Beachtung von (4.9)

$$(4.13) \quad \alpha - \sin \alpha = \frac{1}{3!} (2\sqrt{2k} u)^3 + O(u^4).$$

Das abzuschätzende Integral (2.20) wird wegen $u = t^{1/2}$ nach Einsetzen der gewonnenen Ausdrücke (4.3), (4.11), (4.13) zu

$$W_1(n) = \frac{2}{(l-b)^2} \int_0^b \int_0^{h(s)} \left(1 - \frac{4\sqrt{2k} t^{3/2}}{3(l-b)} + O(t^{5/2}) \right)^{n-2} \left(\frac{8}{3!} (\sqrt{2kt})^3 + O(t^2) \right) (1+tk) dt ds.$$

Substituieren wir nun

$$(4.14) \quad t = \left(\frac{3(l-b)}{4\sqrt{2k}} \frac{x}{n} \right)^{2/3},$$

so ergibt sich nach einigen Umformungen

$$(4.15) \quad W_1(n) = 2 \left(\frac{2}{3(l-b)} \right)^{1/3} \int_0^b k^{2/3} \int_0^\infty \left(1 - \frac{x}{n} \right)^n \frac{x^{2/3}}{n^{5/3}} dx ds + O\left(\frac{1}{n^2}\right).$$

Hieraus folgt

Satz 4. Sei B ein konvexer beschränkter Bereich mit glattem Rand, dessen Krümmung $k = k(s)$ positiv und beschränkt ist. B liege im Innern der konvexen Menge K ; l und b seien der Umfang von K bzw. B . Für die mathematische Erwartung der Eckenzahl X_n eines zufälligen konvexen Polygons Π_n um B gilt dann

$$(4.16) \quad E(X_n) = \left[\left(\frac{2}{3(l-b)} \right)^{1/3} \Gamma\left(\frac{5}{3}\right) \int_0^b k^{2/3} ds \right] n^{1/3} + O(1).$$

Die Größenordnung der Eckenzahl ist also dieselbe wie im Fall der konvexen Hülle von n zufällig im Bereich B gewählten Punkten (vgl. A. RÉNYI, R. SULANKE [2]), die Faktoren unterscheiden sich jedoch wesentlich.

5. Ringgebiet um ein konvexes Polygon

Sei nun B ein konvexes r -Eck. Nach Satz 1 liegt das zufällige Polygon Π_n mit großer Wahrscheinlichkeit in einer beliebigen, festen, konvexen Umgebung U von B ; U sei so gewählt, daß alle Schnittpunkte nicht aneinandergrenzender Seiten von B außerhalb U liegen. Das Ringgebiet $U \setminus B$, für das jetzt das Integral (2.20) auszuwerten ist, wird durch die Seiten von B in r Eckgebiete E_i und in r Seitengebiete T_i zerlegt (Abb. 4), in denen wir die Integration einzeln ausführen.

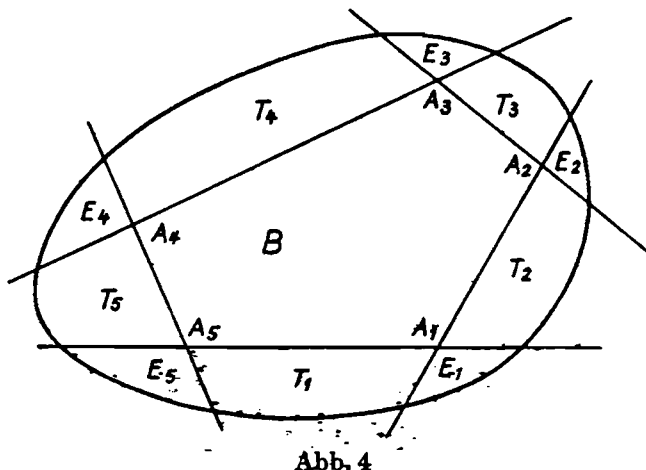


Abb. 4

Sei T eines der Seitengebiete mit den Ecken A, A' an einer Seite der Länge $2c = |AA'|$. Für $S \in T$ gilt

$$(5.1) \quad l_S - b = |SA| + |SA'| - |AA'| = 2(a - c),$$

wobei a die große Halbachse der Ellipse mit den Brennpunkten A, A' durch den

Punkt S ist. Als Koordinaten von S wählen wir a und den Abstand x der Projektion von S auf die große Achse der Ellipse von ihrem Zentrum. Für das Flächenelement dS erhalten wir in diesen Koordinaten

$$(5.2) \quad dS = \frac{a^4 - c^2 x^2}{a^2 \sqrt{(a^2 - c^2)(a^2 - x^2)}} dx da.$$

Für den in (2.20) eingehenden Winkel α , den Außenwinkel des Dreiecks $AA'S$ in S , berechnet man

$$(5.3) \quad \sin \alpha = \frac{2ac \sqrt{(a^2 - c^2)(a^2 - x^2)}}{a^4 - c^2 x^2} = f(x, a).$$

Wir ersetzen nun das Gebiet T durch einen an AA' grenzenden Abschnitt des Halbkreises über der Seite AA' , der in U liegt und in dem $\alpha \leq \pi/2$ gilt; den hierbei entstehenden Fehler schätzen wir später ab. Der Halbkreis wird bestimmt durch $f = 1$; für x, a erhalten wir den Integrationsbereich

$$(5.4) \quad c \leq a \leq \delta c, \quad |x| \leq \frac{a}{c} \sqrt{2c^2 - a^2},$$

hierbei ist δ ($1 < \delta \leq \sqrt{2}$) eine Zahl, die so gewählt wird, daß der Kreisabschnitt in U liegt. Nach (2.20) ist also zunächst das Integral

$$(5.5) \quad W = \frac{8c}{(l-b)^2} \int_c^{\delta c(a/c)} \int_0^{\frac{a}{c} \sqrt{2c^2 - a^2}} \left(1 - \frac{2(a-c)}{l-b}\right)^{n-2} \left(\frac{\arcsin f - f}{af}\right) dx da$$

zu berechnen. Hierzu entwickeln wir das innere Integral

$$(5.6) \quad F(a) = \int_0^{\frac{a}{c} \sqrt{2c^2 - a^2}} \frac{1}{f} (\arcsin f - f) dx$$

nach Potenzen von $a - c$ und setzen

$$(5.7) \quad \frac{1}{f} (\arcsin f - f) = \frac{1}{6} f^2 + R.$$

Das Integral über den ersten Bestandteil ergibt

$$(5.8) \quad \frac{1}{6} \int_0^{\frac{a}{c} \sqrt{2c^2 - a^2}} f^2 dx = -\frac{a^4 - c^4}{6a^2 c} \log(a - c) + O(a - c).$$

Für den Rest R zeigen wir

$$(5.9) \quad \int_0^{\frac{a}{c} \sqrt{2c^2 - a^2}} R dx = O(a - c).$$

Es gilt ja, wenn

$$\arcsin \xi = \sum_{v=0}^{\infty} c_v \xi^{2v+1}$$

gesetzt wird,

$$(5.10) \quad 0 < R = \sum_{v=2}^{\infty} c_v f^{2v} \leq f^4 \sum_{v=2}^{\infty} c_v = f^4 \left(\frac{\pi}{2} - \frac{7}{6}\right).$$

Daher genügt es

$$\int_0^{\frac{a}{c} \sqrt{2c^2 - a^2}} f^4 dx = O(a - c)$$

also

$$(5.11) \quad \int_0^{(a/c)\sqrt{2c^2-a^2}} \frac{(a^2-x^2)^2}{(a^4-c^2x^2)^4} dx = O\left(\frac{1}{a-c}\right)$$

zu beweisen. Nun gilt wegen $0 \leq x \leq c \leq a$

$$(5.12) \quad \frac{(a-x)^2}{16a^6(a^2-cx)^4} \leq \frac{(a^2-x^2)^2}{(a^4-c^2x^2)^4} \leq \frac{4(a-x)^2}{a^6(a^2-cx)^4}.$$

Daher ist noch

$$(5.13) \quad \int_0^{(a/c)\sqrt{2c^2-a^2}} \frac{(a-x)^2}{(a^2-cx)^4} dx = O\left(\frac{1}{a-c}\right)$$

zu zeigen. Diese Beziehung erhält man leicht durch die Substitution $a^2 - cx = t$ und einige einfache Abschätzungen. Aus (5.6)–(5.9) ergibt sich

$$(5.14) \quad F(a) = -\frac{a^4 - c^4}{8a^2c} \log(a-c) + O(a-c).$$

Nach (5.5) gilt also

$$(5.15) \quad W = \frac{-4}{3(l-b)^2} \int_c^{\delta c} \left(1 - \frac{2(a-c)}{(l-b)}\right)^{n-2} \left(\frac{a^4 - c^4}{a^3} \log(a-c) + O(a-c)\right) da.$$

Durch die Substitution

$$\frac{2(a-c)}{l-b} = \frac{Z}{n-2}$$

ergibt sich nach einigen einfachen Rechnungen wegen

$$(5.16) \quad \int_c^{\delta c} \left(1 - \frac{2(a-c)}{(l-b)}\right)^{n-2} \cdot O(a-c) da = O\left(\frac{1}{n^2}\right)$$

die Beziehung

$$(5.17) \quad W = \frac{4}{3n(n-1)} \log(n-2) + O\left(\frac{1}{n^2}\right).$$

Bei der Ersetzung des Seitengebietes T durch einen Halbkreisabschnitt haben wir entweder über ein von der Geraden der benachbarten Seite und einen Kreis-

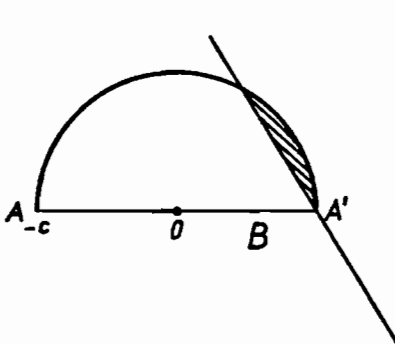


Abb. 5 a

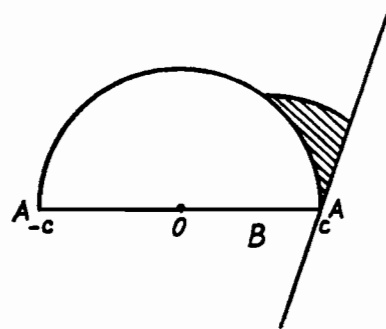


Abb. 5 b

bogen begrenztes Gebiet zuviel (Abb. 5 a) oder zuwenig (Abb. 5 b) integriert. Wir zeigen, daß die hierdurch entstehenden Fehler von der Größenordnung

$O(1/n^2)$ sind. Sei

$$(5.18) \quad x(a) = c + (a - c) \gamma + O((a - c)^2)$$

eine Darstellung der benachbarten Seite. Der Fehler im ersten Fall (Abb. 5a) ist dann

$$(5.19) \quad \Delta = q \int_c^{ac} \left(1 - \frac{2(a-c)}{(l-b)}\right)^{n-2} \frac{1}{a^2 \sqrt{a^2 - c^2}} \int_{x(a)}^{(a/c) \sqrt{2c^2 - a^2}} (\alpha - \sin \alpha) \frac{a^4 - c^2 x^2}{\sqrt{a^2 - x^2}} dx da;$$

hierbei bezeichnet q eine Konstante. Wegen (5.16) genügt es zu zeigen, daß

$$(5.20) \quad I(a) = \int_{x(a)}^{(a/c) \sqrt{2c^2 - a^2}} (\alpha - \sin \alpha) \frac{a^4 - c^2 x^2}{\sqrt{a^2 - x^2}} dx = O((a - c)^{3/2})$$

gilt. Nun ist $\alpha - \sin \alpha$ beschränkt, so daß es genügt,

$$(5.21) \quad \int_{x(a)}^{(a/c) \sqrt{2c^2 - a^2}} \frac{a^4 - c^2 x^2}{\sqrt{a^2 - x^2}} dx = O((a - c)^{3/2})$$

zu beweisen. Für das unbestimmte Integral

$$(5.22) \quad Q(x) = \int \frac{a^4 - c^2 x^2}{\sqrt{a^2 - x^2}} dx = \frac{c^2 x}{2} \sqrt{a^2 - x^2} - a^2 \left(a^2 - \frac{c^2}{2}\right) \arccos \frac{x}{a}$$

erhalten wir wegen $\arccos \frac{x}{a} = \arcsin \frac{1}{a} \sqrt{a^2 - x^2}$ die Entwicklung

$$(5.23) \quad Q(x) = \frac{1}{2} \sqrt{a^2 - x^2} (c^2 x - a^3 + a(c^2 - a^2) + O(a^2 - x^2)).$$

Durch Einsetzen der unteren Grenze $x = x(a)$ nach (5.18) ergibt sich sofort

$$(5.24) \quad Q(x(a)) = O((a - c)^{3/2})$$

Das gleiche gilt aber auch für die obere Grenze, weil der hier einzusetzende Ausdruck ebenfalls die Gestalt (5.18), natürlich mit einer anderen Konstanten γ , besitzt. Somit gilt (5.21). Ganz analog schätzt man auch den zweiten Fehler (Abb. 5b) ab. Somit können wir in (5.17) den Halbkreisabschnitt durch das Seitengebiet T ersetzen und erhalten insgesamt

$$(5.25) \quad W(T) = \frac{4}{3n(n-1)} \log n + O\left(\frac{1}{n^2}\right).$$

Diese Formel gilt auch, wenn B in eine Strecke ausartet.

Nun betrachten wir das Eckgebiet $E = E_t$ bei der Ecke A_t von B . Wir führen wie bei (5.2) wieder halbelliptische Koordinaten ein; nur ist die Basis jetzt die Strecke $A_{t-1}A_{t+1}$, deren Länge wieder durch $2c$ bezeichnet werde. Mit

$$d = \frac{1}{2} (|A_{t-1}A_t| + |A_tA_{t+1}|)$$

ergibt sich für die Abstandsdifferenz

$$(5.26) \quad l_S - b = 2(a - d).$$

Daher gilt nach (2.20) und (5.2) für die entsprechende Wahrscheinlichkeit

$$(5.27) \quad W(E) = \frac{2}{(l-b)^2} \int_d^{a_0} \left(1 - \frac{2(a-d)}{(l-b)}\right)^{n-2} \int_{x_1(a)}^{x_2(a)} (\alpha - \sin \alpha) \frac{a^4 - c^2 x^2}{a^2 \sqrt{a^2 - c^2} (a^2 - x^2)} dx da.$$

Hier bezeichnen $x_1(a)$, $x_2(a)$ die x -Koordinaten der Schnittpunkte der zu a gehörenden Ellipse mit den Verlängerungen der an A_i anstoßenden Seiten über A_i hinaus. Da wir nur eine genügend kleine Umgebung von B betrachten, gilt

$$|x| \leq \max(|x_1(a)|, |x_2(a)|) < a, \quad c < d \leq a.$$

Aus dem Mittelwertsatz folgt wegen der Beschränktheit und Stetigkeit des Integranden

$$(5.28) \quad \int_{x_1(a)}^{x_2(a)} (\alpha - \sin \alpha) \frac{a^4 - c^2 x^2}{a^2 \sqrt{a^2 - c^2} (a^2 - x^2)} dx = M(a) (x_2(a) - x_1(a)),$$

wobei $M(a)$ für alle a aus dem betrachteten Bereich beschränkt bleibt: $|M(a)| \leq M_0$. Für $a = d$ gilt $x_1(d) = x_2(d)$. Die Funktionen $x_i(a)$ sind an der Stelle d genügend oft stetig differenzierbar. Es folgt

$$(5.29) \quad x_2(a) - x_1(a) = h_0(a - d) + O((a - d)^2),$$

wobei h_0 eine gewisse Konstante ist. Setzt man (5.28), (5.29) in (5.27) ein, so folgt nach (5.16) unmittelbar

$$(5.30) \quad W(E) = O\left(\frac{1}{n^2}\right).$$

Wegen Satz 1, (5.25) und (5.30) erhalten wir den folgenden

Satz 5. Sei B ein im Innern von K liegendes konvexes r -Eck, $r \geq 2$. Für die mathematische Erwartung der Eckpunktzahl X_n des zufälligen Polygons Π_n gilt

$$E(X_n) = \frac{2r}{3} \log n + O(1).$$

Das Hauptglied dieser Formel stimmt mit dem entsprechenden Hauptglied aus Satz 1 unserer Arbeit [2] über die konvexe Hülle von in einem Polygon liegenden zufälligen Punkten überein.

Literatur

1. BLASCHKE, W.: Vorlesungen über Integralgeometrie. 3. Aufl. Berlin: VEB Deutscher Verlag der Wissenschaften 1955.
2. RÉNYI, A., u. R. SULANKE: Über die konvexe Hülle von n zufällig gewählten Punkten. Z. Wahrscheinlichkeitstheorie verw. Geb. 2, 75–84 (1963).
3. STEVENS, W. L.: Solution to a geometrical problem in probability. Ann. Eugenics 9, 315–320 (1939).

ON QUADRATIC INEQUALITIES IN PROBABILITY THEORY

by

J. GALAMBOS and A. RÉNYI

Summary

In this paper quadratic inequalities in the probabilities of Boolean functions of n variable events are considered. For a special class of such inequalities — called exact inequalities — a necessary and sufficient condition is given; this general theorem is applied to deduce certain special inequalities. Generalization to inequalities of degree higher than 2 is also considered.

§ 0. Notations

Let $S=(\Omega, \mathcal{A}, P)$ denote a probability space, i.e. let Ω be an arbitrary non-empty set, $\mathcal{A}$ a σ -algebra¹ of subsets of Ω and P a measure on $\mathcal{A}$ such that $P(\Omega)=1$. We call the elements of $\mathcal{A}$ events and denote them by capital letters. We denote by $A+B$ the union and by AB the intersection of the sets A and B , and by $\bar{A}$ the complement of the set A with respect to Ω . As usual, $\bar{A}$ is interpreted as the event consisting in the non-occurrence of the event A , while $A+B$ and AB respectively, are interpreted as the event that at least one of the events A, B occurs, resp. that both the events A, B occur.

Let $p_1, p_2, \dots, p_r$ be any set of positive numbers such that

$$\sum_{j=1}^r p_j = 1$$

We shall denote by $S_r(p_1, \dots, p_r)$ that (finite) probability space in which the set Ω consists of r elements $\omega_1, \omega_2, \dots, \omega_r$. $\mathcal{A}$ is the set of all 2^r subsets of Ω , and P is defined by

$$(0.1) \quad P(A) = \sum_{\omega_j \in A} p_j$$

Especially $S_1(1)$ is the trivial probability space which contains only two events: the "certain event" Ω and the "impossible event" $\emptyset$ (the empty set). Further $S_2(\frac{1}{2}, \frac{1}{2})$ is the probability space (describing e.g. the throw of a fair coin) which contains only four events: $\Omega, \emptyset, \alpha = \{\omega_1\}$ and $\beta = \{\omega_2\}$ and $P(\alpha) = P(\beta) = \frac{1}{2}$.

A Boolean function $F = F(A_1, A_2, \dots, A_n)$ of n variable events $A_1, \dots, A_n$ is a function of these events which can be expressed by means of the variables

¹ All results of this paper are valid also if $\mathcal{A}$ is only an algebra of subsets of Ω and P a finitely additive nonnegative set function on $\mathcal{A}$ for which $P(\Omega)=1$.

$A_1, \dots, A_n$ and a finite number of Boolean operations, i.e. the operations $A+B$, AB , $\bar{A}$. We introduce the notation

$$A^1 = A, \quad A^{-1} = \bar{A}.$$

Let us denote by $\delta_k(m)$ the k -th digit of the binary representation of the non-negative integer m , i.e. we put

$$(0.2) \quad m = \sum_{k \geq 0} \delta_k(m) 2^k$$

Let us put further

$$(0.3) \quad \varepsilon_k(m) = 2\delta_{k-1}(m) - 1 \quad (k=1, 2, \dots).$$

Clearly $\varepsilon_k(m) = \pm 1$, and if m runs over the integers $0, 1, \dots, 2^n - 1$, the n -tuple $\{\varepsilon_1(m), \dots, \varepsilon_n(m)\}$ runs over all 2^n possible n -tuples of the signs $+1$ and -1 .

Let us put

$$(0.4) \quad B_n(m) = A_1^{\varepsilon_1(m)} A_2^{\varepsilon_2(m)} \dots A_n^{\varepsilon_n(m)} \quad (0 \leq m \leq 2^n - 1)$$

We call the $B_n(m)$ the basic Boolean functions of the variables $A_1, \dots, A_n$. Clearly

$$(0.5) \quad B_n(m_1) B_n(m_2) = 0 \quad \text{if} \quad m_1 \neq m_2$$

and

$$(0.6) \quad \sum_{m=0}^{2^n-1} B_n(m) = \Omega$$

It is well known that every Boolean function $F(A_1, \dots, A_n)$ can be uniquely represented in a „canonical form” as the sum of certain basic functions $B_n(m)$; thus there are only 2^{2^n} different Boolean functions of n variable events.

§ 1. Introduction

Some time ago, the second named author has proved ([1], see also [2]) the following

THEOREM 1. *Let $F_j = F_j(A_1, A_2, \dots, A_n)$ ($j=1, 2, \dots, N$) be arbitrary Boolean functions of the n variable events $A_1, \dots, A_n$. The linear inequality*

$$(1.1) \quad \sum_{j=1}^N c_j P(F_j) \geq 0$$

(where $c_1, \dots, c_N$ are real constants) is valid in every probability space S if it is valid in the trivial probability space $S_1(1)$.

This simple theorem is useful because it makes it possible to reduce the proof of any linear inequality among probabilities of Boolean functions to a corresponding combinatorial inequality.

To make this paper self-contained we reproduce here the proof of Theorem 1, especially as the proof is very short.

PROOF OF THEOREM 1. Let the expression of the functions $F_1, \dots, F_N$ in canonical form be

$$(1.2) \quad F_j = \sum_{m \in E_j} B_n(m) \quad (j=1, 2, \dots, N)$$

where E_j is some subset of the set $\{0, 1, \dots, 2^n - 1\}$. It follows from (0.5) that

$$(1.3) \quad P(F_j) = \sum_{m \in E_j} P(B_n(m))$$

and thus

$$(1.4) \quad \sum_{j=1}^N c_j P(F_j) = \sum_{m=0}^{2^n-1} d_m P(B_n(m))$$

where

$$(1.5) \quad d_m = \sum_{m \in E_j} c_j$$

Now evidently if $A_k = \Omega$ if $\varepsilon_k(m) = 1$ and $A_k = \emptyset$ if $\varepsilon_k(m) = -1$, then $B_n(m) = \Omega$ and $B_n(l) = \emptyset$ for $l \neq m$, $0 \leq l \leq 2^n - 1$, thus for this special choice of the values of the variables $A_1, \dots, A_n$ we have

$$(1.6) \quad \sum_{j=1}^N c_j P(F_j) = d_m$$

Thus if (1.1) holds on $S_1(1)$ we have $d_m \geq 0$ for $m = 0, 1, \dots, 2^n - 1$ and thus it follows from (1.4) that (1.1) holds for every choice of the values of the events $A_1, \dots, A_n$ in every probability space S . Thus Theorem 1 is proved.

It is evident that Theorem 1 can be used also to prove identities. To prove that a relation

$$(1.7) \quad \sum_{j=1}^N c_j P(F_j) = 0$$

is valid, according to Theorem 1 it is sufficient to verify that (1.7) holds if all A_k are equal either to Ω or to $\emptyset$.

A typical example of an inequality which can be obtained as a special case of Theorem 1 is the following inequality, due to GUMBEL ([3]): Putting

$$(1.8) \quad \sigma_k^{(n)} = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} P(A_{i_1} A_{i_2} \dots A_{i_k}) \quad (k = 1, 2, \dots, n)$$

one has for $2 \leq k \leq n$

$$(1.9) \quad (n - k + 1) \sigma_{k-1}^{(n)} \leq \binom{n}{k} + (k - 1) \sigma_k^{(n)}.$$

By means of Theorem 1 the proof of (1.9) is reduced to a simple inequality between binomial coefficients (see [2], p. 30).

The aim of this paper is to prove a theorem similar to Theorem 1 for *quadratic* (instead of linear) inequalities. This will be done in § 2. In § 3 we give some applications of the general theorem of § 2. In § 4 we discuss the possibility of generalizing the result of § 2 to polynomial inequalities of the third and still higher degrees.

§ 2. A General Theorem on Quadratic Inequalities

In this § we consider quadratic inequalities of the form

$$(2.1) \quad \sum_{i=1}^N \sum_{j=1}^N c_{i,j} P(F_i) P(F_j) \geq 0$$

where the $c_{i,j}$ are real constants, and $F_1, F_2, \dots, F_N$ are Boolean functions of the variable events $A_1, \dots, A_n$.

Note that it is no restriction that in (2.1) no linear terms occur, because one of the F_i may be equal to Ω (which is also a Boolean function, namely a constant function) and thus inequalities which contain both quadratic and linear terms can be also written in the form (2.1).

We shall call an inequality (2.1) *exact*, if in (2.1) the equality sign is valid every time when each A_k is equal either to Ω or to $\emptyset$. By other words (2.1) is exact if equality is valid in (2.1) when the variables $A_1, \dots, A_n$ are restricted to events in the trivial probability space $S_1(1)$.

We shall prove now the following

THEOREM 2. *Let (2.1) be an exact inequality. In order that (2.1) should be valid on every probability space S it is sufficient (and of course also necessary) that it should be valid on the probability space $S_2(\frac{1}{2}, \frac{1}{2})$.*

PROOF OF THEOREM 2. Let again (1.2) be the expression of the function $F_j (1 \leq j \leq N)$ in canonical form. In view of (1.3) we get

$$(2.2) \quad \sum_{i=1}^N \sum_{j=1}^N c_{i,j} P(F_i) P(F_j) = \sum_{r=0}^{2^n-1} \sum_{s=0}^{2^n-1} d_{r,s} P(B_n(r)) P(B_n(s)),$$

where

$$(2.3) \quad d_{r,s} = \sum_{\substack{r \in E_i \\ s \in E_j}} c_{i,j}$$

Now let us choose $A_k = \Omega$ if $\varepsilon_k(r) = 1$ and $A_k = \emptyset$ if $\varepsilon_k(r) = -1$ ($k = 1, 2, \dots, n$).

It follows that $P(B_n(r)) = 1$ and $P(B_n(s)) = 0$ if $s \neq r$; thus for this special choice of the values of the variables $A_1, \dots, A_n$ we have

$$(2.4) \quad \sum_{i=1}^N \sum_{j=1}^N c_{i,j} P(F_i) P(F_j) = d_{r,r}$$

As we have supposed that the inequality (2.1) is exact, it follows that

$$(2.5) \quad d_{r,r} = 0 \quad \text{for} \quad 0 \leq r \leq 2^n - 1.$$

Putting

$$(2.6) \quad D_{r,s} = d_{r,s} + d_{s,r} \quad \text{for} \quad r \neq s$$

we obtain

$$(2.7) \quad \sum_{i=1}^N \sum_{j=1}^N c_{i,j} P(F_i) P(F_j) = \sum_{0 \leq r < s \leq 2^n - 1} D_{r,s} P(B_n(r)) P(B_n(s))$$

Now let us choose an arbitrary pair (r, s) of integers, $0 \leq r < s \leq 2^n - 1$, and let us choose the values of the events A_k as follows:

$$(2.8) \quad \begin{aligned} A_k &= \Omega & \text{if } \varepsilon_k(r) = \varepsilon_k(s) = 1 \\ A_k &= \alpha & \text{if } \varepsilon_k(r) = 1 \text{ and } \varepsilon_k(s) = -1 \\ A_k &= \beta & \text{if } \varepsilon_k(r) = -1 \text{ and } \varepsilon_k(s) = +1 \\ A_k &= \emptyset & \text{if } \varepsilon_k(r) = \varepsilon_k(s) = -1 \end{aligned}$$

where α and β are the events $\alpha = \{\omega_1\}$, $\beta = \{\omega_2\}$ of the probability space $S_2(\frac{1}{2}, \frac{1}{2})$. For this special choice of the values of the variables A_k we have clearly

$$(2.9) \quad B_n(r) = \alpha, B_n(s) = \beta \text{ and } B_n(t) = \emptyset \text{ for } t \neq r, t \neq s.$$

Thus we obtain for this choice of the values of the A_k

$$(2.10) \quad P(B_n(r)) = P(B_n(s)) = \frac{1}{2}, \quad P(B_n(t)) = 0 \text{ for } t \neq r, t \neq s,$$

and therefore

$$(2.11) \quad \sum_{i=1}^N \sum_{j=1}^N c_{i,j} P(F_i) P(F_j) = \frac{1}{4} D_{r,s}$$

Thus if (2.1) is valid on $S_2(\frac{1}{2}, \frac{1}{2})$, then we must have $D_{r,s} \geq 0$ for all pairs (r, s) and thus in view of (2.7) it follows that (2.1) is valid on every probability space S and for every choice of the value of the variables A_k .

Thus Theorem 2 is proved.

Similarly as Theorem 1, Theorem 2 can be used also to prove identities. As a matter of fact we obtain from Theorem 2 the following

COROLLARY. *If*

$$(2.12) \quad \sum_{i=1}^N \sum_{j=1}^N c_{i,j} P(F_i) P(F_j) = 0$$

holds on $S_1(1)$ and on $S_2(\frac{1}{2}, \frac{1}{2})$, then it holds identically on every probability space.

§ 3. Some Applications of the General Theorem of § 2

In this § we consider some examples of quadratic inequalities which can be easily proved by means of Theorem 2.

EXAMPLE 1. Let us put $\sigma_0^{(n)} = 1$ and

$$(3.1) \quad \sigma_k^{(n)} = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} P(A_{i_1} A_{i_2} \dots A_{i_k})$$

We shall prove that the inequality

$$(3.2) \quad k \sigma_k^{(n)} \geq \sigma_{k-1}^{(n)} (\sigma_1^{(n)} - k + 1) \quad (k = 1, 2, \dots, n)$$

is valid.

To prove (3.2) we first remark that it is a quadratic inequality of type (2.1). Further it is easy to see that (3.2) is an exact inequality. As a matter of fact if l among the events $A_1, \dots, A_n$ are equal to Ω and the other $n-l$ to $\emptyset$, then three cases are possible:

a) either $l \leq k-2$, in which case $\sigma_k^{(n)} = \sigma_{k-1}^{(n)} = 0$ and thus both sides of (3.2) are equal to 0,

b) or $l = k-1$ in which case $\sigma_k^{(n)} = 0$ and $\sigma_1^{(n)} - k + 1 = 0$ and thus again both sides of (3.2) are equal to 0,

c) or $l \geq k$, in which case $\sigma_k^{(n)} = \binom{l}{k}$, $\sigma_{k-1}^{(n)} = \binom{l}{k-1}$ and $\sigma_1^{(n)} = l$. As however

$$k \binom{l}{k} = \binom{l}{k-1} (l - k + 1)$$

we have equality in (3.2) in this case too. Thus (3.2) is exact. Now let us check that (3.2) holds for $S_2(\frac{1}{2}, \frac{1}{2})$. Suppose that among the events $A_1, \dots, A_n$ l_1 are equal to Ω , l_2 to α , l_3 to β ($l_1 + l_2 + l_3 \leq n$) and the remaining $n - l_1 - l_2 - l_3$ to $\emptyset$. In this case

$$\sigma_j^{(n)} = \frac{1}{2} \left[\binom{l_1 + l_2}{j} + \binom{l_1 + l_3}{j} \right] \quad \text{for } 1 \leq j \leq n$$

and thus

$$(3.3) \quad k\sigma_k^{(n)} - \sigma_{k-1}^{(n)}(\sigma_1^{(n)} - k + 1) = \frac{1}{4}(l_2 - l_3) \left[\binom{l_1 + l_2}{k-1} - \binom{l_1 + l_3}{k-1} \right] \geq 0$$

Thus by Theorem 2 (3.2) holds on every probability space S for any choice of the events $A_1, \dots, A_n$.

It is interesting to compare (3.2) with GUMBEL's inequality (1.9). The fact that (3.2) is exact, while in GUMBEL's inequality we have equality (as seen from the proof) on $S_1(1)$ only if $l=n$ or $l=n-1$, shows that, (3.2) gives sometimes a better estimate than (1.9). Another such instance is when the events all have probability $\frac{1}{2}$, and $k=2$. In this case (1.9) gives for $\sigma_2^{(n)}$ only the trivial lower estimate 0, while (3.2) gives the non-trivial (in fact, asymptotically best possible) lower estimate $\sigma_2^{(n)} \geq \frac{n(n-2)}{8}$.

For $k=2$ we obtain as a special case of (3.2) the well known inequality

$$(3.4) \quad \sigma_2^{(n)} \geq \binom{\sigma_1^{(n)}}{2}.$$

It follows from (3.2) by induction that

$$(3.5) \quad \sigma_k^{(n)} \geq \binom{\sigma_1^{(n)}}{k}.$$

It should be noted that one can deduce from (3.4) the following inequality:

$$\text{If } \sigma_2^{(n)} \geq \binom{n}{2} p^2 \quad \text{then} \quad \sigma_1^{(n)} \leq np + \frac{1}{2}(1-p) + \frac{1-p^2}{4p(2n-1)}$$

As a matter of fact, it follows from (3.4) and the inequality $\sqrt{1+x} \leq 1 + \frac{x}{2}$ that

$$\sigma_1^{(n)} \leq \frac{1 + \sqrt{1 + 8\sigma_2^{(n)}}}{2} \leq \frac{1}{2} + \frac{1}{2}(2np - p) \sqrt{1 + \frac{1-p^2}{(2np-p)^2}}$$

and thus that

$$\sigma_1^{(n)} \leq np + \frac{1-p}{2} + \frac{1-p^2}{4p(2n-1)}$$

REMARK. The exact maximum of $\sigma_1^{(n)}$ under condition $\sigma_2^{(n)} \leq \binom{n}{p} p^2$ was determined in [4].

EXAMPLE 2. Let us consider the quadratic relation

$$(3.6) \quad P^2(A+B) + P^2(\bar{A}\bar{B}) = P^2(A) + P^2(B) + 2P(A\bar{B})P(\bar{A}B)$$

It is evidently valid on $S_1(1)$ and also on $S_2(\frac{1}{2}, \frac{1}{2})$, thus it holds identically.

§ 4. Cubic Inequalities

Theorem 2 can be generalized for cubic inequalities

$$(4.1) \quad \sum_{i_1=1}^N \sum_{i_2=1}^N \sum_{i_3=1}^N c_{i_1, i_2, i_3} P(F_{i_1}) P(F_{i_2}) P(F_{i_3}) \geq 0$$

where $F_1, \dots, F_N$ are Boolean functions of the variable events $A_1, \dots, A_n$. The inequality (4.1) is called *exact of order 2* if for every p ($0 \leq p \leq 1$) equality stands in (4.1), if $A_1, \dots, A_n$ are all events of $S_2(p, 1-p)$. (Clearly an inequality which is exact of order 2 is exact.)

We prove the following

THEOREM 3. *Let (4.1) be an inequality which is exact of order 2. If (4.1) holds on $S_3(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$, it holds on every probability space.*

PROOF. If (1.2) is the canonical form of F_j we have

$$(4.2) \quad \begin{aligned} & \sum_{i_1=1}^N \sum_{i_2=1}^N \sum_{i_3=1}^N c_{i_1, i_2, i_3} P(F_{i_1}) P(F_{i_2}) P(F_{i_3}) = \\ & = \sum_{r_1=0}^{2^n-1} \sum_{r_2=0}^{2^n-1} \sum_{r_3=0}^{2^n-1} d(r_1, r_2, r_3) P(B_n(r_1)) P(B_n(r_2)) P(B_n(r_3)) \end{aligned}$$

where

$$(4.3) \quad d(r_1, r_2, r_3) = \sum_{r_h \in E_{i_h} (h=1, 2, 3)} c_{i_1, i_2, i_3} (h=1, 2, 3)$$

Clearly (4.1) being exact implies that

$$d(r, r, r) = 0 \quad (0 \leq r \leq 2^n - 1).$$

Let us put for $r \neq s$

$$D(r, s) = d(r, r, s) + d(r, s, r) + d(s, r, r).$$

Now from the supposition that in (4.1) equality holds on $S_2(p, q)$ ($q = 1-p$) it follows that for any pair of numbers r, s ($r \neq s$)

$$(4.4) \quad D(r, s)p + D(s, r)q = 0.$$

By supposition (4.4) holds for $p = \frac{1}{2}$ and also for some p for which $0 < p < \frac{1}{2}$; it follows that

$$(4.5) \quad D(r, s) = 0 \quad \text{if } s \neq r.$$

Thus we obtain, putting

$$\begin{aligned} D(r_1, r_2, r_3) &= d(r_1, r_2, r_3) + d(r_1, r_3, r_2) + d(r_2, r_1, r_3) + \\ &+ d(r_2, r_3, r_1) + d(r_3, r_1, r_2) + d(r_3, r_2, r_1) \end{aligned}$$

that

$$(4.6) \quad \begin{aligned} & \sum_{i_1=1}^N \sum_{i_2=1}^N \sum_{i_3=1}^N c_{i_1, i_2, i_3} P(F_{i_1}) P(F_{i_2}) P(F_{i_3}) = \\ & = \sum_{0 \leq r_1 < r_2 < r_3 \leq 2^n - 1} D(r_1, r_2, r_3) P(B_n(r_1)) P(B_n(r_2)) P(B_n(r_3)) \end{aligned}$$

$$(4.7) \quad B_n(r_i) = \alpha_i \quad (i = 1, 2, 3).$$

As a matter of fact $A_k^{e_k(r_i)} \supseteq \alpha_i$ ($k = 1, 2, \dots, n$) thus

$$(4.8) \quad B_n(r_i) = \prod_{k=1}^n A_k^{e_k(r_i)} \supseteq \alpha_i$$

As however the events $B_n(r_1), B_n(r_2), B_n(r_3)$ are disjoint, (4.8) implies (4.7).

Clearly (4.7) implies that for any s , different from each of r_1, r_2, r_3 , one has $B_n(s) = \emptyset$. Thus for the above choice of the values of the variables $A_1, \dots, A_n$ we have

$$(4.9) \quad \sum_{i_1=1}^N \sum_{i_2=1}^N \sum_{i_3=1}^N c_{i_1, i_2, i_3} P(F_{i_1}) P(F_{i_2}) P(F_{i_3}) = \frac{1}{27} D(r_1, r_2, r_3)$$

As by supposition (4.1) holds on $S_3(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$, we obtain from (4.9)

$$(4.10) \quad D(r_1, r_2, r_3) \geq 0 \quad \text{for} \quad 0 \leq r_1 < r_2 < r_3 \leq 2^n - 1.$$

In view of (4.6) it follows that (4.1) holds for every probability space S .

As an example consider the following cubic inequality

$$(4.11) \quad P(AB)P(BC)P(AC) \geq P^2(ABC)[P(AB) + P(AC) + P(BC) - 2P(ABC)]$$

Clearly (4.11) is exact of order two. Thus we have to check only that (4.11) holds on $S_3(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$, which is easily done.

Theorem 3 could be generalized also for polynomial inequalities of degree greater than 3.

REFERENCES

- [1] RÉNYI, A.: Quelques remarques sur les probabilités d'événements dépendantes, *Journal de Math.* 37 (1958) 393—398.
- [2] RÉNYI, A.: *Wahrscheinlichkeitsrechnung mit einer Anhang über Informationstheorie*, Deutscher Verlag der Wissenschaften, Berlin, 1962.
- [3] FRÉCHET, M.: *Les probabilités associées à un système d'événements compatibles et dépendants, I, II*, Hermann, Paris, 1940, 1943.
- [4] RÉNYI, A., ERDŐS, P., NEVEU, J.: An elementary inequality between the probability of events, *Math. Scandinavica* 13 (1963) 99—104.

ON RANDOM MATRICES II

by

P. ERDŐS and A. RÉNYI

§ 0. Introduction

This paper is a continuation of our paper [1]. Let $\mathcal{M}(n)$ denote the set of all n by n zero-one matrices; let us denote the elements of a matrix $M_n \in \mathcal{M}(n)$ by ε_{jk} ($1 \leq j \leq n; 1 \leq k \leq n$). Let p denote an arbitrary permutation $p = (p_1, p_2, \dots, p_n)$ of the integers $(1, 2, \dots, n)$ and Π_n the set of all $n!$ such permutations. Let us put for each $p \in \Pi_n$

$$(0.1) \quad \varepsilon(p) = \varepsilon_{1p_1} \cdot \varepsilon_{2p_2} \cdots \varepsilon_{np_n}.$$

Thus the permanent $\text{perm}(M_n)$ of M_n can be written in the form

$$(0.2) \quad \text{perm}(M_n) = \sum_{p \in \Pi_n} \varepsilon(p)$$

Thus each $\varepsilon(p)$ ($p \in \Pi_n$) is a term of the expansion of $\text{perm}(M_n)$.

Let us call two permutations $p' = (p'_1, \dots, p'_n)$ and $p'' = (p''_1, \dots, p''_n)$ ($p' \in \Pi_n, p'' \in \Pi_n$) *disjoint* if $p'_k \neq p''_k$ for $k=1, 2, \dots, n$. Let now define (for each $M_n \in \mathcal{M}(n)$) $v = v(M_n)$ as the largest number of pairwise disjoint permutations $p^{(1)}, \dots, p^{(v)}$ such that $\varepsilon(p^{(i)}) = 1$ ($i=1, 2, \dots, v$). Clearly

$$(0.3) \quad \text{perm}(M_n) \geq v(M_n)$$

thus $v(M_n) \geq 1$ is equivalent to $\text{perm}(M_n) > 0$.

Let us denote by $\mathcal{M}(n, N)$ the set of those n by n zero-one matrices, among the n^2 elements of which exactly N elements are equal to 1 and the remaining $n^2 - N$ to 0 ($0 < N < n^2$). Let us choose at random a matrix $M_{n,N}$ from the set $\mathcal{M}(n, N)$

with uniform distribution, i.e. so that each of the $\binom{n^2}{N}$ elements of $\mathcal{M}(n, N)$ has the

same probability $\binom{n^2}{N}^{-1}$ to be chosen.

Let us denote by $P(n, N, r)$ the probability of the event

$$v(M_{n,N}) \geq r \quad (r=1, 2, \dots).$$

Clearly $P(n, N, 1)$ is the probability of the event $\text{perm}(M_{n,N}) > 0$.

In [1] we have shown that if

$$(0.4) \quad N_1(n) = n \log n + cn + o(n)$$

where c is any fixed real number, one has

$$(0.5) \quad \lim_{n \rightarrow \infty} P(n, N_1(n), 1) = e^{-2e^{-c}}.$$

This implies that if $\omega(n)$ tends arbitrarily slowly to $+\infty$ for $n \rightarrow +\infty$ and

$$(0.6) \quad N_1^*(n) = n \log n + \omega(n)n$$

then

$$(0.7) \quad \lim_{n \rightarrow \infty} P(n, N_1^*(n), 1) = 1.$$

In the present paper we shall extend this result, and prove the following

THEOREM 1. *For any fixed natural number r , if*

$$(0.8) \quad N_r^*(n) = n \log n + (r-1)n \log \log n + n\omega(n)$$

where $\omega(n)$ tends arbitrarily slowly to $+\infty$ for $n \rightarrow +\infty$, we have

$$(0.9) \quad \lim_{n \rightarrow +\infty} P(n, N_r^*(n), r) = 1.$$

Clearly (0.7) is the special case $r=1$ of (0.9). (0.5) can be generalized in a similar way (see Theorem 2). Evidently, the interesting case is when $\omega(n)$ tends slower to $+\infty$ than $\log \log n$.

The method of the proof of Theorem 1 and 2 follows the same pattern as that in [1].

In § 2 we formulate — similarly as in [1] — an analogous result for random zero-one matrices with independent elements, while in § 3 we add some remarks and mention some related open problems.

§ 1. Random matrices with a prescribed number of zeros and ones

We prove in this § Theorem 1. We suppose $r \geq 2$ as the theorem was proved for $r=1$ in [1].

Suppose that M is an n by n zero-one matrix belonging to the set $\mathcal{M}(n, N_r^*(n))$ where $N_r^*(n)$ is defined by (0.8), and suppose that $v(M) \leq r-1$.

Clearly we can delete from each row and column of such a matrix $r-1$ suitably selected ones so that the permanent of the remaining matrix M' should be equal to 0. As regards the matrix M' we distinguish two cases: either the deletion can be made so that M' contains a row or a column which consists of zeros only, or not. Let us denote by $Q_1(n, r)$ the probability of the first case, and by $Q_2(n, r)$ the probability of the second case. Clearly if a row (column) of M' consists of zeros only, the corresponding row (column) of M contains at most $r-1$ ones. Conversely, if M contains such a row or column, then clearly $v(M) \leq r-1$. Thus $Q_1(n, r)$ is equal to the probability of the event that in M there is at least one row or column which contains at most $r-1$ ones. Thus we have

$$(1.1) \quad Q_1(n, r) \leq 2n \sum_{j=0}^{r-1} \binom{n}{j} \frac{\binom{n^2-n}{N_r(n)-j}}{\binom{n^2}{N_r(n)}} = O(e^{-\omega(n)}) = o(1).$$

Let us pass now to the second case. Let k be the least number such that one can find in M' either k columns and $n-k-1$ rows, or k rows and $n-k-1$ columns, which contain all the ones of M' ; according to the theorem of Frobenius (see [2] and [3]) as $\text{perm}(M') = 0$, such a k exists, and $1 \leq k \leq \left\lfloor \frac{n-1}{2} \right\rfloor$ because the case $k=0$ has already been taken into account (this was our first case). We may suppose that all ones of M' are covered by k columns and $n-k-1$ rows (the probability of the other case when the ones of M' are covered by k rows and $n-k-1$ columns being the same by symmetry). It follows — as in [1] — that M' contains a submatrix C' consisting of $k+1$ rows and k columns, such that each column of C' contains at least two ones. Let C be the corresponding submatrix of M . It follows that

$$(1.2) \quad Q_2(n, r) \leq 2 \sum_{k=1}^{\left\lfloor \frac{n-1}{2} \right\rfloor} q_k$$

where $q_k \left(1 \leq k \leq \left\lfloor \frac{n-1}{2} \right\rfloor \right)$ is the probability of the event that M contains a $k+1$ by k submatrix C such that each column of C contains at least two ones, and the submatrix D of M formed by the same rows as C and by those columns which do not intersect C , contains at most $r-1$ ones in each row. Evidently

$$(1.3) \quad q_k \leq \frac{\binom{n}{k} \binom{n}{k+1} \binom{k+1}{2}^k \sum_{j=0}^{(k+1)(r-1)} \frac{\binom{(k+1)(n-k)}{j} \binom{n(n-k-1)+k(k-1)}{N_r^* - 2k - j}}{\binom{n^2}{N_r^*}}}{\binom{n^2}{N_r^*}}.$$

It follows from (1.2) and by an asymptotic evaluation of the expression at the right hand side of (1.3) that

$$(1.4) \quad Q_2(n, r) = o(1).$$

As

$$(1.5) \quad 1 - P(n, N_r^*(n), r) = Q_1(n, r) + Q_2(n, r)$$

it follows in view of (1.1) and (1.4) that (0.9) holds. Thus Theorem 1 is proved.

By the same method we can prove the following result, which generalizes (0.5) for $r \geq 2$.

THEOREM 2. *If*

$$(1.6) \quad N_r(n) = n \log n + (r-1)n \log \log n + cn + o(n)$$

where $r \geq 1$ is an integer and c is any real number, we have

$$(1.7) \quad \lim_{n \rightarrow +\infty} P(n, N_r(n), r) = e^{-\frac{2e^{-c}}{(r-1)!}}.$$

§ 2. Random zero-one matrices with independent elements

Similarly as in [1] let us consider now random n by n matrices $M = (\varepsilon_{ij})$ ($1 \leq i, j \leq n$) such that the ε_{ij} are independent random variables which take on the values 1 and 0 with probabilities p_n and $(1 - p_n)$. It can be shown that the following result is valid:

THEOREM 3. *For any fixed natural number r , put*

$$(2.1) \quad p_n = \frac{\log n + (r-1) \log \log n + \omega(n)}{n}$$

where $\omega(n)$ tends arbitrarily slowly to $+\infty$ and let M be an n by n random matrix the elements of which are independent random variables, taking on the values 1 and 0 with probability p_n and $1 - p_n$ respectively. Then the probability of $v(M) \geq r$ tends to 1 for $n \rightarrow +\infty$.

Note that the special case $r=1$ of Theorem 3 is contained in Theorem 2 of our previous paper [1].

As the idea of the proof is essentially the same as that of (0.9), and the computation even somewhat simpler, we omit the proof of Theorem 3. Theorem 3 can be sharpened in the same way as Theorem 2 sharpens Theorem 1.

§ 3. Remarks and open problems

Let us put

$$(3.1) \quad \mu(n, k) = \min_{\substack{v(M_n)=k \\ M_n \in \mathcal{M}(n)}} (\text{perm}(M_n)).$$

Clearly $\mu(n, 1) = 1$ and $\mu(n, 2) = 2$; however, for $k \geq 3$ the question concerning the value of $\mu(n, k)$ is open. We have clearly $\mu(k, k) = k!$ and

$$(3.2) \quad \mu(k, k-1) = k! \left(\frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^k}{k!} \right)$$

but the value of $\mu(n, k)$ for $n \geq k+2$ is not known. Clearly for determining $\mu(n, k)$ it is sufficient to consider those matrices M_n which contain exactly k ones in each row and in each column. As each such matrix is the sum of k disjoint permutation matrices, i.e. for such a matrix we have $v(M_n) = k$, thus the problem of determining $\mu(n, k)$ is the same as the problem raised by RYSER (see [7], p. 77) concerning the minimum of the permanent of n by n zero-one matrices having exactly k ones in each row and each column. Of course for particular values of n and k one can determine $\mu(n, k)$ (e.g. $\mu(5, 3) = 12$), but what would be of real interest is the asymptotic behaviour of $\mu(n, k)$ for fixed $k \geq 3$ and $n \rightarrow +\infty$.

Let us put

$$(3.3) \quad \liminf_{n \rightarrow \infty} \sqrt[n]{\mu(n, k)} = \mu_k.$$

It seems likely that $\mu_k > 1$ for $k \geq 3$. One reason for this conjecture is that if the conjecture of VAN DER WAERDEN is true, we have

$$(3.4) \quad \mu(n, k) \cong \frac{k^n n!}{n^n} \cong \left(\frac{k}{e}\right)^n$$

i.e. $\mu_k \cong \frac{k}{e} > 1$ for $k \geq 3$. We guess that μ_k is even larger than $\frac{k}{e}$.

If in particular M_n is the matrix defined by $\varepsilon_{j,j} = \varepsilon_{j,j+1} = \varepsilon_{j,j-1} = 1$ (we put $\varepsilon_{j,m} = \varepsilon_{j,m-n}$ for $m > n$) and $\varepsilon_{jl} = 0$ if $|l-j| \geq 2$, then it can be easily shown that $\text{perm}(M_n) = L_n + 2$ where L_n is the n -th LUCAS number, i.e. the n -th term of the Fibonacci-type sequence

$$(3.5) \quad 1, 3, 4, 7, 11, 18, \dots$$

and

$$(3.6) \quad \lim_{n \rightarrow \infty} \sqrt[n]{L_n} = \frac{\sqrt{5} + 1}{2} > \frac{3}{e}.$$

As regards $\mu(n, k)$, at present it is known only that

$$(3.7) \quad \lim_{n \rightarrow +\infty} \mu(n, 3) = +\infty.$$

This was conjectured by MARSHALL HALL and proved by R. SINKHORN [8]. As a matter of fact, SINKHORN proved $\mu(n, 3) \geq n$ for all $n \geq 3$. Of course (3.7) implies $\lim_{n \rightarrow +\infty} \mu(n, k) = +\infty$ for $k = 4, 5, \dots$ too.

An interesting open problem is the following: evaluate asymptotically $P(n, n \log n + (r-1)n \log \log n, r)$ if r is not constant, but increases together with n .

There is a striking analogy between Theorem 1 and the following well known result (see e.g. [4]): If $N_r^*(n)$ balls are placed at random into n urns, and $N_r^*(n)$ is given by (0.8) (with $\omega(n) \rightarrow +\infty$) then the probability of each urn containing at least r balls, tends to 1 for $n \rightarrow +\infty$. The relation between this problem and that of § 1 is made clear by the following remark. If we interpret the rows (columns) of M as urns and the ones as balls, then there are n urns, and each of the $N_r^*(n)$ „balls” falls with the same probability $1/n$ in any of the „urns”.

In another paper ([5]) we have proved the following theorem (Theorem 1 of [5]): a random graph $\Gamma(n, N)$ with n vertices where n is even and $N = \frac{1}{2} n \log n + n \omega(n)$ edges where $\omega(n) \rightarrow +\infty$ for $n \rightarrow +\infty$, contains a factor of degree one with probability tending to 1 for $n \rightarrow +\infty$.

Theorem 1 of the present paper suggests the following problem: does a random graph $\Gamma(n, N)$ where n is even and

$$N = \frac{1}{2} n \log n + \frac{r-1}{2} n \log \log n + \omega(n)n$$

where $\omega(n) \rightarrow +\infty$, contain at least r disjoint factors of degree one with probability tending to 1 for $n \rightarrow \infty$? To prove this, besides the method of [5] the results of [6] have to be used.

REFERENCES

- [1] ERDŐS, P. and RÉNYI A.: On random matrices, *Magyar Tud. Akad. Mat. Kutató Int. Közl* 8 (1964) 455—461.
- [2] FROBENIUS, G.: Über zerlegbare Determinanten, *Sitzungsberichte der Berliner Akademie*, 1917, 274—277.
- [3] KÖNIG, D.: Graphok és matrixok, *Mat. Fiz. Lapok* 38 (1931) 116—119.
- [4] ERDŐS, P. and RÉNYI, A.: On a classical problem of probability theory, *Magyar Tud. Akad. Mat. Kutató Int. Közl.* 6 (1961) 215—220.
- [5] ERDŐS, P. and RÉNYI, A.: On the existence of a factor of degree one of a connected random graphs, *Acta Math. Acad. Sci. Hungar.* 17 (1966) 359—368.
- [6] ERDŐS, P. and RÉNYI, A.: On the strength of connectedness of random graphs, *Acta Math. Acad. Sci. Hungar.* 12 (1961) 261—267.
- [7] RYSER, H. J.: *Combinatorial mathematics*, Carus Math. Monographs, No. 14. Wiley, 1965.
- [8] SINKHORN, R.: Concerning a conjecture of Marshall Hall (in print).

INFORMATION AND STATISTICS

by

A. RÉNYI

Mathematical Institute of the Hungarian Academy of Sciences
Budapest, Hungary

To anybody familiar with the principles of information theory it should be evident that statistical methods can be considered from the point of view of how they handle the available *amount* of information. It seems to the author that in current statistical thinking this point of view is not as consequently applied as it deserves. The reason for this seems to be that if one accepts as a leading principle in statistics to look at everything from the point of view of information theory, one is forced to accept the Bayesian point of view, and the amount of relevant information from sampling can be measured only if the prior information is taken into account, because the amount of information concerning the parameter obtained from the sample can be computed only by comparing the prior and posterior distributions of the parameter.

In what follows we try to outline some fundamental questions of the information theoretical approach to certain basic problems of statistics.

Before going into details we have to define certain notions of information theory. If ξ and ϑ are discrete random variables defined on the same probability space, ξ taking on the different values $a_1, a_2, \dots$ and ϑ the values $b_1, b_2, \dots$ the amount of information contained in the value of ξ with respect to ϑ is given by

$$I(\xi, \vartheta) = \sum_{j,k} r_{jk} \log \frac{r_{jk}}{p_j q_k}, \quad (1)$$

where

$$r_{jk} = \mathbf{P}(\xi = a_j, \vartheta = b_k), \quad p_j = \mathbf{P}(\xi = a_j), \quad q_k = \mathbf{P}(\vartheta = b_k).$$

The *gain of information* concerning a discrete random variable ζ obtained from observing the event 0, if the prior distribution of ζ before taking the observations was $\mathbf{P} = \{p_1, p_2, \dots\}$ where $p_i = \mathbf{P}(\zeta = Z_i)$ and the posterior distribution of ζ after observing 0 is $\mathbf{Q} = \{q_1, q_2, \dots\}$ where $q_i = \mathbf{P}(\zeta = Z_i)$ is given by

$$I(\mathbf{Q} \parallel \mathbf{P}) = \sum_i q_i \log \frac{q_i}{p_i}. \quad (2)$$

The entropy of a discrete distribution $\mathbf{P} = \{p_1, p_2, \dots\}$ is defined by

$$\mathbf{H}(\mathbf{P}) = \sum_k p_k \log \frac{1}{p_k}. \quad (3)$$

Now let us consider the following basic problem of statistics: We observe a sample, i.e. a random vector ξ the distribution of which depends on the parameter ϑ (which may be a single number or a vector) then in case ϑ itself is a discrete valued random variable, the amount of information in the sample ξ concerning the parameter ϑ is given — in case ξ is also discrete valued — by $I(\xi, \vartheta)$ as defined by (1). This quantity can be expressed also as

$$I(\xi, \vartheta) = E(I\langle Q_\xi || P \rangle), \quad (4)$$

where P is the prior distribution of ϑ and Q_ξ its posterior distribution after observing the sample ξ , computed according to Bayes's theorem and $I\langle Q_\xi || P \rangle$ is defined by (2), Q_ξ depends of course on the sample and thus $I\langle Q_\xi || P \rangle$ is itself a random variable, and $I(\xi, \vartheta)$ is equal to its expectation. Formula (4) may serve as the definition of $I(\xi, \vartheta)$ in case ξ has an arbitrary (not discrete) distribution. A third expression of $I(\xi, \vartheta)$ is

$$I(\xi, \vartheta) = H(\vartheta) - E(H(\vartheta | \xi)), \quad (5)$$

where $H(\vartheta)$ and $H(\vartheta | \xi)$ denote the entropy of the prior resp. posterior distribution of ϑ . Formula (5) is valid in the general case (i.e. not only for discrete-valued random variables). The use of the quantity $I(\xi, \vartheta)$ in this context is quite natural and was suggested by several statisticians (see e.g. D. V. Lindley [1], where references to previous literature are also given), but it was not very frequently used up to now. The evaluation of the amount of information in a sample concerning the parameter is very useful e.g. in the design of experiments as it helps in choosing that alternative which gives the maximal amount of information, or to compare different sampling plans from the same point of view. If one chooses a statistic $S(\xi)$, the ratio

$$\frac{I(S(\xi), \vartheta)}{I(\xi, \vartheta)} \quad (6)$$

shows how large a part of the available information is really utilized by using only the statistic $S(\xi)$; it is easy to show that the ratio (6) is equal to 1 if and only if $S(\xi)$ is a *sufficient statistic* for ϑ . If an infinite sequence of observations $\xi_1, \xi_2, \dots, \xi_n, \dots$ is taken and we use the notation $\xi^{(n)} = (\xi_1, \xi_2, \dots, \xi_n)$ for the set of the first n observations, the sequence of random variables $I\langle Q_{\xi^{(n)}} || P \rangle$ is a semi-martingale. If the random variables ξ_k are independent and identically distributed for each fixed value of the parameter (in which case the observations ξ_k are equivalent random variables) and these distributions are different for different values of the parameter, then if ϑ is discrete valued, one has

$$\lim_{n \rightarrow \infty} I(\xi^{(n)}, \vartheta) = H(\vartheta); \quad (7)$$

moreover the (non-negative) difference

$$H(\vartheta) - I(\xi^{(n)}, \vartheta) \quad (8)$$

tends to 0 for $n \rightarrow \infty$ exponentially fast (i.e. is of order $O(q^n)$ where $0 < q < 1$).

As an example for the use of the information-theoretical point of view let us consider the case when ϑ has only two possible values ϑ_0 and ϑ_1 . Let us denote the hypothesis $\vartheta = \vartheta_i$ by H_i ($i = 0, 1$). If in the sample space a critical region A is chosen and the statistic $\alpha = \alpha(\xi)$ is defined by $\alpha = 1$ if $\xi \in A$ and $\alpha = 0$ if $\xi \notin A$, then $I(\alpha, \vartheta)$ gives us the amount of information contained in the observation (of the sample lying in the critical region or not), concerning the question whether H_0 or H_1 is true.

According to the above point of view we should choose such a region A as the critical region for which $I(\alpha, \vartheta)$ is maximal; thus $I(\alpha, \vartheta)$ acts like a loss-function. As it is well known, while in industrial applications the loss function can often be determined it usually cannot be done if the purpose of the statistical analysis is scientific. In such cases the measurement of the amount of information replaces the loss function, and eliminates the arbitrariness in the choice of the level of the error of the first kind. However, the best choice of the critical region depends of course on the prior probability $w_0 = P(H_0)$ of the hypothesis H_0 ; to make the problem definite, one has to know the value of w_0 . If w_0 is unknown, one has to choose for w_0 some value in order to get a definite test. Thus the arbitrariness which was thrown out concerning the choice of the error of the first kind returns in certain cases by another door, namely when the problem is such that w_0 is unknown. However, the dependence of the critical region on a slight change of w_0 is usually not strong and thus a reasonable estimate of w_0 is practically sufficient.

Finally it should be added that while most statisticians who advocate the Bayesian point of view consider the prior distribution as necessarily of a subjective nature, expressing the experimenters beliefs, in many cases a prior distribution having an objective meaning can — at least approximately — be given, e.g. by evaluation of some preliminary experiments as is shown by the results of H. Robbins concerning what he calls the "empirical Bayes approach". A highly illuminating discussion of this point of view was recently given by J. Neyman [2].

The proofs of the results announced here, and further developments of these ideas are given elsewhere (see: [3], [4], [5], [6], [7] [8]).

REFERENCES

1. LINDLEY, D. V., On a Measure of the Information Provided by an Experiment. *Annals of Math. Stat.* **27**, 986–1005 (1956).
2. NEYMAN, J., Two Breakthroughs in the Theory of Statistical Decision Making. *Revue de l'Inst. Internat. de Statistique* **30**, 11–27 (1962).
3. RÉNYI, A., On the Amount of Information Concerning an Unknown Parameter in a Sequence of Observations. *Publ. Math. Inst. Hung. Acad. Sci.* **9**, 617–624 (1964).
4. RÉNYI, A., On the Amount of Missing Information and the Neyman–Pearson Lemma. *Research Papers in Statistics, Festschrift for J. Neyman*, Wiley, London, 281–288 (1966).
5. RÉNYI, A., On some Basic Problems of Statistics from the Point of View of Information Theory. *Proceedings of the 5th Berkeley Symposium* (in print).
6. RÉNYI, A., On the Amount of Information in a Frequency Count. *35th Session of the ISI Beograd, 1965*.
7. RÉNYI, A., On the Amount of Information in a Random Variable Concerning an Event. *Journal of Mathematical Sciences (Delhi)* **1**, 30–33 (1966).
8. RÉNYI, A., Statistics and Information Theory. *Studia Sci. Math. Acad. Sci. Hung.* **2**, 249–256 (1967).

SOME REMARKS ON THE LARGE SIEVE OF YU. V. LINNIK

By

P. ERDŐS and A. RÉNYI

Mathematical Institute of the Hungarian Academy of Sciences, Budapest

§ 1. Introduction

YU. V. LINNIK has discovered (see [1]) in 1941 a very powerful new method of elementary number theory, which he called the large sieve¹. In his original formulation the large sieve asserts that if we take any sequence S_N consisting of Z positive integers $\leq N$, and if Y denotes the number of those primes² $p \leq \sqrt{N}$ for which all the elements of the sequence S_N are contained in $\leq p(1-\varepsilon)$ residue classes mod p , where $0 < \varepsilon < 1$, then one has

$$(1.1) \quad Y \leq \frac{20\pi N}{\varepsilon^2 Z}.$$

As shown by the second named author in [3], Linnik's method is capable to prove much more, namely that if Z is not too small compared with N , then the elements of the sequence S_N not only occupy "almost all" residue classes mod p with respect to most primes $p \leq \sqrt{N}$, but are almost uniformly distributed in the p residue classes mod p for most primes $p \leq \sqrt{N}$. More exactly, let us denote by $Z(a, p)$ (where $a = 0, 1, \dots, p-1$) the number of elements of the sequence S_N which are congruent to a mod p . Then one has, putting

$$(1.2) \quad \Delta^2(p) = p \sum_{a=0}^{p-1} \left(Z(a, p) - \frac{Z}{p} \right)^2.$$

the inequality³

¹ As regards important applications of the large sieve in number theory, see e.g. [2] 3], [4], [5], [6]; [5] and [6] contain many further references.

² In this paper p always denotes a prime number.

³ Here and in what follows all the constants of the O -estimates are absolute, i.e. do not depend on N , nor on the sequence S_N nor on Q .

$$(1.3) \quad \sum_{p \leq Q} \Delta^2(p) = O(Z^{2/3} N^{4/3} Q^{1/3})$$

for $Q \leq N^{3/5}$. Later, the second named author has found (see [7]), a new probabilistic method for proving theorems of the type of the large sieve. This method (developed further and generalized in the papers [8], [9], [10], [11], [12]) gave the result

$$(1.4) \quad \sum_{p \leq Q} \Delta^2(p) = O(Z(Q^3 + N))$$

for $Q \leq \sqrt{N}$. This estimate is better than (1.3) for $Q \leq N^{3/8}$, but weaker if $N^{3/8} < Q \leq \sqrt{N}$.

Especially for $Q = N^{1/3}$ this result gives

$$(1.5) \quad \sum_{p \leq N^{1/3}} \Delta^2(p) = O(NZ).$$

The estimate (1.5) is essentially best possible, because if for instance S_N is the sequence of odd numbers $\leq N$, one has $Z(0, 2) = 0$ and thus $2 \left| Z(0, 2) - \frac{Z}{2} \right|^2 = \frac{Z^2}{2}$ i.e. this single term is already of order NZ .

The probabilistic approach, besides leading to a very sharp estimate for $Q \leq N^{1/3}$, has thrown light on the reasons why an arbitrary sufficiently dense subsequence of the sequence $1, 2, \dots, N$ has to be almost uniformly distributed among the residue classes mod p for most $p \leq N^{1/3}$; it became obvious that this is due to the statistical independence (more exactly: almost independence) of the distribution mod p and mod q of the numbers $n \leq N$ for any two primes $p, q \leq N^{1/3}$, $p \neq q$.

In the last two years important progress was made on the large sieve. The first essential improvement was obtained by K. F. ROTH [13]. His result was sharpened by BOMBIERI [14] who has shown that (1.5) holds also for $Q = \sqrt{N}$. More exactly Bombieri proved

$$(1.6) \quad \sum_{p \leq Q} \Delta^2(p) = O(Z(Q^2 + N)).$$

Clearly (1.6) is superior to both (1.3) and (1.4) for the full ranges $Q \leq N^{3/8}$ resp. $Q \leq \sqrt{N}$.

An important generalization of Bombieri's theorem has been obtained by H. DAVENPORT and H. HALBERSTAM [15]. To make this advance clear one has to notice that putting

$$(1.7) \quad S(x) = \sum_{n \in S_N} e^{2\pi i n x}$$

one has

$$(1.8) \quad \Delta^2(p) = \sum_{a=1}^{p-1} \left| S\left(\frac{a}{p}\right) \right|^2.$$

Now DAVENPORT and HALBERSTAM have proved that if $\alpha_1, \alpha_2, \dots, \alpha_D$ are arbitrary real numbers in the interval $(0, 1)$ such that $|\alpha_i - \alpha_j| \geq \delta > 0$ for $i \neq j$, one has

$$(1.9) \quad \sum_{i=1}^D |S(\alpha_i)|^2 = O\left(Z\left(\frac{1}{\delta} + N\right)\right).$$

Clearly, if the numbers $\frac{a}{p}$ ($a = 1, 2, \dots, p-1$; $p \leq Q$) are taken as the numbers $\alpha_1, \dots, \alpha_D$ ($D = \sum_{p \leq Q} (p-1)$) then $\delta \geq \frac{1}{Q^2}$ and thus (in view of (1.8)) (1.9) implies (1.6).

Note that from (1.9) one obtains even more than (1.6), namely that

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a, q)=1}}^q \left| S\left(\frac{a}{q}\right) \right|^2 = O\left(Z\left(\frac{1}{\delta} + N\right)\right)$$

because if $(a, q) = 1$, $(a', q') = 1$ (here (a, q) denotes the greatest common divisor of a and q) one has for $q, q' \leq Q$ and $\frac{a}{q} \neq \frac{a'}{q'}$

$$\left| \frac{a}{q} - \frac{a'}{q'} \right| \geq \frac{1}{Q^2}.$$

Recently P. X. GALLAGHER [16] has found a very elegant and simple method for proving (1.9). More exactly, he proved

$$(1.10) \quad \sum_{v=1}^D |S(\alpha_v)|^2 \leq Z\left(\frac{1}{\delta} + \pi N\right)$$

which implies by (1.8)

$$(1.11) \quad \sum_{p \leq Q} \Delta^2(p) \leq Z(Q^2 + \pi N).$$

Thus we have for $Q = \sqrt{N}$

$$(1.12) \quad \sum_{p \leq Q} \Delta^2(p) \leq (\pi + 1)ZN.$$

In the paper [17] of the first named author it has been mentioned (without giving the proof in detail) that by a probabilistic argument it can be shown that (1.12) cannot hold if Q is of larger order of magnitude than $\sqrt{N \log N}$. The aim of the present paper is to prove this statement in detail, and to get some related results concerning the behaviour of $\sum_{p \leq Q} \Delta^2(p)$, when S_N is a *random* subset of the set $\{1, 2, \dots, N\}$.

The results obtained throw some light on certain open problems connected with the large sieve.

§ 2. Equidistribution of random sequences in arithmetic progressions

In this § let S_N denote a random subsequence of the sequence $\{1, 2, \dots, N\}$ obtained as follows: let $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_N$ be independent random variables, each of which takes on the values 1 and 0 with probability $\frac{1}{2}$; let S_N denote the set of those $n \leq N$ for which $\varepsilon_n = 1$. (It is easy to see that under these suppositions each of the 2^N subsets of the set $\{1, 2, \dots, N\}$ has the same probability to be chosen.) In this case

$$(2.1) \quad Z = \sum_{n=1}^N \varepsilon_n$$

$$(2.2) \quad Z(a, p) = \sum_{k=0}^{\left[\frac{N-a}{p}\right]} \varepsilon_{kp+a}$$

and consequently

$$(2.3) \quad \Delta^2(p) = p \cdot \sum_{a=0}^{p-1} \left(Z(a, p) - \frac{Z}{p} \right)^2$$

are all random variables. One obtains easily

$$(2.4) \quad \Delta^2(p) = p \cdot \sum_{a=0}^{p-1} Z^2(a, p) - Z^2$$

and thus, putting⁴

$$(2.5) \quad \pi_r(Q) = \sum_{p \leq Q} p^r \quad (r = 0, 1, 2, \dots)$$

we have

$$(2.6) \quad R(Q) = \sum_{p \leq Q} \Delta^2(p) = \sum_{n=1}^N \sum_{m=1}^N [A_Q(n-m) - \pi_0(Q)] \varepsilon_n \varepsilon_m,$$

where

$$(2.7) \quad A_Q(k) = \sum_{\substack{p|k \\ p \leq Q}} p$$

and thus $A_Q(-k) = A_Q(k)$ and especially

$$(2.8) \quad A_Q(0) = \pi_1(Q).$$

Let us determine first the expectation⁵ of $R(Q)$. As

$$(2.9) \quad E(\varepsilon_n) = \frac{1}{2} \quad \text{and} \quad E(\varepsilon_n \varepsilon_m) = \begin{cases} \frac{1}{4} & \text{if } n \neq m \\ \frac{1}{2} & \text{if } n = m \end{cases}$$

⁴ Thus $\pi_0(Q)$ denotes the number of primes $\leq Q$.

⁵ The expectation of a random variable ξ will be denoted by $E(\xi)$.

we obtain

$$(2.10) \quad E(R(Q)) = \frac{1}{4} \sum_{n=1}^N \sum_{m=1}^N (A_Q(n-m) - \pi_0(Q)) + \frac{N}{4} \pi_1(Q).$$

Now clearly

$$(2.11) \quad \sum_{n=1}^N \sum_{m=1}^N [A_Q(n-m) - \pi_0(Q)] = \sum_{p \leq Q} p \left\{ \sum_{a=0}^{p-1} \left[\left(\left[\frac{N-a}{p} \right] + 1 \right)^2 - \frac{N^2}{p^2} \right] \right\}.$$

Let us suppose that $N \equiv r \pmod{p}$, where $0 \leq r < p$. Then we have

$$(2.12) \quad p \cdot \left\{ \sum_{a=0}^{p-1} \left[\left(\left[\frac{N-a}{p} \right] + 1 \right)^2 \right] \right\} = 2N + r(p-r) + p - 2r.$$

Thus it follows that

$$(2.13) \quad \sum_{n=1}^N \sum_{m=1}^N [A_Q(n-m) - \pi_0(Q)] = 2N\pi_0(Q) + O(Q^2\pi_0(Q))$$

and thus, taking into account that $\pi_0(Q) = \frac{Q}{\log Q} + O\left(\frac{Q}{\log^2 Q}\right)$ and

$$(2.14) \quad \pi_1(Q) = \frac{Q^2}{2 \log Q} + O\left(\frac{Q^2}{\log^2 Q}\right)$$

it follows

$$(2.15) \quad E(R(Q)) = \frac{NQ\pi_0(Q)}{8} + O(Q^2\pi_0(Q)) + O\left(\frac{Q^2N}{\log^2 Q}\right).$$

Thus the expectation of $R(Q)$ is smaller by a factor of order $\frac{1}{\log Q}$ as NQ^2 .

Note that the expectation of $R(Q)$ can be interpreted as its average over all 2^N subsequences of the sequence $\{1, 2, \dots, N\}$. Thus the average of $R(Q)$ is of order $O(N^2)$ even for $Q = O(\sqrt{N \log N})$ while for its maximum according to (1.6) this is known only for $Q = O(\sqrt{N})$. It is an open question whether the estimate

$$(2.16) \quad R(Q) = O(N^2)$$

holds for all sequences S_N if $Q \sim \sqrt{N} \psi(N)$ for some function $\psi(N)$ such that $\psi(N) \rightarrow \infty$ for $N \rightarrow \infty$. Our method is not capable of giving such a result; however by evaluating the variance of the random variable $R(Q)$ we can show by Čebishev's inequality that the estimate (2.16) is valid at least for most subsequences S_N .

To evaluate the variance⁶ of $R(Q)$ note that though the random variables $\varepsilon_n \varepsilon_m$ are not independent, they are pairwise uncorrelated and thus the variance

⁶ The variance of a random variable ξ will be denoted by $D^2(\xi)$.

of the sum on the right hand side of (2.6) is equal to the sum of the variances of the single terms. As $D^2(\varepsilon_n \varepsilon_m) = \frac{3}{16}$ if $n \neq m$ and $D^2(\varepsilon_n^2) = \frac{4}{16}$.

$$(2.17) \quad D^2(R(Q)) = \frac{3}{16} \sum_{n=1}^N \sum_{m=1}^N (A_Q(n-m) - \pi_0(Q))^2 + \frac{N}{16} (\pi_1(Q) - \pi_0(Q))^2.$$

Now clearly

$$(2.18) \quad \sum_{n=1}^N \sum_{m=1}^N A_Q^2(n-m) \leq N^2[\pi_0^2(Q) + \pi_1(Q) - \pi_0(Q)] + 2N\pi_1^2(Q) + \pi_2^2(Q).$$

As further from (2.11) we have

$$\sum_{n=1}^N \sum_{m=1}^N A_Q(n-m) \cong N^2\pi_0(Q) - 2N\pi_0(Q) + \pi_1(Q)$$

it follows

$$(2.19) \quad D^2(R(Q)) \leq \frac{3}{16} N^2(\pi_1(Q) - \pi_0(Q)) + \\ + \frac{3N}{8} \left(\pi_1^2(Q) + 2\pi_0^2(Q) + \frac{(\pi_1(Q) - \pi_0(Q))^2}{6} \right) + \frac{3}{16} \pi_2^2(Q) - \frac{3}{8} \pi_1(Q)\pi_0(Q).$$

In view of (2.14), it follows

$$(2.20) \quad D^2(R(Q)) = O\left(\frac{N^2 Q^2}{\log Q}\right) + Q\left(\frac{NQ^4}{\log^2 Q}\right)$$

i.e.

$$(2.21) \quad \frac{D(R(Q))}{E(R(Q))} = O\left(\frac{\sqrt{\log Q}}{Q}\right) + O\left(\frac{1}{\sqrt{N}}\right).$$

It follows from Čebishev's inequality that for $\lambda > 1$ with probability $\geq 1 - \frac{1}{\lambda^2}$ $R(Q)$ is contained in an interval

$$[E(R(Q)) - \lambda D(R(Q)), E(R(Q)) + \lambda D(R(Q))].$$

Choosing for λ the value $\lambda = \min\left(\frac{Q}{(\log Q)^{3/2}}, \frac{\sqrt{N}}{\log Q}\right)$ it follows that for all but $\frac{2^N}{\lambda^2}$ possible exceptions for all other sequences, i.e. for the large majority of all sequences, $R(Q)$ is of order $\frac{NQ^2}{8 \log Q} + O\left(\frac{NQ^2}{\log^2 Q}\right)$.

Thus we have proved the following

THEOREM 1. Let us consider all 2^N subsequences S_N of the sequence $\{1, 2, \dots, N\}$. We have for all these subsequences with the possible exception of $\frac{2^N}{\lambda^2}$ such sequences

$$(2.22) \quad R(Q) = \frac{NQ^2}{8 \log Q} + O\left(\frac{NQ^2}{\log^2 Q}\right)$$

where $Q \geq N^{1/3}$ and

$$(2.23) \quad \lambda = \min\left(\frac{Q}{(\log Q)^{3/2}}, \frac{\sqrt{N}}{\log Q}\right).$$

Thus, if $Q \leq \sqrt{N \log N}$, (2.22) holds except for at most $\frac{2^N \log^3 Q}{Q^2}$ sequences, while for $Q > \sqrt{N \log N}$ (2.22) holds, except for at most $\frac{2^N \log^2 N}{N}$ sequences.

COROLLARY. If $Q = \sqrt{AN \log N}$ ($A > 1$) then $R(Q) \sim \frac{AN^2}{8}$ except for at most $\frac{2^N \log^2 N}{N}$ sequences.

Let us now consider the quantity

$$\text{Max}_{p \leq Q} \left[\text{Max}_{0 \leq a \leq p-1} \left| Z(a, p) - \frac{Z}{p} \right| \right].$$

It is easy to show [using the central limit theorem and the fact that for any given p the quantities $Z(a, p)$ ($a = 0, 1, \dots, p-1$) are independent], that

$$(2.24) \quad P\left(\text{Max}_{0 \leq a \leq p-1} \left| Z(a, p) - \frac{Z}{p} \right| > \sqrt{\frac{N \log pQ}{2p}}\right) = O\left(\frac{1}{Q}\right)$$

and thus except for at most $O\left(\frac{2^N}{\log Q}\right)$ exceptional sequences we have

$$\left| Z(a, p) - \frac{Z}{p} \right| \leq \sqrt{\frac{N \log pQ}{2p}}$$

for all a and p ($0 \leq a \leq p-1$, $p \leq Q$).

On the other hand, using again the independence of the random variables $Z(a, p)$ ($a = 0, 1, \dots, p-1$) and the central limit theorem it follows that for all except for at most $O\left(\frac{2^N}{N}\right)$ sequences S^N , one has, for all p such that

$$C \log N < p < \frac{N}{\sqrt{\log N}}$$

$$\Delta^2(p) = \frac{Np}{4} \left(1 + O\left(\frac{1}{\sqrt{\log N}}\right) \right)$$

if C is a sufficiently large positive number.

§ 3. The values of a random trigonometrical polynomial at well spaced points

In this § we shall consider the sum

$$(3.1) \quad T(\alpha, S) = \sum_{\nu=1}^D |S(\alpha_\nu)|^2$$

where $\alpha_1, \alpha_2, \dots, \alpha_D$ are real numbers "well spaced" in the sense of Davenport and Halberstam, satisfying

$$(3.2) \quad 0 < \alpha_1 < \alpha_2 < \dots < \alpha_D < 1 \quad \text{and} \\ \alpha_{\nu+1} - \alpha_\nu \geq \delta > 0 \quad \text{for } \nu = 1, 2, \dots, D-1$$

and $S(\alpha)$ is the random trigonometric polynomial

$$(3.3) \quad S(\alpha) = \sum_{n=1}^N \varepsilon_n e^{2\pi i n \alpha}$$

where $\varepsilon_1, \dots, \varepsilon_N$ are independent random variables, each taking on the values 1 and 0 with probability $\frac{1}{2}$.

We first evaluate the expectation of $T(\alpha, S)$. We have clearly

$$(3.4) \quad T(\alpha, S) = \sum_{n=1}^N \sum_{m=1}^N \varepsilon_n \varepsilon_m \sum_{\nu=1}^D e^{2\pi i (n-m)\alpha_\nu}$$

and thus

$$(3.5) \quad E(T(\alpha, S)) = \frac{1}{2} \sum_{\nu=1}^D \left(\frac{N}{2} + \sum_{l=1}^{N-1} (N-l) \cos 2\pi l \alpha_\nu \right) + \frac{ND}{4}.$$

Now it is well known that

$$(3.6) \quad \frac{N}{2} + \sum_{l=1}^{N-1} (N-l) \cos 2\pi l \alpha_\nu = \frac{\sin^2 N\pi \alpha_\nu}{2 \sin^2 \pi \alpha_\nu}.$$

As a matter of fact the formula (3.6) is well known as a formula for Fejér's kernel of the arithmetic means of Fourier series.

It follows from (3.5) and (3.6) that

$$(3.7) \quad E(T(\alpha, S)) = \frac{1}{4} \sum_{\nu=1}^D \frac{\sin^2 N\pi \alpha_\nu}{\sin^2 \pi \alpha_\nu} + \frac{ND}{4}.$$

Let us now consider the special case when $\alpha_Q^* = (\alpha_1^*, \dots, \alpha_D^*)$ is the set of all numbers $\frac{a}{q}$ with $(a, q) = 1$, $1 \leq a \leq q$, $1 < q \leq Q \leq N$. It is easy to see that

$$(3.8) \quad \sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^q \frac{\sin^2 N\pi \frac{a}{q}}{\sin^2 \pi \frac{a}{q}} = O(Q^3)$$

thus, denoting by $\varphi(q)$ the number of numbers $a < q$ relatively prime to q , we have

$$(3.9) \quad E(T(\alpha_Q^*, S)) = \frac{N}{4} \sum_{q=1}^Q \varphi(q) + O(Q^3).$$

As however

$$(3.10) \quad \sum_{q=1}^Q \varphi(q) = \frac{3Q^2}{\pi^2} + O(Q \log Q)$$

it follows that

$$(3.11) \quad E(T(\alpha_Q^*, S)) = \frac{3Q^2 N}{4\pi^2} + O(NQ \log Q) + O(Q^3).$$

It follows that for $Q = o(N)$ there exists for each $\varepsilon > 0$ a sequence S_N for which

$$(3.12) \quad T(\alpha_Q^*, S_N) > \frac{3Q^2 N(1 - \varepsilon)}{4\pi^2}.$$

Thus the estimate

$$(3.13) \quad \sum_{q \leq Q} \sum_{\substack{a=1 \\ (a, q)=1}}^q \left| S\left(\frac{a}{q}\right) \right|^2 = O(N^2)$$

which according to the theorem of Davenport and Halberstam is valid for $Q \leq \sqrt{N}$ cannot be valid if Q is of larger order of magnitude than $\sqrt{N}$. By evaluating the variance of $T(\alpha, S)$ one can prove even more, namely that $T(\alpha_Q^*, S_N) \sim \sim \frac{3Q^2 N}{4\pi^2}$ for all except $o(2^N)$ sequences S_N , if $\frac{1}{Q} = o(1)$ and $\frac{Q}{N} = o(1)$. In particular one can prove that

$$(3.14) \quad D \left(\sum_{q \leq \sqrt{N}} \sum_{\substack{a=1 \\ (a, q)=1}}^{q-1} \left| S\left(\frac{a}{q}\right) \right|^2 \right) = O(N^{3/2})$$

which implies that except for at most $O\left(\frac{2^N \log N}{N}\right)$ exceptional sequences

$$(3.15) \quad \sum_{q \leq \sqrt{N}} \sum_{\substack{a=1 \\ (a, q)=1}}^{q-1} \left| S\left(\frac{a}{q}\right) \right|^2 \sim \frac{3N^2}{4\pi^2}.$$

Let us summarize now our results: Theorem 1 shows that the estimate

$$(3.16) \quad R(Q) = O(N^2)$$

cannot hold if Q is of larger order of magnitude than $\sqrt{N \log N}$. It remains an open question whether (3.16) holds if $\sqrt{N} \leq Q \leq \sqrt{N \log N}$. However, (3.11) shows that even if (3.16) is true for the range $\sqrt{N} \leq Q \leq \sqrt{N \log N}$ it cannot be proved by the methods used up to now, as all these methods gave estimates for $R(Q)$ through estimating $T(\alpha_Q^*, S)$.

§ 4. Some open problems

Let S_N denote a subsequence of the sequence $\{1, 2, \dots, N\}$ which contains at least cN elements ($0 < c < 1$). Let $Y(\alpha, \varepsilon)$ where $0 < \varepsilon < 1$ and $1/2 \leq \alpha < 1$ denote the number of those primes $p \leq N^\alpha$ for which at least $p\varepsilon$ residue classes mod p do not contain any element of S_N . It follows already from Linnik's result (1.1) that $Y\left(\frac{1}{2}, \varepsilon\right)$ is bounded, namely that

$$(4.1) \quad Y\left(\frac{1}{2}, \varepsilon\right) \leq \frac{20\pi}{c\varepsilon^2}.$$

From (1.12) one obtains the slightly better estimate

$$(4.2) \quad Y\left(\frac{1}{2}, \varepsilon\right) \leq \frac{\pi+1}{\varepsilon c}.$$

As regards $Y(\alpha, \varepsilon)$ with $1/2 < \alpha < 1$ we get from (1.11) the estimate

$$(4.3) \quad Y(\alpha, \varepsilon) \leq \frac{N^{2\alpha-1}}{\varepsilon c} + \frac{\pi}{\varepsilon c}.$$

It seems probable that (4.3) is far from being best possible; it is an open problem whether $Y(\alpha, \varepsilon)$ is bounded for every α with $\frac{1}{2} < \alpha < 1$, or not. Of course, $Y(1, \varepsilon)$ is not bounded: as a matter of fact if S_N is the sequence of numbers $\leq Nc$ $\left(0 < c < \frac{1}{2}\right)$ and $0 < \varepsilon < \frac{1}{2}$ then for all primes p with $\frac{cN}{1-\varepsilon} < p < N$ at least $p\varepsilon$ residue classes mod p do not contain any element of S_N , and thus

$$Y(1, \varepsilon) \geq \frac{N}{\log N} \left(1 - \frac{c}{1-\varepsilon}\right) + O\left(\frac{N}{\log^2 N}\right).$$

Another related problem is the following: if $0 < \varepsilon < 1$ let S_N be a subsequence of the sequence $\{1, 2, \dots, N\}$ such that for every p with $A_\varepsilon < p < N^\alpha$ where $A_\varepsilon > 0$, $0 < \alpha < 1$ there are at least εp residue classes mod p which do not contain any element of S_N . What is the maximum $M_N(\varepsilon, \alpha)$ of the number of terms of such a sequence S_N ? It is easy to show that for each ε with $0 < \varepsilon < 1/2$ $M_N(\varepsilon, 1) \geq [\sqrt{N}]$. As a matter of fact let S_N denote the sequence of squares $\leq N$. Clearly if b is a quadratic non-residue mod p , then there is no element of the sequence $1^2, 2^2, \dots, k^2, \dots$ which is congruent to b mod p ; thus for each p the number of empty residue classes is at least $\frac{p-1}{2}$ if $p \geq 3$.

References

- [1] YU. V. LINNIK, The large sieve, *Comptes Rendus (Doklady) de l'Académie des Sci. de l'URSS*, **30** (1941), 292–294.
- [2] YU. V. LINNIK, Remark on the least quadratic non-residue, *Comptes Rendus (Doklady) de l'Académie des Sci. de l'URSS*, **36** (1942), 131.
- [3] A. RÉNYI, On the representation of an even number as the sum of a prime and of an almost prime, *Izvestiya Akad. Nauk. SSSR, Ser. Math.*, **12** (1948), 57–78 (in Russian), (see also *American Math. Soc., Translation Series 2.*, **19** (1962), 299–321).
- [4] P. T. BATEMAN – S. CHOWLA – P. ERDŐS, Remarks on the size of $L(1, \chi)$ *Publ. Math.*, **1** (1950), 165–182.
- [5] M. B. BARBAN, The large sieve and its applications in number theory, *Uspechi Mat. Nauk*, **21** (1966), 51–102, (in Russian).
- [6] H. HALBERSTAM – K. F. ROTH, *Sequences*, Vol. I. (Oxford, Clarendon Press, 1966). Ch. IV. § 10. The large sieves of Linnik and Rényi (pp. 224–237).
- [7] A. RÉNYI, On the large sieve of Yu. V. Linnik, *Compositio Math.*, **8** (1950), 68–75.
- [8] A. RÉNYI, Un nouveau théorème concernant les fonctions indépendantes et ses applications à la théorie des nombres, *Journal Math. Pure et Appl.*, **28** (1949), 137–149.
- [9] A. RÉNYI, Sur un théorème général de probabilité, *Annales de l'Institut Fourier*, **1** (1950), 43–52.
- [10] A. RÉNYI, On a general theorem in probability theory and its application in the theory of numbers, *Zprávy o společném 3. sjezdu matematikůu československých a 7. sjezdu matematikůu polských*, Praha 1950. 167–174.
- [11] A. RÉNYI, On the probabilistic generalization of the large sieve of Linnik, *MTA Mat. Kut. Int. Köz.*, **3** (1958), 199–206.
- [12] A. RÉNYI, New version of the probabilistic generalization of the large sieve, *Acta Math. Acad. Sci. Hung.*, **10** (1959), 217–226.
- [13] K. F. ROTH, On the large sieve of Linnik and Rényi, *Mathematika*, **12** (1965), 1–9.
- [14] E. BOMBIERI, On the large sieve, *Mathematika*, **12** (1965), 201–225.
- [15] H. DAVENPORT – H. HALBERSTAM, The values of a trigonometrical polynomial at well spaced points, *Mathematika*, **13** (1966), 91–96.
- [16] P. X. GALLAGHER, The large sieve, *Mathematika*, **14** (1967), 14–20.
- [17] P. ERDŐS, Remarks on number theory V., *Mat. Lapok*, **17** (1966), 135–155. (In Hungarian).

NOTE

The result of Wolke, quoted in the Notes to paper No. 200 has connection to (2.22) too. The remarks on p. 5. in the paper indicate that (1.12) cannot hold “probably” for $Q > \sqrt{N \log N}$ which indicates that Bombieri’s theorem can “probably” not be extended to $Q = x^{1-\epsilon}$ via large sieve (though probably true). Halberstam remarked that such a theorem with $Q = x^{4/7}$ would imply already the representability $2n = p + P_2$ for all sufficiently large n ’s. (P. T.)

P. ERDÖS and A. RÉNYI (Budapest)

ON RANDOM ENTIRE FUNCTIONS

This paper deals with random power series, a topic concerning which the first important results are due to H. Steinhaus [4].

While in [4] power series with a finite radius of convergence were considered, we study random entire functions.

Let

$$(1) \quad f(z) = \sum_{n=0}^{\infty} a_n z^n$$

be an arbitrary entire function; let

$$(2) \quad M(r) = \max_{|z|=r} |f(z)|$$

denote the maximum-modulus function of $f(z)$ and

$$(3) \quad \mu(r) = \max_n |a_n| r^n$$

the maximal term of the series (1).

According to Wiman's well known theorem, for every $\delta > 0$ there exists a set E_δ of finite logarithmic measure (i.e. such that $\int_{E_\delta} \frac{dr}{r} < \infty$) such that if $r \notin E_\delta$ one has

$$(4) \quad M(r) < \mu(r) (\log \mu(r))^{\frac{1}{2} + \delta}.$$

The simplest proof of this theorem is the probabilistic proof given by Rosenbloom [2], which deduces (4) from Chebishev's inequality.

It is known that the number $\frac{1}{2}$ in the exponent of $\log \mu(r)$ on the right hand side of (4) is best possible, as there exist entire functions $f(z)$ for which there exists a constant $c > 0$ such that

$$M(r) > c \mu(r) (\log \mu(r))^{\frac{1}{2}} \quad \text{for all } r \geq 0.$$

As a matter of fact, if $f(z) = e^z$, $M(r) = e^r$ and $\mu(r) = \frac{r^{[r]}}{[r]!}$ for $r > 0$ where $[r]$ denotes the integral part of r ; thus by Stirling's formula

$$(5) \quad \lim_{r \rightarrow \infty} \frac{M(r)}{\mu(r)(\log \mu(r))^{1/2}} = \sqrt{2\pi}.$$

The first-named author has stated without proof some years ago — in a paper [1] which was dedicated to Professor Steinhaus — that if we give random signs to the terms of the power series of e^z then for almost all choices of the sequence of signs the exponent $\frac{1}{2}$ in (4) can be replaced by $\frac{1}{4}$ but by no smaller number. In the present paper we consider the same question for an arbitrary entire function. By other words we consider the class of entire functions obtained by giving random signs to the terms of the series (1), i.e. we consider the entire functions

$$(6) \quad f(z, t) = \sum_{n=0}^{\infty} a_n R_n(t) z^n \quad (0 \leq t < 1)$$

where $R_n(t)$ is the n -th Rademacher function, $R_n(t) = \text{sign} \sin(2^n \pi t)$.

We shall prove that for almost all values of t in the inequality (4) for $f(z, t)$ the exponent $\frac{1}{2}$ of $\log \mu(r)$ can be replaced by $\frac{1}{4}$.

We shall prove even more. Rosenbloom in his above mentioned paper⁽¹⁾ [2] has proved the following sharper form of Wiman's theorem: for every $\delta > 0$ there exists a set E_δ of finite logarithmic measure, such that if $r \notin E_\delta$ one has

$$(4^*) \quad M(r) < \mu(r)(\log \mu(r))^{1/2}(\log \log \mu(r))^{1+\delta}.$$

We shall prove that for almost all values of t , in the corresponding inequality for $f(z, t)$ the exponent $\frac{1}{2}$ of $\log \mu(r)$ can be replaced by $\frac{1}{4}$. Thus we prove the following

THEOREM 1. *Let (1) be an arbitrary entire function and let $\mu(r)$ be defined by (3). Let the entire function $f(z, t)$ be defined by (6) and put*

$$(7) \quad M(r, t) = \max_{|z|=r} |f(z, t)| \quad (0 \leq t < 1).$$

Then for every $\delta > 0$, for almost all values of t there exists a subset $E_\delta(t)$ (depending on t) of the half line $r \geq 0$ of finite logarithmic measure, such that for $r \notin E_\delta(t)$ one has

$$(8) \quad M(r, t) < \mu(r)(\log \mu(r))^{1/4}(\log \log \mu(r))^{1+\delta}.$$

⁽¹⁾ The formulation of Theorem 1 in paper [2] contains some misprints: In formula (2) (p. 327) the integral sign is missing; in row 9 of p. 327 the sign = has to be replaced by <; in row 10 of p. 327 instead of "inequality (2)" one should read "inequality (3)".

Proof. Let us put

$$(9) \quad f_1(z) = \sum_{n=0}^{\infty} |a_n| z^n.$$

We may suppose that $a_0 = 1$, which implies $\mu(0) = 1$. As (4*) is valid for $f_1(z)$, there exists for every $\delta > 0$ a set E_δ of finite logarithmic measure such that for $r \notin E_\delta$ the inequality

$$(10) \quad f_1(r) < \mu(r) (\log \mu(r))^{1/2} (\log \log \mu(r))^{1+\delta}$$

is valid. We may suppose that the set E_δ is the union of a denumerable set of disjoint open intervals, the endpoints of which have no finite limit point. Let us define the sequence r_n of nonnegative numbers as follows. We put $r_0 = 0$; if r_k is already defined for $k \leq n$, let $r_n^* > r_n$ be defined by

$$(11) \quad \log \mu(r_n^*) = \log \mu(r_n) + 1.$$

If $r_n^* \notin E_\delta$, put $r_{n+1} = r_n^*$. If however $r_n^* \in E_\delta$, then r_n^* is contained in one of the open intervals of E_δ ; in this case let r_{n+1} be the lower end-point and r_{n+2} the upper end-point of this interval.

The increasing sequence r_n defined in this way has the following properties:

a) $r_n \notin E_\delta$ for $n \geq 1$.

b) If the open interval (r_n, r_{n+1}) contains a number r not belonging to the set E_δ , then

$$\log \mu(r_{n+1}) = \log \mu(r_n) + 1.$$

c) $\log \mu(r_n) \geq [n/2]$ where $[n/2]$ denotes the integral part of $n/2$.

Now let us suppose that for some t one has for $n \geq n_0(t)$

$$(12) \quad M(r_n, t) \leq \frac{1}{3} \mu(r_n) (\log \mu(r_n))^{1/4} (\log \log \mu(r_n))^{1+\delta}.$$

As $M(r, t)$ and $\mu(r)$ are both increasing functions of r , it follows (in view of property b) of the sequence r_n) that for $n \geq n_0(t)$ and for $r_n < r < r_{n+1}$ and $r \notin E_\delta$ one has

$$M(r, t) \leq \frac{e}{3} \mu(r) (\log \mu(r) + 1)^{1/4} (\log (\log \mu(r) + 1))^{1+\delta},$$

and thus one can find an $n_1(t)$ such that

$$(13) \quad M(r, t) < \mu(r) (\log \mu(r))^{1/4} (\log \log \mu(r))^{1+\delta}$$

if $r \notin E_\delta(t)$ where $E_\delta(t)$ denotes the union of the set E_δ and the set $r \leq r_{n_1(t)}$.

Thus to prove our theorem it is sufficient to prove that for almost all values of t there exists a number $n_0(t)$ such that (12) holds for $n \geq n_0(t)$.

Now let us put

$$(14) \quad g(x) = \log f_1(e^x),$$

$$(15) \quad A(r) = g'(\log r) = \frac{\sum_{n=1}^{\infty} n |a_n| r^n}{f_1(r)}$$

and

$$(16) \quad B^2(r) = g''(\log r) = \frac{\sum_{n=1}^{\infty} n^2 |a_n| r^n}{f_1(r)} - A^2(r).$$

If ξ_r is a random variable such that⁽²⁾

$$(17) \quad \mathbf{P}(\xi_r = n) = \frac{|a_n| r^n}{f_1(r)} \quad (n = 0, 1, \dots)$$

then clearly $A(r)$ is the expectation and $B^2(r)$ the variance of ξ_r and thus by Chebishev's inequality one gets⁽³⁾ for every $T > 1$

$$(18) \quad \sum_{|n - A(r)| \geq B(r)T} |a_n| r^n \leq \frac{f_1(r)}{T^2}$$

and thus, choosing $T = (\log \mu(r))^{1/8} (\log \log \mu(r))^{(1+\delta)/2}$ we get from (10) for every $r \notin E_\delta$, putting

$$(19) \quad C(r) = B(r) (\log \mu(r))^{1/8} (\log \log \mu(r))^{(1+\delta)/2},$$

$$(20) \quad \sum_{|n - A(r)| \geq C(r)} |a_n| r^n \leq \mu(r) (\log \mu(r))^{1/4}.$$

Now, in Rosenbloom's proof of (4*) the set E_δ is defined as the set, on which $B^2(r) > (\log f_1(r)) (\log \log f_1(r))^{2+2\delta}$; thus for $r \notin E_\delta$ and $\delta < 1/4$, using again (10) we have

$$(21) \quad B^2(r) < 4 (\log \mu(r))^{1+\delta}$$

and therefore, in view of (20), we obtain, putting

$$(22) \quad C_1(r) = (\log \mu(r))^{3/4}$$

that

$$\sum_{|n - A(r)| \geq C_1(r)} |a_n| r^n < \mu(r) (\log \mu(r))^{1/4}.$$

(2) $\mathbf{P}(\dots)$ denotes the probability of the event in the brackets.

(3) This is the main step in Rosenbloom's proof of (4*).

It follows that for $r \notin E_\delta$

$$(23) \quad M(r, t) \leq \mu(r)(\log \mu(r))^{1/4} + \max_{0 \leq \varphi < 2\pi} \left| \sum_{|k-A(r)| < C_1(r)} a_k R_k(t) r^k e^{ik\varphi} \right|.$$

Now we need the following lemma:

LEMMA. Let $b_1, b_2, \dots, b_D$ ($D \geq e^{10}$) be arbitrary complex numbers, $\xi_1, \xi_2, \dots, \xi_D$ independent random variables, taking on the values ± 1 with probability $\frac{1}{2}$. Then, putting

$$S = \sum_{k=1}^D |b_k|^2$$

one has

$$(24) \quad \mathbf{P} \left(\max_{0 \leq \varphi < 2\pi} \left| \sum_{k=1}^D b_k \xi_k e^{ik\varphi} \right| > 2\sqrt{22S \log D} \right) \leq \frac{1}{D^4}.$$

Proof. The idea of the proof of this lemma is well known, and is due originally to S. Bernstein. Clearly, if $\gamma_1, \gamma_2, \dots, \gamma_D$ are arbitrary complex numbers, $\gamma_k = \alpha_k + i\beta_k$ for every $A > 0$ and $\varepsilon > 0$, in view of $|x + iy| \leq \sqrt{2} \max(|x|, |y|)$, one has

$$\mathbf{P} \left(\left| \sum_{k=1}^D \gamma_k \xi_k \right| > A \right) \leq 2\mathbf{P} \left(e^{\varepsilon \sum_{k=1}^D \alpha_k \xi_k} > e^{\frac{\varepsilon A}{\sqrt{2}}} \right) + 2\mathbf{P} \left(e^{\varepsilon \sum_{k=1}^D \beta_k \xi_k} > e^{\frac{\varepsilon A}{\sqrt{2}}} \right)$$

and thus, by the Markov inequality $\mathbf{P}(\zeta > B) \leq E(\zeta)/B$ (valid for $B > 0$ and for every nonnegative random variable ζ with finite expectation $E(\zeta)$),

$$\mathbf{P} \left(\left| \sum_{k=1}^D \gamma_k \xi_k \right| > A \right) \leq 2e^{-\frac{\varepsilon A}{\sqrt{2}}} [E(e^{\varepsilon \sum_{k=1}^D \alpha_k \xi_k}) + E(e^{\varepsilon \sum_{k=1}^D \beta_k \xi_k})]$$

where $E(\dots)$ denotes the expectation of the random variable in the brackets. Now clearly, using the inequality $\frac{1}{2}(e^x + e^{-x}) \leq e^{x^2/2}$,

$$E(e^{\varepsilon \sum_{k=1}^D \alpha_k \xi_k}) = \prod_{k=1}^D \left(\frac{e^{\varepsilon \alpha_k} + e^{-\varepsilon \alpha_k}}{2} \right) \leq e^{\frac{\varepsilon^2}{2} (\sum_{k=1}^D \alpha_k^2)}$$

and similarly

$$E(e^{\varepsilon \sum_{k=1}^D \beta_k \xi_k}) \leq e^{\frac{\varepsilon^2}{2} (\sum_{k=1}^D \beta_k^2)}$$

and thus

$$\mathbf{P} \left(\left| \sum_{k=1}^D \gamma_k \xi_k \right| > A \right) \leq 4e^{-\frac{\varepsilon A}{\sqrt{2}} + \frac{\varepsilon^2}{2} \sum_{k=1}^D |\gamma_k|^2}.$$

Choosing

$$A = \lambda \left(\sum_{k=1}^D |\gamma_k|^2 \right)^{1/2} \quad \text{and} \quad \varepsilon = \frac{\lambda}{\sqrt{2} \left(\sum_{k=1}^D |\gamma_k|^2 \right)^{1/2}}$$

it follows

$$(25) \quad \mathbf{P} \left(\left| \sum_{k=1}^D \gamma_k \xi_k \right| > \lambda \left(\sum_{k=1}^D |\gamma_k|^2 \right)^{1/2} \right) \leq 4e^{-\lambda^2/4}.$$

Now let us apply (25) for $\gamma_k = b_k e^{ik\varphi}$ with an arbitrary real value of φ ; it follows

$$(26) \quad \mathbf{P} \left(\left| \sum_{k=1}^D b_k \xi_k e^{ik\varphi} \right| > \lambda \sqrt{S} \right) \leq 4e^{-\lambda^2/4}.$$

Let us substitute in place of φ successively the values $\varphi_j = 2\pi j/N$ ($j = 0, 1, \dots, N-1$) where the positive integer N is defined by the inequality

$$(27) \quad \frac{2\pi D^{3/2}}{\lambda} \leq N < \frac{2\pi D^{3/2}}{\lambda} + 1.$$

It follows

$$(28) \quad \mathbf{P} \left(\max_{0 \leq j \leq N-1} \left| \sum_{k=1}^D b_k \xi_k e^{jk\varphi_j} \right| > \lambda \sqrt{S} \right) \leq 4 \left(\frac{2\pi D^{3/2}}{\lambda} + 1 \right) e^{-\lambda^2/4}.$$

On the other hand, if $\varphi_j \leq \varphi < \varphi_{j+1}$

$$(29) \quad \left| \sum_{k=1}^D b_k \xi_k e^{ik\varphi} - \sum_{k=1}^D b_k \xi_k e^{ik\varphi_j} \right| \leq \lambda \sqrt{S}.$$

From (28) and (29), putting $\lambda = \sqrt{22 \log D}$, we obtain (24).

Let us now apply the lemma to the estimation of the second term on the right of (23). As the Rademacher functions are independent with respect to the Lebesgue measure and take on the values ± 1 with probability $\frac{1}{2}$, and for $r \notin E_\delta$

$$(30) \quad \sum_{|k-A(r)| < C_1(r)} |a_k|^2 r^{2k} \leq \sum_{k=0}^{\infty} |a_k|^2 r^{2k} \leq \mu^2(r) (\log \mu(r))^{1/2} (\log \log \mu(r))^{1+\delta},$$

it follows for $r \notin E_\delta$ (denoting by $V(\dots)$ the Lebesgue measure of the set of values of t for which the condition in the brackets holds), and, taking (22) into account, that, if r is sufficiently large,

$$(31) \quad \mathbf{P} \left(\max_{0 \leq \varphi < 2\pi} \left| \sum_{|k-A(r)| < C_1(r)} a_k r^k R_k(t) e^{ik\varphi} \right| \geq \frac{1}{3} \mu(r) (\log \mu(r))^{1/4} (\log \log \mu(r))^{1+\delta} \right) \leq \frac{1}{2^8 (\log \mu(r))^3}.$$

Now let us apply (31) for $r = r_n$. It follows that denoting by A_n the set of those t for which

$$(32) \quad \max_{0 \leq \varphi < 2\pi} \left| \sum_{|k - A(r_n)| < C_1(r_n)} a_k r_n^k R_k(t) e^{ik\varphi} \right| > \frac{1}{2} \mu(r_n) (\log \mu(r_n))^{1/4} (\log \log \mu(r_n))^{1+\delta}$$

in view of property c) of the sequence r_n

$$\sum_{n=1}^{\infty} V(A_n) < +\infty.$$

Thus by the Borel-Cantelli lemma, for almost all values of t ($0 \leq t \leq 1$) the inequality (32) can hold only for a finite number of values of n . Thus with respect to (23) for almost all t (12) holds for $n \geq n_0(t)$.

As was pointed out earlier, this proves our theorem.

As mentioned above, our result is best possible as regards the exponent of $\log \mu(r)$; however, it is not best possible as regards the exponent of $\log \log \mu(r)$. For instance for the case of $f(z) = e^z$ one can prove more, namely that there exist positive constants c_1 and c_2 such that for almost all values of t one has⁽⁴⁾

$$(33) \quad c_1 \leq \limsup_{r \rightarrow \infty} \frac{M(r, t)}{\mu(r) (\log \mu(r))^{1/4} (\log \log \mu(r))^{1/2}} \leq c_2.$$

To prove the lower inequality of (33), one needs the results of R. Salem and A. Zygmund contained in their paper [3], dedicated to Professor Steinhaus at his 65th birthday.

To get the upper inequality of (33) one has to notice that the proof of Theorem 1 yields also the following result, which is slightly stronger than Theorem 1.

THEOREM 2. *Let $f(z)$ be an arbitrary entire function, having the power series (1). Let $\mu(r)$ be defined by (3) and put*

$$(34) \quad S^2(r) = \sum_{n=1}^{\infty} |a_n|^2 r^{2n}$$

Let $f(z, t)$ be defined by (6) and $M(r, t)$ by (7). Then for almost all t and for $r \notin E_\delta(t)$ where $E_\delta(t)$ is a set of finite logarithmic measure, one has

$$(35) \quad M(r, t) < c_3 S(r) (\log \log \mu(r))^{1/2}$$

where $c_3 > 0$ is a constant, not depending on r or t .

REMARK. For the case $f(z) = e^z$ we have $S(r) = O(e^r/r^{1/4})$ and $\log \mu(r) \sim r$, and thus we get for almost all t

$$(36) \quad M(r, t) < c_4 \frac{e^r \sqrt{\log r}}{\sqrt[4]{r}} \quad \text{for } r \notin E_\delta(t).$$

⁽⁴⁾ In what follows $c_1, c_2, c_3, \dots$ denote positive constants, not depending on r or t , but they may depend on the function $f(z)$ considered.

Moreover in this case the set $E_\delta(t)$ is an interval $0 \leq r \leq r_1(t)$. Thus the upper inequality of (33) follows. We can write (33) also in the form: for almost all t

$$(37) \quad 0 < c_5 \leq \limsup_{r \rightarrow \infty} \frac{M(r, t) \sqrt[4]{r}}{e^r \sqrt{\log r}} \leq c_6$$

where c_5 and c_6 are positive constants.

Note that (37) is sharper than the corresponding statement in [3].

Proof of Theorem 2. The proof of Theorem 2 follows that of Theorem 1 step by step, only instead of estimating $S^2(r)$ as in (30) we express our result in terms of $S(r)$. As by (30) we have for $r \notin E_\delta$

$$S(r) < \mu(r) (\log \mu(r))^{1/4} (\log \log \mu(r))^{(1+\delta)^2}$$

it is clear that Theorem 1 is contained in Theorem 2.

Using the mentioned results of Salem and Zygmund one can prove that for all those entire functions $f(z)$ for which there exists an $\varepsilon > 0$ such that

$$(38) \quad S(r) \geq \mu(r) (\log \mu(r))^\varepsilon \quad \text{for} \quad r \geq c_7$$

one has for almost all t

$$(39) \quad \limsup_{r \rightarrow \infty} \frac{M(r, t)}{S(r) (\log \log \mu(r))^{1/2}} \geq c_8 > 0.$$

It should be however mentioned that (39) does not mean that the statement of Theorem 2 cannot be improved for those functions $f(z)$ for which (38) is valid, because (39) does not exclude the possibility that those values of r for which

$$\frac{M(r, t)}{S(r) (\log \log \mu(r))^{1/2}} > c > 0$$

are contained in a set of finite logarithmic measure. However, by restricting ourselves to the class of those entire functions for which the statement of Wiman's theorem is valid for sufficiently large values of r , our result is best possible.

Thus the following result is valid:

THEOREM 3. *Let $f(z)$ be an entire function with the power series (1) such that defining $M(r)$ by (2) and $\mu(r)$ by (3) one has for some $c_9 > 0$ and $c_{10} > 0$*

$$M(r) < c_9 \mu(r) (\log \mu(r))^{c_{10}}$$

for all $r \geq 1$. Let $S(r)$ be defined by (34) and suppose that (38) holds. Let $f(z, t)$ be defined by (6) and $M(r, t)$ by (7). Then for almost all values of t we have

$$(40) \quad c_{11} \leq \limsup_{r \rightarrow \infty} \frac{M(r, t)}{S(r)(\log \log \mu(r))^{1/2}} \leq c_{12}.$$

REMARK 1. Clearly Theorem 3 includes our statement (37) about the function e^z , as all the assumptions of Theorem 3 are satisfied for $f(z) = e^z$.

REMARK 2. Let us point out that there exist entire functions, having a lacunary power series such that $M(r)/\mu(r)$ is bounded; for such functions for all values of t $M(r, t)/\mu(r)$ is of course bounded too.

Finally we should like to mention that our results remain valid if instead of the Rademacher functions we multiply the terms of the series (1) by the Steinhaus-functions, i.e. by the functions $e^{2\pi i \vartheta_n(t)}$ where $\vartheta_1(t), \dots, \vartheta_n(t), \dots$ are independent functions, uniformly distributed in the interval $(0, 1)$.

REMARK ADDED IN PROOF. The random entire functions obtained by using Steinhaus factors have been studied first by P. Lévy (*Sur la croissance des fonctions entières*, Bull. Soc. Math. France 58 (1930), pp. 29-59, 127-149), who has proved for a class of entire functions, the coefficients of which satisfy certain conditions of regularity, the inequality corresponding to (35). The class considered by P. Lévy includes the function e^z . Thus the inequality corresponding to (36) (if instead of random signs Steinhaus factors are used) is due to P. Lévy who conjectured also for this variant of the problem that the lower inequality of (37) holds.

References

- [1] P. Erdős *On the uniform but not absolute convergence of power series with gaps*, Ann. Soc. Polon. Math. 25 (1952), pp. 162-168.
- [2] P. C. Rosenbloom, *Probability and entire functions*, in "Studies in Mathematical analysis and related topics, Essays in honor of G. Pólya", Stanford University Press, Stanford 1962, pp. 325-332.
- [3] R. Salem and A. Zygmund, *Some properties of trigonometric series whose terms have random signs*, Acta Mathematica 91 (1954), pp. 245-301.
- [4] H. Steinhaus, *Über die Wahrscheinlichkeit dafür, dass der Konvergenzkreis einer Potenzreihe ihre natürliche Grenze ist*, Math. Zeitschr. 31 (1930), pp. 408-416.

NOTE

This paper constitutes one of the first developments concerning the Wiman—Valiron method initiated by the beautiful paper of P. C. Rosenbloom entitled "Probability and entire functions" from 1962. Another important one is the extension of Wiman—Valiron's results to entire functions of several complex variables by A. Schumitzky from 1965 (unpublished so far). (P. T.)

MEASURES IN DENUMERABLE SPACES

H. HANISCH, City College of New York, W. M. HIRSCH, Courant Institute,
New York City, and A. RENYI, Hungarian Academy of Sciences.

1. Introduction. The purpose of this paper is essentially didactic: to call attention to and make explicit certain properties of measures on denumerable spaces (i.e., spaces with a denumerable number of points) that justify the conventional treatment of such spaces in probability texts. After our results were obtained we discovered that the main one could be derived easily from some theorems of Boolean algebra. Since our theorems have not, to our knowledge, been previously pointed out, and since our proofs are in a measure-theoretic setting that requires no knowledge of Boolean algebra, we have been motivated to contribute this note.

By a *ring* $\mathcal{R}$ of subsets of a space Ω is meant a nonempty class of subsets that is closed under finite union and difference. If $\mathcal{R}$ is closed under countable union, it is called a σ -ring. The terms *algebra* and σ -*algebra* refer, respectively, to rings and σ -rings containing the space Ω . The sets in a ring $\mathcal{R}$ are called $\mathcal{R}$ -*measurable*. We use the term *measure* to mean an extended real-valued, nonnegative, countably-additive set function defined on a ring.

The *power set*, $\mathcal{P}(\Omega)$, is the σ -algebra of all subsets of Ω . A measure μ is called *continuous* if each singleton set A is measurable, and $\mu(A) = 0$ for all singletons. The *trivial measure* is the measure on $\mathcal{P}(\Omega)$ that vanishes identically. The symbol " $\emptyset$ " denotes the empty set.

Our results fill a small gap in the literature on measure theory concerning the possibility of extending a measure from a given σ -ring to the power set.

Let $\mathfrak{M}$ denote the family of all measures on all σ -rings of an arbitrary space Ω , and let $\mathfrak{N}$ denote the family of all measures on $\mathcal{P}(\Omega)$. It may happen that each measure in $\mathfrak{M}$ is the restriction of at least one measure in $\mathfrak{N}$, or loosely speaking, that the class of all measures on all σ -rings is no richer than the class of all measures on the power set. In this case we shall say that Ω , or more precisely the cardinal number of Ω , has the *full extension property*; it is clear that either all sets of the same cardinality have the full extension property or none do. It is evident also that if a cardinal $\aleph$ fails to have the full extension property, so does every cardinal $\aleph^*$ with $\aleph^* > \aleph$. (This is also true if " σ -ring" is replaced

by " σ -algebra" in the formulation of the notion of full extension property.)

Ulam [7] has shown that the only real-valued continuous measure on the power set of a space whose cardinality is less than the first weakly inaccessible cardinal is the trivial one. (A cardinal number $\aleph_\alpha$ is called weakly inaccessible if (a) $\aleph_\alpha > \aleph_0$, (b) α is a limit ordinal, (c) $\aleph_\alpha$ is not the sum of fewer than $\aleph_\alpha$ numbers each of which is less than $\aleph_\alpha$.) Hence, in particular, if the cardinality of Ω is $\aleph_1$, $\mathcal{P}(\Omega)$ cannot carry a nontrivial continuous measure. On the other hand, an example in Sect. 2 demonstrates the existence of a space Ω of cardinality $\aleph_1$ which has a σ -algebra $\mathcal{F}$ of subsets containing all singletons and a nontrivial continuous probability measure μ on $\mathcal{F}$. By Ulam's Theorem μ cannot be extended to $\mathcal{P}(\Omega)$, so that $\aleph_1$ and hence all greater cardinals fail to have the full extension property. Intuitively it seems clear that if $\text{card } \Omega \leq \aleph_0$, all measures on sub- σ -rings of $\mathcal{P}(\Omega)$ should be compatible with the assignments of masses to points, and thus that $\aleph_0$ should have the full extension property. We shall show that this is so in Section 3. The connection between our results and Boolean algebra is described in Section 4. The implications for probability theory are discussed in Section 5.

2. An example of a nonextendible measure. Let α be any ordinal greater than zero, and let Ω_α denote the set of all ordinal numbers less than α . Let α^* denote the smallest ordinal α such that Ω_α is uncountable. Then the cardinal number of Ω_{α^*} is $\aleph_1$.

We shall call a set $A \subset \Omega_{\alpha^*}$ a cosection if there exists a number $\beta \in \Omega_{\alpha^*}$ such that $\alpha > \beta$ implies $\alpha \in A$. It is not difficult to verify from well-known properties of Ω_{α^*} ([2], p. 29) that the class of sets $\mathcal{F}$ consisting of all cosections and their complements is a σ -algebra. Moreover, the function

$$\mu: \mathcal{F} \rightarrow [0, 1]$$

defined by setting

$$\mu(A) = \begin{cases} 1, & \text{if } A \text{ is a cosection} \\ 0, & \text{if } A^c \text{ is a cosection} \end{cases}$$

is a probability measure which, by Ulam's Theorem, cannot be extended to $\mathcal{P}(\Omega_{\alpha^*})$. We therefore have the following result:

THEOREM 2.1. *If $\text{card } \Omega \geq \aleph_1$, Ω does not have the full extension property.*

3. Structure of σ -rings and measures in a countable space. As is shown in Theorem 3.1, every σ -ring of subsets of a countable space has a particularly simple structure, an important feature of which is implied by the following lemma:

LEMMA 3.1. *Let Ω be a space containing a countable number of points. If $\mathcal{F}$ is a nonempty class of subsets of Ω closed under countable union or countable intersection, then $\mathcal{F}$ is closed, respectively, under arbitrary union or intersection.*

Proof. We give the proof only for the case of intersections; the proof for unions is similar.

Suppose that $\mathfrak{F}$ is closed under countable intersection. Let $\mathcal{C} \subset \mathfrak{F}$ be an arbitrary class of sets and put

$$D = \bigcap_{A \in \mathcal{C}} A.$$

Consider the complementary set D^c . If D^c is empty, then $\mathcal{C}$ is the class whose only member is Ω , so that $D \in \mathfrak{F}$.

If D^c is not empty, to each $\omega \in D^c$ there corresponds a set A_ω^c such that $\omega \in A_\omega^c$ and $A_\omega^c \in \mathcal{C}$. Let

$$E = \bigcap_{\omega \in D^c} A_\omega^c;$$

plainly $E \supset D$. Since D^c is countable and $A_\omega^c \in \mathcal{C}$, we have $E \in \mathfrak{F}$. Noting that

$$\omega \in D^c \Rightarrow \omega \in A_\omega^c \Rightarrow \omega \in E^c,$$

that is, $D \supset E$, we conclude that $D = E \in \mathfrak{F}$.

Now let $\mathcal{R}$ denote a σ -ring of subsets of a countable space Ω . We define a binary relation " $\sim$ " on Ω by setting

$$\omega \sim \omega'$$

if and only if every set in $\mathcal{R}$ that contains ω' also contains ω . It is clear from the definition that this relation is reflexive and transitive; it follows from the properties of $\mathcal{R}$ that the relation is also symmetric. For suppose that $\omega \sim \omega'$ but

$$\omega' \not\sim \omega.$$

Then there exists a set $A \in \mathcal{R}$ such that $\omega \in A$ and $\omega' \notin A$. Setting $\Omega_{\mathcal{R}} = \bigcup_{E \in \mathcal{R}} E$, it follows from Lemma 3.1 that $\Omega_{\mathcal{R}} \in \mathcal{R}$. Hence

$$\Omega_{\mathcal{R}} - A \in \mathcal{R},$$

$$\omega' \in \Omega_{\mathcal{R}} - A,$$

and $\omega \notin \Omega_{\mathcal{R}} - A$, which contradicts the relation $\omega \sim \omega'$.

Thus " $\sim$ " is an equivalence relation on Ω . Plainly $\omega \sim \omega'$ if and only if $\omega \in \bigcap_{A \in \mathcal{R}} A$. Hence we have proved:

LEMMA 3.2. *The equivalence class, $[\omega']$, of ω' is given by $[\omega'] = \bigcap_{A \in \mathcal{R}} A$.*

It follows from Lemmas 3.1 and 3.2 that the class of sets $\{[\omega'] : \omega' \in \Omega_{\mathcal{R}}\}$ is a measurable partition of $\Omega_{\mathcal{R}}$, i.e., one in which each set is in $\mathcal{R}$.

An *atom* of a ring $\mathcal{R}$ of sets is a nonempty, $\mathcal{R}$ -measurable set A whose only $\mathcal{R}$ -measurable subsets are A and $\emptyset$. The theorem below shows that a σ -ring in a countable space is generated by its atoms.

THEOREM 3.1. *If Ω is countable and $\mathcal{R}$ is an arbitrary σ -ring of subsets of Ω , there exists a countable, measurable partition of $\Omega_{\mathcal{R}}$ into atoms. The atoms are just the equivalence classes $[\omega]$, $\omega \in \Omega_{\mathcal{R}}$, and each $\mathcal{R}$ -measurable set A is the union of the atoms contained in A .*

Proof. Suppose there is a point $\omega \in \Omega_{\mathcal{R}}$ and a set $B \in \mathcal{R}$ such that B is a non-empty, proper subset of $[\omega]$. Then there are equivalent points $\omega' \in B$ and $\omega'' \in [\omega] - B$, which contradicts the definition of equivalence.

Thus the sets $[\omega]$, $\omega \in \Omega_{\mathcal{R}}$, are atoms which form a measurable partition of $\Omega_{\mathcal{R}}$; plainly there are no other atoms. To complete the proof we note that $B \in \mathcal{R}$ implies

$$B = B \cap \Omega_{\mathcal{R}} = B \cap \bigcup_{\omega \in \Omega_{\mathcal{R}}} [\omega] = \bigcup_{\omega \in \Omega_{\mathcal{R}}} B \cap [\omega] = \bigcup_{[\omega] \subset B} [\omega],$$

since $B \cap [\omega] = [\omega]$ if $[\omega] \subset B$ and is empty otherwise.

Let $\mathcal{F}$ and $\mathcal{F}^*$ be σ -algebras of subsets of spaces Ω and Ω^* , respectively. We shall say that $\mathcal{F}$ and $\mathcal{F}^*$ are isomorphic if there exists a 1:1 mapping ϕ of $\mathcal{F}$ onto $\mathcal{F}^*$ that preserves countable unions and complements, i.e.,

$$(a) \quad \phi\left(\bigcup_{i=1}^{\infty} A_i\right) = \bigcup_{i=1}^{\infty} \phi(A_i),$$

$$(b) \quad \phi(A^c) = (\phi(A))^c.$$

It follows easily from (a) and (b) that ϕ also preserves countable intersections, differences, and set inclusion. We can now state the following corollary to Theorem 3.1:

COROLLARY. *If Ω is countable, any σ -algebra $\mathcal{F}$ of subsets of Ω is isomorphic to the σ -algebra $\mathcal{F}^*$ of all subsets of the set Ω^* of all atoms of $\mathcal{F}$.*

Proof. We should like to emphasize that each point $\omega^* \in \Omega^*$ is a subset of Ω . Thus if A is a subset of Ω and A^* is a subset of Ω^* , ω^* can bear the relation of inclusion to A and the relation of membership to A^* . With this in mind, we define a mapping

$$\phi: \mathcal{F} \rightarrow \mathcal{F}^*$$

by setting, for $A \in \mathcal{F}$, $\phi(A) = \{\omega^* \in \Omega^*: \omega^* \subset A\}$.

The mapping ϕ is "onto" since, if $A^* \in \mathcal{F}^*$, then the set A defined by

$$A = \left(\bigcup_{\omega^* \in A^*} \omega^* \right) \in \mathcal{F}$$

has the property

$$\phi(A) = A^*.$$

Moreover, ϕ is 1:1; for if $A \in \mathcal{F}$, $B \in \mathcal{F}$, $A \neq B$, there exists a point ω in one of the

sets that is not in the other, say $\omega \in A$, $\omega \notin B$. Then $[\omega] \subset A$ and $[\omega] \subset B^c$, so that $\phi(A) \neq \phi(B)$.

To show that ϕ preserves countable unions, it suffices to note that for any sequence $A_1, A_2, \dots$ of $\mathfrak{F}$ -measurable sets,

$$\phi(A_i) = \{[\omega]: \omega \in A_i\}$$

and

$$\phi\left(\bigcup_{i=1}^{\infty} A_i\right) = \{[\omega]: \omega \in \bigcup_{i=1}^{\infty} A_i\} = \bigcup_{i=1}^{\infty} \{[\omega]: \omega \in A_i\} = \bigcup_{i=1}^{\infty} \phi(A_i).$$

Similarly the relation

$$\begin{aligned}\phi(A^c) &= \{[\omega]: \omega \in A^c\} = \{[\omega]: \omega \in \Omega\} - \{[\omega]: \omega \in A\} \\ &= \phi(\Omega) - \phi(A) = \Omega^* - \phi(A) = (\phi(A))^c\end{aligned}$$

shows that ϕ preserves complements. Thus $\mathfrak{F}$ and $\mathfrak{F}^*$ are isomorphic.

It follows easily from Theorem 3.1 that $\mathfrak{N}_0$ has the full extension property. For completeness the argument is given below.

THEOREM 3.2. *Let Ω be a countable set, $\mathfrak{A}$ a σ -ring of subsets, and μ an arbitrary measure on $\mathfrak{A}$. There exists a measure μ^* on the class of all subsets of Ω whose restriction to $\mathfrak{A}$ is μ .*

Proof. For each equivalence class $[\omega]$, $\omega \in \Omega_{\mathfrak{A}}$, let $p_{[\omega]}: [\omega] \rightarrow \bar{\mathbb{R}}_+$ be any function such that

$$\sum_{\alpha \in [\omega]} p_{[\omega]}(\alpha) = \mu([\omega]).$$

Assume that $\Omega_{\mathfrak{A}} = \Omega$. Let $p: \Omega \rightarrow \bar{\mathbb{R}}_+$ be the mapping whose restriction to $[\omega]$ is $p_{[\omega]}$ for all $\omega \in \Omega$. For each set $A \subset \Omega$ define

$$\mu^*(A) = \sum_{\omega \in A} p(\omega).$$

Clearly $\mu^*: \mathcal{P}(\Omega) \rightarrow \bar{\mathbb{R}}_+$ is a measure and $\mu^*([\omega]) = \mu([\omega])$, $\omega \in \Omega$. More generally, for $B \in \mathfrak{A}$ we have from Theorem 3.1,

$$\mu^*(B) = \mu^*\left(\bigcup_{[\omega] \subset B} [\omega]\right) = \sum_{[\omega] \subset B} \mu^*([\omega]) = \sum_{[\omega] \subset B} \mu([\omega]) = \mu(B).$$

If $\Omega_{\mathfrak{A}} \neq \Omega$, we define p on $\Omega_{\mathfrak{A}}$ as before and define it arbitrarily on $\Omega - \Omega_{\mathfrak{A}}$.

4. Related theorems of Boolean algebra. Let $\mathfrak{A}$ be a Boolean algebra and let m be an infinite cardinal. $\mathfrak{A}$ is said to be *m-complete* if for every indexed family $\{A_i\}_{i \in T}$, where $\text{card } T = m$ and $A_i \in \mathfrak{A}$, the join $\bigcup_{i \in T} A_i$ exists in $\mathfrak{A}$. This is equivalent to the condition that for every m -indexed family $\{A_i\}_{i \in T}$, the meet $\bigcap_{i \in T} A_i$ exists in $\mathfrak{A}$. If $\mathfrak{A}$ is an m -complete Boolean algebra for every m , then $\mathfrak{A}$ is said to be a *complete* Boolean algebra. (For the definitions of

Boolean algebra, infinite joins, and infinite meets, see [4].) A Boolean algebra $\mathcal{A}$ is said to satisfy the *m-chain condition* provided that every set of disjoint elements in $\mathcal{A}$ has cardinality $\leq m$. (Since an algebra of sets may be viewed as a Boolean algebra, the terminology introduced in this section may also be applied to algebras of sets.)

In this terminology, Lemma 3.1 of the previous section has an obvious corollary.

COROLLARY TO LEMMA 3.1. *A σ -algebra of subsets of a countable space is a complete Boolean algebra.*

It is interesting to note that this corollary is a special case of a much more general theorem of Boolean algebra due to Tarski.

THEOREM (Tarski). *Every m -complete Boolean algebra $\mathcal{A}$ satisfying the m -chain condition is a complete Boolean algebra.*

For a detailed proof of this theorem the reader is referred to [4, 5]. The proof rests on the inductively proved fact that if the join $\bigcup_{i \in I} A_i$ exists for any m -indexed set $\{A_i\}_{i \in I}$ of disjoint elements of a Boolean algebra $\mathcal{A}$, then $\mathcal{A}$ is m -complete. Under the hypothesis of Tarski's Theorem it is evident that the join of any indexed set of disjoint elements exists.

Since a σ -algebra of subsets of a countable space is not only $\aleph_0$ -complete but also satisfies the $\aleph_0$ -chain condition, the corollary to Lemma 3.1 is a special case of Tarski's Theorem.

Our Theorem 3.1 also has a more general Boolean algebra counterpart. An element $A \neq 0$ of a Boolean algebra $\mathcal{A}$ is said to be an *atom* of $\mathcal{A}$ if for every $B \in \mathcal{A}$ the inclusion

$$B \subset A$$

implies that either $B = 0$ or $B = A$. A Boolean algebra is called *atomic* if for every element $A \neq 0$ there exists an atom $B \subset A$. The following theorem, due to Lindenbaum and Tarski [4, 6], relates completeness to atomicity:

THEOREM (Lindenbaum and Tarski). *A complete Boolean algebra $\mathcal{A}$ is isomorphic to a complete algebra of sets if and only if $\mathcal{A}$ is atomic. In this case $\mathcal{A}$ is isomorphic to the algebra of all subsets of the set of all atoms of $\mathcal{A}$.*

Two Boolean algebras are called *isomorphic* if there exists a 1:1 mapping of one onto the other that preserves binary join and complement.

Since, as we have seen, a σ -algebra of subsets of a countable space is complete, it follows from the Theorem of Lindenbaum and Tarski that it is atomic. It is evident that the atoms of a Boolean algebra are disjoint. Hence, there are only countably many atoms in a σ -algebra of subsets of a countable space Ω . Clearly the union of these atoms is Ω , so that they form a countable, measurable partition of the space.

5. Implications for probability theory. In the Kolmogorov formulation of the axioms of probability, the mathematical description of a random experiment $\mathcal{E}$ consists of a triple $(\Omega, \mathcal{F}, P)$, where Ω is a set, $\mathcal{F}$ is a σ -algebra of subsets of Ω , and $P: \mathcal{F} \rightarrow [0, 1]$ is a probability measure. In applications of the Kolmogorov model each point in Ω is interpreted as a possible "primary" or "indecomposable" outcome of $\mathcal{E}$, and each set $A \in \mathcal{F}$ is interpreted as the event that "the outcome of $\mathcal{E}$ is one of the points in A ." Thus the intuitive notion of event is formalized as a set and, moreover, it is postulated that the only events of $\mathcal{E}$ to which probabilities are associated are the sets in $\mathcal{F}$. These probabilities are given, of course, by the measure P .

In this approach any σ -algebra of subsets of Ω is admissible as an event class; in particular, for example, it is not required that the singleton sets themselves be events, despite the fact that each point is intuitively thought of as a possible outcome. Keeping this intuitive interpretation of the points of Ω in mind, it is natural for the student of probability to wonder why an arbitrary subset of Ω should not be regarded as a possible event to which a probability is attached. Indeed, from the point of view of the scientist or engineer interested in applications, the definition of an event as a member of a distinguished σ -algebra of subsets may seem decidedly unnatural. Certainly the problem of justifying it is faced by every teacher of probability.

One argument, which we shall not elaborate here, rests on a distinction between events and observable events [3]. This argument gives an intuitive interpretation of the fact that probability is not defined for all events, only for observable events. However, a purely mathematical argument can also be given, based on the theorems proved in the previous section. Although in every application of probability the governing probability measure must satisfy the axioms of probability, i.e., be ≥ 0 , countably additive, and have $P(\Omega) = 1$, each application typically involves its own additional set of conditions, conditions dictated by a combination of empirical and theoretical considerations peculiar to the particular application; these additional restrictions may, in a certain sense, clash with the general probability axioms.

Consider, for example, the idealized experiment of making an infinite sequence of tosses of a coin. Suppose that each toss is made independently of the others and that the tosses are made under identical conditions. A possible outcome of this experiment is an infinite sequence of heads and tails such as

$$H, T, T, T, H, T, H, H, \dots,$$

where H stands for head and T for tail. The sample space Ω for this experiment may be taken to be the collection of all infinite sequences of H 's and T 's. Let p , $0 < p < 1$, denote the probability of head in a single toss. The set of all sequences having exactly k H 's among the first n coordinates corresponds to the event that exactly k heads occurred among the first n tosses, and elementary probabilistic considerations lead to the conclusion that to this set of sequences we should associate the probability $\binom{n}{k} p^k (1-p)^{n-k}$. It can be shown that this

assignment of probabilities leads to a unique probability measure on the ring of all subsets of Ω determined by conditions on a finite number of coordinates. (A set A is said to be determined by conditions on a finite number of coordinates if there exists an integer n such that for each point ω in Ω the first n coordinates of ω determine whether or not ω is in A .) It is evident that the singleton sets do not belong to the ring of sets to which we have thus far attached probabilities. Suppose now that we try to extend the probability measure we have defined to some σ -algebra of subsets of Ω containing all the singletons. Consider the singleton set whose only member is the point $(H, H, H, \dots)$. For every integer n , this event is contained in the event " n heads in the first n tosses." Since probability is monotonic, it follows that the probability of the singleton is, for every n , less than or equal to p^n . This implies that the probability of the singleton is zero. A similar argument leads to the conclusion that each singleton set must have probability zero. Thus, if we could extend the probability measure we originally defined to some σ -algebra containing all of the singleton sets, the extended probability measure would have to be continuous. Since the cardinality of the space under consideration is that of the continuum, it follows from Ulam's Theorem [7], under the continuum hypothesis, that $\mathcal{P}(\Omega)$ cannot carry a nontrivial continuous measure. (This was also shown independently by Banach and Kuratowski [1].) Yet physical considerations dictate that each singleton in Ω must have probability zero. Hence, if the probability model is to be faithful to the physical situation, it is impossible in the present example to define an event to be an arbitrary subset of Ω . (At least this is so if the continuum hypothesis is adopted as an axiom of set theory. Even if it is not, if the question of whether or not $\mathcal{P}(\Omega)$ can carry a nontrivial continuous measure is decidable from the other axioms of set theory, it must be decided in the negative, since this is the conclusion when the continuum hypothesis is used.) It is, of course, possible to define a continuous measure on the σ -algebra generated by the ring with which we started, which is done in the usual treatment of this problem in probability theory. By restricting the notion of event to such a σ -algebra, we obtain a model that fits the physical situation at the price of seeming artificiality in the definition of event. This example illustrates the fact that the class of probability measures on arbitrary σ -algebras in a space whose cardinality is that of the continuum is more useful than measures obtained by restriction from the power set. Hence, the decisive advantage of Kolmogorov's definition of event is that it leads to a larger and more useful class of probability spaces than would result from defining an event to be an arbitrary subset of a sample space.

The treatment of countable spaces in probability is in striking contrast to that of uncountable spaces. In the former case it is assumed invariably that the event class is the power set of the sample space. There appears to be no justification for this in the literature other than the fact that the procedure of assigning probabilities to all singletons leads in a simple way to a measure on the power set. Yet how can we be sure that we shall not encounter an experiment in which the sample space is countable and the conditions associated with the experi-

ment are incompatible with all measures arising from point masses? The assurance is given by Theorem 3.2 which shows that the class of all measures on all σ -algebras of subsets of a countable space is no richer than the class of measures on the power set, i.e., the class arising from point masses.

Another way of viewing the situation in the countable case is suggested by the corollary to Theorem 4.1, which shows that no theory in which events are defined as elements of an arbitrary σ -algebra can be more general than one in which events are defined as members of the power set; for each σ -algebra $\mathcal{F}$ of subsets of a countable space is isomorphic to the power set $\mathcal{O}$ of some space, so that a mathematical model involving $\mathcal{F}$ can be replaced by one involving $\mathcal{O}$. In the countable case, therefore, the definition of an event as an arbitrary subset of the sample space is not only natural but correct.

The work of the second author was supported by the Office of Naval Research, Contract Nonr-285(38). Reproduction in whole or in part is permitted for any purpose of the United States Government.

References

1. S. Banach and C. Kuratowski, Sur une généralisation du problème de la mesure, *Fund. Math.*, 14 (1929) 128-131.
2. E. Hewitt and K. Stromberg, *Real and Abstract Analysis*, Springer-Verlag, New York, 1965.
3. A. Rényi, *Lectures on Probability*, Stanford University, Summer, 1966 (Mimeographed).
4. R. Sikorski, *Boolean Algebras*, Springer, Berlin, 1960.
5. A. Tarski, Über additive und multiplikative Mengenkörper und Mengenfunktionen, *C. R. Soc. Sci. Lettr. Varsovie, Cl. III.* 30 (1937) 151-181.
6. ———, Zur Grundlegung der Booleschen Algebra, *Fund. Math.*, 24 (1935) 177-198.
7. S. Ulam, Zur Masstheorie in der allgemeinen Mengenlehre, *Fund. Math.*, 16 (1930) 140-150.

On some problems of statistics from the point of view of information theory

by

A. Rényi

Math. Inst. of the Hung. Acad. of Sci, Budapest, Hungary

We consider the following basic problem of (Bayesian) statistics: the statistician is interested in the value of a random variable θ , called the parameter; he is however not in the position to observe θ directly, he can observe only the value of another - vector-valued - random variable ξ , called the statistic. In case θ and ξ are not independent, the observed value of ξ contains a certain amount $I(\theta, \xi)$ of information concerning θ . In what follows we shall consider only the case when the set $\Gamma = \{\theta_1, \dots, \theta_r\}$ of possible values of θ is finite. In this case $I(\theta, \xi)$ is defined by the well-known formula

$$(0.1) \quad I(\theta, \xi) = H(\theta) - R(\theta|\xi)$$

where $H(\theta)$ is the entropy of θ , i. e.

$$(0.2) \quad H(\theta) = \sum_{k=1}^r p_k \log_2 \frac{1}{p_k}$$

where $p_k = P(\theta = \theta_k)$, and $R(\theta|\xi)$ is the (average) amount of information on θ still missing after having observed ξ ; $R(\theta|\xi)$ is defined as the expectation of the conditional entropy of θ given, ξ , i. e.

$$(0.3) \quad R(\theta|\xi) = E\left(\sum_{k=1}^r p_k(\xi) \log_2 \frac{1}{p_k(\xi)}\right)$$

where

$$(0.4) \quad p_k(\xi) = P(\theta = \theta_k | \xi) \quad (k = 1, 2, \dots, r)$$

is the conditional probability of the event $\theta = \theta_k$ given ξ . After having observed ξ the statistician has to make a decision, that is he has to select, on the basis of the information contained in the observation of ξ , one of the possible values of θ . Thus a decision is a (Borel-measurable) function $d(\xi)$ of ξ , with values in the set Γ . The error $e(d)$ of a decision is defined as the probability of the decision being false, i. e.

$$(0.5) \quad e(d) = P(d(\xi) \neq \theta).$$

It is known (this is essentially the Bayesian variant of the fundamental lemma of Neyman and Pearson, see [1] and [17]) that the error of the decision d is minimal if d is the standard decision Δ consisting in choosing that value of θ the posterior (conditional) probability of which (given ξ) is maximal. (In case there is more than one such value, any rule (random or not) of choosing one among them will do.)

Let $R(\theta|\Delta)$ denote the amount of information on θ missing if from the observation of ξ only the value of the standard decision $\Delta(\xi)$ is utilized; by other words, $R(\theta|\Delta)$ is the expectation of the conditional entropy of θ given the value of Δ .

Now one can show that the following inequalities are valid:

$$(0.6) \quad \log_2 \frac{1}{1 - e(\Delta)} \leq R(\theta|\xi) \leq R(\theta|\Delta) \leq h(e(\Delta)) + e(\Delta) \log_2(r-1)$$

where

$$h(x) = x \log_2 \frac{1}{x} + (1-x) \log_2 \frac{1}{1-x} \quad (0 \leq x \leq 1).$$

For $r=2$ one has

$$(0.7) \quad 2e(\Delta) \leq R(\theta|\xi) \leq R(\theta|\Delta) \leq h(e(\Delta))$$

the lower inequality being slightly better for $e(\Delta) \rightarrow 0$ than that in (0.6).

The lower inequality of (0.6) has been proved in [2], and also independently by A. Perez as a special case of a more general inequality (see

[12], formula (3.19)). The lower inequality in (0.7) has been proved by the author in the paper [14]; it has been obtained independently (not only for $r=2$ but also for an arbitrary $r \geq 2$) for the case when ξ has a discrete distribution by J. T. Chu and J. C. Chueh in [13]. Previously a slightly weaker inequality was proved by the author in [15] and [16]. The upper inequality of (0.7) is due to Fano [3] (see also [4]).

In this paper we specialize the problem as follows: let $\eta_1, \eta_2, \dots, \eta_n, \dots$ be a sequence of random variables which are, under the condition that the value of θ is fixed, $\theta = \theta_k$ say, independent and identically distributed, their common distribution depending on k ($k=1, 2, \dots, r$). Let the observed statistic $\xi = \xi^{(n)}$ be the vector $\xi^{(n)} = (\eta_1, \eta_2, \dots, \eta_n)$. Let us denote in this case the standard decision by Δ_n . In § 2 it is shown that $e(\Delta_n)$ tends for $n \rightarrow \infty$ exponentially fast to 0, further that the quantity $R(\theta | \xi^{(n)})$ is of the same order of magnitude as $e(\Delta_n)$ while $R(\theta | \Delta_n)$ is of the same order of magnitude as $h(e(\Delta_n))$. In § 3 a special case is discussed, which was already considered in [8], and some remarks are added.

One of the tools needed for the proof of the mentioned statements is a theorem on large deviations given in § 1.

§ 1. A THEOREM ON LARGE DEVIATIONS

Generalizing the results of H. Cramér [5] and H. Chernoff [6], R. R. Bahadur and R. Ranga Rao [7] have proved the following

Theorem 1 (of Bahadur and Ranga Rao): Let $\xi_1, \xi_2, \dots, \xi_n, \dots$ be independent and identically distributed random variables, with the (non-degenerate) distribution function $F(x)$. Suppose that the moment generating function

$$(1.1) \quad \varphi(t) = \int_{-\infty}^{+\infty} e^{tx} dF(x)$$

exists in a non-degenerate interval I of the real line. Let α be a real number such that $\psi(t) = e^{-\alpha t} \cdot \varphi(t)$ takes on its minimum

$$(1.2) \quad \lambda = \min_{t \in I} \psi(t)$$

in an interior point τ of the interval I . Suppose that $\xi_1, \xi_2, \dots$ are non-lattice variables. Then

$$(1.3) \quad 0 < \lambda < 1, \quad \frac{\varphi'(\tau)}{\varphi(\tau)} = \alpha$$

and putting

$$(1.4) \quad S_n = \xi_1 + \dots + \xi_n$$

one has

$$(1.5) \quad P(S_n \geq n\alpha) = \frac{B\lambda^n}{\sqrt{2\pi n}} (1 + o(1)) \quad \text{for} \quad n \rightarrow +\infty$$

where $B = \frac{1}{\sigma\tau}$.

Remark 1. It is easy to see that (1.5) can be generalized as follows. For every fixed b

$$(1.5^*) \quad P(S_n \geq n\alpha + b) = \frac{B e^{-b\tau} \lambda^n}{\sqrt{2\pi n}} (1 + o(1)) \quad \text{for} \quad n \rightarrow \infty.$$

Remark 2. If the ξ_i are lattice-variables, it is still true that $P(S_n \geq n\alpha + b)$ is of the order of magnitude $\frac{\lambda^n}{\sqrt{n}}$.

We shall now prove, using the same method of H. Cramér as that used in [5], [6] and [7], the following

Theorem 2. Under the conditions of Theorem 1 and with the same notations one has for $n \rightarrow \infty$

$$(1.6) \quad E(S_n | S_n \geq n\alpha) = n\alpha + O(1).$$

Proof of Theorem 2. Put $\xi_k^* = \xi_k - \alpha$ and denote by $F^*(x)$ the distribution function of ξ_k^* , i. e. put $F^*(x) = F(x + \alpha)$. Let $F_n^*(x)$ denote the distribution function of $S_n - n\alpha$. Let us define the distribution function $G(x)$ by

$$(1.7) \quad G(x) = \frac{1}{\lambda} \int_{-\infty}^x e^{\tau y} dF^*(y).$$

Clearly, if $\eta_1, \dots, \eta_n, \dots$ are independent, identically distributed random variables, with the distribution function $G(x)$ then

$$(1.8) \quad E(\eta_k) = 0, \quad D^2(\eta_k) = \sigma^2 = \frac{\varphi''(\tau)}{\varphi(\tau)} - \alpha^2 > 0$$

and denoting by $G_n(x)$ the distribution function of the sum

$$(1.9) \quad \zeta_n = \eta_1 + \dots + \eta_n$$

one has

$$(1.10) \quad G_n(x) = \frac{1}{\lambda^n} \int_{-\infty}^x e^{\tau y} dF_n(y).$$

It follows that

$$(1.11) \quad F_n(x) = \lambda^n \int_{-\infty}^x e^{-\tau y} dG_n(y)$$

and

$$(1.12) \quad E(S_n | S_n \geq na) = na + \frac{\int_0^{\infty} x e^{-\tau x} dG_n(x)}{\int_0^{\infty} e^{-\tau x} dG_n(x)}$$

Putting

$$(1.13) \quad H_n(y) = G_n(y\sigma\sqrt{n})$$

it follows

$$(1.14) \quad E(S_n | S_n \geq na) = na + \frac{\sigma\sqrt{n} \int_0^{\infty} y e^{-\tau\sigma y\sqrt{n}} dH_n(y)}{\int_0^{\infty} e^{-\tau\sigma y\sqrt{n}} dH_n(y)}$$

Now the central limit theorem can be applied to the sum ζ_n and it follows (see [9] or [10]), that (as the distribution function $G(x)$ possesses finite moments of all orders)

$$(1.15) \quad H_n(y) = \phi(y) + O\left(\frac{1}{\sqrt{n}}\right).$$

Now by Theorem 1

$$(1.16) \quad \int_0^{\infty} e^{-\tau \sigma y \sqrt{n}} dH_n(y) = \frac{B}{\sqrt{2\pi n}} (1 + o(1))$$

and by (1.15) and partial integration, taking into account that

$$(1.17) \quad \int_x^{\infty} e^{-u^2/2} du = \frac{e^{-x^2/2}}{x} (1 + O\left(\frac{1}{x^2}\right))$$

we get

$$(1.18) \quad \sigma \sqrt{n} \int_0^{\infty} y e^{-\tau \sigma y \sqrt{n}} dH_n(y) = O\left(\frac{1}{\sqrt{n}}\right).$$

Clearly (1.6) follows from (1.14), (1.16) and (1.17). Thus Theorem 2 is proved.

Remark 1. In the same way one can prove also that for every fixed b we have

$$(1.6^*) \quad E(S_n | S_n \geq na + b) = na + O(1).$$

Remark 2. If the ξ_i are lattice variables it is still true that $E(S_n | S_n \geq na + b)$ has the order of magnitude n .

§ 2. ASYMPTOTIC RESULTS ON THE AMOUNT OF MISSING INFORMATION

In this § we restrict ourselves to the special case when the parameter θ has only two possible values θ_0 and θ_1 . The general case, when the number r of possible values of θ is arbitrary, does not present any essential new difficulty.

Let $\mathfrak{S} = (\Omega, \mathfrak{A}, P)$ be a probability space, $\theta = \theta(\omega)$ a random variable on $\mathfrak{S}$, taking on the values θ_0 and θ_1 with positive probabilities

$w_0 = P(\theta = \theta_0)$ and $w_1 = P(\theta = \theta_1)$. ($0 < w_0 < 1$, $w_1 = 1 - w_0$).

Let $\eta_1, \eta_2, \dots, \eta_n, \dots$ be real valued random variables on $\mathfrak{S}$ which are independent and identically distributed under the condition $\theta = \theta_i$ and let their common distributions under condition $\theta = \theta_i$ be absolutely continuous with respect to a measure μ with density function $f_i(x)$ ($i=0,1$). We suppose that $f_0(x)$ and $f_1(x)$ are different on a set of positive measure. If

$x^{(n)} = (x_1, x_2, \dots, x_n)$ is an n -tuple of real numbers, let us put

$$(2.1) \quad f_i(x^{(n)}) = \prod_{k=1}^n f_i(x_k) \quad (i=0,1).$$

Let $\xi^{(n)}$ denote the random vector $(\eta_1, \eta_2, \dots, \eta_n)$. In this case the standard decision Δ_n concerning the value of the parameter θ after having observed $\xi^{(n)}$ consists in accepting θ_0 if

$$w_0 f_0(\xi^{(n)}) \geq w_1 f_1(\xi^{(n)})$$

and accepting θ_1 , if

$$w_0 f_0(\xi^{(n)}) < w_1 f_1(\xi^{(n)}).$$

The error $e(\Delta_n)$ of the standard decision is in this case

$$(2.2) \quad e(\Delta_n) = w_0 \alpha_n + w_1 \beta_n$$

where

$$(2.3) \quad \alpha_n = \int_{w_1 f_1(x^{(n)}) > w_0 f_0(x^{(n)})} f_0(x^{(n)}) \mu(dx^{(n)})$$

and

$$(2.4) \quad \beta_n = \int_{w_1 f_1(x^{(n)}) \leq w_0 f_0(x^{(n)})} f_1(x^{(n)}) \mu(dx^{(n)})$$

Here and in what follows we use for the sake of brevity the notation

$$\mu(dx^{(n)}) = \prod_{k=1}^n \mu(dx_k).$$

Let $S_i^{(n)}$ denote the probability space $(E^n, \mathfrak{A}_n, P_i^{(n)})$ where

E^n is the n -dimensional Euclidean space, $\mathcal{A}_n$ the family of Borel subsets of E^n and $P_i^{(n)}$ the measure

$$(2.5) \quad P_i^{(n)}(A) = \int_A f_i(x^{(n)}) \mu(dx^{(n)}) \quad (i = 0, 1).$$

Clearly the random variables

$$(2.6) \quad \delta_k^{(i)} = \log \frac{f_{1-i}(x_k)}{f_i(x_k)} \quad (k = 1, 2, \dots, n; i = 0, 1)$$

are independent and identically distributed on $S_i^{(n)}$ and have the moment-generating function

$$(2.7) \quad \varphi_i(t) = \int_{-\infty}^{+\infty} f_{1-i}^t(x) f_i^{1-t}(x) \mu(dx)$$

which exists for $0 \leq t \leq 1$ (by Hölder's inequality) and is a convex function of t . Clearly $\varphi_1(t) = \varphi_0(1-t)$.

Let us put

$$(2.8) \quad \lambda = \min_{0 \leq t \leq 1} \varphi_0(t) = \min_{0 \leq t \leq 1} \varphi_1(t) = \varphi_0(\tau) = \varphi_1(1-\tau).$$

Then we have

$$0 \leq \lambda < 1, \quad 0 < \tau < 1$$

We may exclude the case $\lambda=0$ which can happen only if $f_0(x)f_1(x) = 0$ almost everywhere, in which case a single observation is sufficient to decide with probability of error equal to 0 whether $\theta = \theta_0$ or $\theta = \theta_1$.

Now clearly

$$(2.9) \quad \begin{aligned} \alpha_n &= P_0^{(n)}(\delta_1^{(0)} + \dots + \delta_n^{(0)} > \log \frac{w_0}{w_1}) \\ \beta_n &= P_1^{(n)}(\delta_1^{(1)} + \dots + \delta_n^{(1)} > \log \frac{w_1}{w_0}). \end{aligned}$$

If the $\delta_k^{(i)}$ are not lattice variables the conditions of Theorem 1 are satisfied; and from (1.5^{*}) for $\alpha=0$ we obtain

$$(2.10/a) \quad \alpha_n = \frac{B_0 \lambda^n}{\sqrt{2\pi n}} (1 + o(1))$$

and

$$(2.10/b) \quad \beta_n = \frac{B_1 \lambda^n}{\sqrt{2\pi n}} (1 + o(1))$$

where B_0 and B_1 are positive constants.

Thus we have

$$(2.11) \quad e(\Delta_n) = \frac{B \lambda^n}{\sqrt{2\pi n}} (1 + o(1))$$

where $B > 0$, $0 < \lambda < 1$. Thus $e(\Delta_n)$ tends exponentially fast to 0 for $n \rightarrow +\infty$. Now let us consider the quantity $R(\theta | \xi^{(n)})$. We have clearly

$$(2.12) \quad \begin{aligned} R(\theta | \xi^{(n)}) &= w_0 \int_{E^n} f_0(x^{(n)}) \log_2 \left(1 + \frac{w_1 f_1(x^{(n)})}{w_0 f_0(x^{(n)})} \right) \mu(dx^{(n)}) + \\ &+ w_1 \int_{E^n} f_1(x^{(n)}) \log_2 \left(1 + \frac{w_0 f_0(x^{(n)})}{w_1 f_1(x^{(n)})} \right) \mu(dx^{(n)}) . \end{aligned}$$

Let C_n denote the set of those $x^{(n)}$ for which

$$w_1 f_1(x^{(n)}) > w_0 f_0(x^{(n)}) .$$

Now we split both integrals on the right hand side of (2.12) into two parts, corresponding to the set C_n and its complementary set $\bar{C}_n$. In the first integral on C_n we apply the inequality $\log_2(1+x) \leq 1 + \log_2 x$ for $x \geq 1$, and on $\bar{C}_n$ the inequality $\log_2(1+x) \leq x \log_2 e$ ($x \geq 0$) while conversely, in the second integral we apply on $\bar{C}_n$ the inequality $\log_2(1+x) \leq 1 + \log_2 x$ and on C_n the inequality $\log_2(1+x) \leq x \log_2 e$. Thus we obtain

$$\begin{aligned}
 R(\theta|\xi^{(n)}) &\leq w_1(1+\log_2 e + \log_2 \frac{w_0}{w_1})\beta_n + w_0(1+\log_2 e + \log_2 \frac{w_1}{w_0})\alpha_n + \\
 (2.13) \quad &+ w_0 \int_{C_n} f_0(x^{(n)}) \log_2 \frac{f_1(x^{(n)})}{f_0(x^{(n)})} \mu(dx^{(n)}) + w_1 \int_{\bar{C}_n} f_1(x^{(n)}) \log_2 \frac{f_0(x^{(n)})}{f_1(x^{(n)})} \mu(dx^{(n)}).
 \end{aligned}$$

Now clearly, putting

$$(2.14) \quad s_n^{(i)} = \sum_{k=1}^n \delta_k^{(i)} \quad (i = 0, 1)$$

$$\frac{1}{\log_2 e} \int_{C_n} f_0(x^{(n)}) \log_2 \frac{f_1(x^{(n)})}{f_0(x^{(n)})} \mu(dx^{(n)}) = \alpha_n E(S_n^{(0)} | S_n^{(0)} > \log \frac{w_1}{w_0})$$

and

$$(2.15) \quad \frac{1}{\log_2 e} \int_{\bar{C}_n} f_1(x^{(n)}) \log_2 \frac{f_0(x^{(n)})}{f_1(x^{(n)})} \mu(dx^{(n)}) = \beta_n E(S_n^{(1)} | S_n^{(1)} > \log \frac{w_0}{w_1}).$$

Thus using (1.6*) we obtain from (2.13), (2.14) and (2.15) that

$$(2.16) \quad R(\theta|\xi^{(n)}) \leq A_1 \alpha_n + A_2 \beta_n$$

and thus

$$(2.17) \quad R(\theta|\xi^{(n)}) \leq A_3 e(\Delta_n)$$

where A_1, A_2 , and A_3 are positive constants, not depending on n .

In view of Remark 2 to Theorem 1 and Theorem 2 the inequality (2.17) remains valid also when the $\delta_k^{(i)}$ are lattice-variables. Thus we have proved

Theorem 3. For $n \rightarrow +\infty$ $R(\theta|\xi^{(n)})$ has the same order of magnitude as $e(\Delta_n)$.

Let us now consider the quantity $R(\theta|\xi^{(n)})$. We have evidently

$$\begin{aligned}
 R(\Theta|\Delta_n) = & w_0 \alpha_n \log_2 \left(1 + \frac{w_1(1-\beta_n)}{w_0 \alpha_n}\right) + w_1 \beta_n \log_2 \left(1 + \frac{w_0(1-\alpha_n)}{w_1 \beta_n}\right) + \\
 (2.18) \quad & + w_0(1-\alpha_n) \log_2 \left(1 + \frac{w_1 \beta_n}{w_0(1-\alpha_n)}\right) + w_1(1-\beta_n) \log_2 \left(1 + \frac{w_0 \alpha_n}{w_1(1-\beta_n)}\right)
 \end{aligned}$$

It follows from (2.18) immediately that

$$(2.19) \quad R(\Theta|\Delta_n) \geq A_4 h(e(\Delta_n)).$$

Thus we have proved

Theorem 4. For $n \rightarrow +\infty$ $R(\Theta|\Delta_n)$ has the same order of magnitude as $h(e(\Delta_n))$.

§ 3. SOME FURTHER REMARKS

We have considered the special case when the variables η_k take on only two values, in a previous paper [8]. Let the possible values of the variables η_k be 0 and 1, and let us put for $i = 0, 1$

$$\begin{aligned}
 (3.1) \quad & P(\eta_k = 1 | \Theta = \theta_i) = p_i > 0 \\
 & P(\eta_k = 0 | \Theta = \theta_i) = q_i = 1 - p_i > 0.
 \end{aligned}$$

It follows from the discussion of § 2. that in this case

$$(3.2) \quad R(\Theta|\xi^{(n)}) = O\left(\frac{\lambda^n}{\sqrt{n}}\right)$$

where

$$(3.3) \quad \lambda = \min_{0 \leq t \leq 1} (p_0^t p_1^{1-t} + q_0^t q_1^{1-t}).$$

In [8] we have defined the number λ as follows. Let us put

$$(3.4) \quad \Delta(x, y) = x \log_2 \frac{x}{y} + (1-x) \log_2 \frac{1-x}{1-y}$$

for $0 \leq x \leq 1$, $0 \leq y \leq 1$. Let φ denote the (unique) solution of the equation

$$(3.5) \quad \Delta(\varphi, p_0) = \Delta(\varphi, p_1)$$

and put

$$(3.6) \quad d(p_0, p_1) = \Delta(\varphi, p_0) = \Delta(\varphi, p_1).$$

Then one has

$$(3.7) \quad \lambda = 2^{-d(p_0, p_1)}.$$

It is not difficult to show that the number λ defined by (3.7) is identical to the number defined by (3.3). This is a particular case of a general relation. Let τ ($0 < \tau < 1$) denote that value of t for which

$$(3.8) \quad \int f_0(x)^t f_1(x)^{1-t} \mu(dx)$$

takes on its minimal value λ . It follows that

$$(3.9) \quad \int_{-\infty}^{+\infty} f_0(x)^\tau f_1(x)^{1-\tau} \log_2 \frac{f_0(x)}{f_1(x)} \mu(dx) = 0.$$

Thus, putting

$$(3.10) \quad g(x) = \frac{f_0(x)^\tau f_1(x)^{1-\tau}}{\lambda}$$

we get

$$(3.11) \quad \int_{-\infty}^{+\infty} g(x) \log_2 \frac{g(x)}{f_0(x)} \mu(dx) = \int_{-\infty}^{+\infty} g(x) \log_2 \frac{g(x)}{f_1(x)} \mu(dx) = \log_2 \frac{1}{\lambda}.$$

This implies the equivalence of the two definitions of λ in the special case considered.

In the special case considered, when the variables η_k take on only the values 0 and 1, the equation

$$(3.12) \quad \int_{-\infty}^{+\infty} h(x) \log_2 \frac{h(x)}{f_0(x)} \mu(dx) = \int_{-\infty}^{+\infty} h(x) \log_2 \frac{h(x)}{f_1(x)} \mu(dx)$$

(which in this case reduces to (3.5)) determines the function $h(x)$ uniquely, i. e. it follows from (3.12) that $h(x)=g(x)$ where $g(x)$ is the density function defined by (3.10). This is however not true in the general case, as (3.12) has an infinity of solutions. In the general case the function $g(x)$ given by (3.10) can be characterized as that solution of (3.12) for which the common value of

$\int h(x) \log_2 \frac{h(x)}{f_0(x)} \mu(dx)$ and $\int h(x) \log_2 \frac{h(x)}{f_1(x)} \mu(dx)$ is minimal (see [18] p. 148-150). As a matter of fact if $h(x)$ is any solution of (3.12) one has

$$(3.13) \quad \begin{aligned} \int_{-\infty}^{+\infty} h(x) \log_2 \frac{h(x)}{f_0(x)} \mu(dx) &= \int_{-\infty}^{+\infty} h(x) \log_2 \frac{h(x)}{f_1(x)} \mu(dx) = \\ &= \tau \int_{-\infty}^{+\infty} h(x) \log_2 \frac{h(x)}{f_0(x)} \mu(dx) + (1-\tau) \int_{-\infty}^{+\infty} h(x) \log_2 \frac{h(x)}{f_1(x)} \mu(dx) \end{aligned}$$

and for any $h(x)$ one has

$$(3.14) \quad \begin{aligned} \tau \int_{-\infty}^{+\infty} h(x) \log_2 \frac{h(x)}{f_0(x)} \mu(dx) + (1-\tau) \int_{-\infty}^{+\infty} h(x) \log_2 \frac{h(x)}{f_1(x)} \mu(dx) = \\ = \log_2 \frac{1}{\lambda} + \int_{-\infty}^{+\infty} h(x) \log_2 \frac{h(x)}{g(x)} \mu(dx) \geq \log_2 \frac{1}{\lambda} \end{aligned}$$

equality being valid if and only if $h(x)=g(x)$.

One can reformulate this characterization of $g(x)$ as a definition of λ , as follows:

Theorem 5.

$$(3.15) \quad \log_2 \frac{1}{\lambda} = \min \left[\max \left(\int_{-\infty}^{+\infty} h(x) \log_2 \frac{h(x)}{f_0(x)} \mu(dx), \int_{-\infty}^{+\infty} h(x) \log_2 \frac{h(x)}{f_1(x)} \mu(dx) \right) \right]$$

where the minimum is taken over all density functions $h(x)$ with respect to the measure μ .

Proof of Theorem 5. The proof follows simply from the inequality

$$\max(a, b) \geq \tau a + (1-\tau)b \quad (0 < \tau < 1)$$

and from (3.14).

It follows from our results that both the lower and upper inequality of (0.6) is best possible, at least up to a constant factor. Our results

imply that the amount of missing information given Δ_n is essentially larger (by a factor of order n) than the amount of missing information given the whole sample $\xi^{(n)}$ (or a sufficient statistic, e.g. the posterior distribution $P(\theta = \theta_i | \xi^{(n)})$ of θ), even if the standard decision is taken (which has minimal error). Note however, that the standard decision is not necessarily the most informative decision^{*/} - Nevertheless, the amount of missing information is not much less even if the most informative decision is applied. As a matter of fact, it follows from the results of Nemetz, that the amount of missing information is decreased only by a constant factor if the most informative decision is adopted.

REFERENCES

- [1] A. RÉNYI: On the amount of missing information and the Neyman-Pearson lemma. Festschrift for J. Neyman, Wiley, London, 1966, . 281-288.
- [2] A RÉNYI: Statistics and information theory, Studia Sci. Math. Hung. 2(1967) 249-256.
- [3] R. M. FANO: Statistical theory of communication, M.I.T., Cambridge, Mass. 1954.
- [4] A. FEINSTEIN: Foundations of information theory, McGraw-Hill, New York, 1958.
- [5] H. CRAMÉR: Sur un nouveau théorème-limite de la théorie des probabilités. Actualités Scientifiques et Industrielles, 736, Hermann, Paris, 1938.
- [6] H. CHERNOFF: Large sample theory: parametric case, Annals of Math. Stat. 27 (1956) 1-22.
- [7] R. R. BAHADUR-R. RANGA RAO: On deviation of the sample mean. Annals of Math. Stat. 31 (1960) 1015-1027.
- [8] A. RÉNYI: On the amount of information in a frequency count. Bull. Internat. Statistical Institute, Vol. 46. Book II (1965) 623-626.
- [9] C. G. ESSEEN: Fourier analysis of distribution functions. Acta Math. 77 (1945) 1-125.

^{*/} This question has been investigated by T. Nemetz. See [11] and his paper in this volume.

- [10] B. V. GNEDENKO-A. N. KOLMOGOROV: Limit distributions for sums of independent random variables. Addison-Wesley, Cambridge, Mass. 1954, p.201.
 - [11] T. NEMETZ: Maximally informative decisions. (In Hungarian) MTA III. Oszt. Közl. 17 (1967) 455-465.
 - [12] A. PEREZ: Information-theoretic risk estimates in statistical decision. Kybernetika, 3 (1967).
 - [13] J. T. CHU and J. C. CHUEH: Inequalities between information measures and error probability. Journal of the Franklin Institute 282 (1966) 121-125.
 - [14] A. RÉNYI: On the amount of information in a random variable concerning an event. Journal of Math. Sciences (Delhi) 1966, 30-33.
 - [15] A. RÉNYI: On some basic problems of statistic from the point of view of information theory. Proc. 5th Berkeley Symposium. Vol. 1. 531-543.
 - [16] A. RÉNYI: On the amount of information concerning an unknown parameter in a sequence of observations. Publ. Math. Inst. Hung. Acad. Sci. 9 (1964) 617-624.
 - [17] J. T. CHU: Optimal decision functions for computer character recognition. Journal of the Association for Computing Machinery 12 (1965) 213-226.
 - [18] M. SAKAGUCHI: Information theory and decision making (Mimeographed lecture notes) The George Washington University, 1964.
- 231, 236, 265, 266, 267, 285, 288, 305

NOTE

Rényi's papers on the application of information theory to statistics — on a Bayesian basis — have effectively called attention to this subject and strongly influenced further research. The work started with the paper No. 231 and had been continued by Rényi himself (Nos. 236, 265, 266, 267, 285, 288, 305, 328) as well as by other mathematicians. Of Rényi's own contributions, the most significant ones are No. 231, No. 288, and No. 328 which contains the sharpest results. References to related works are given in Rényi's papers. Some recent developments will be discussed below.

Though the random variables $\eta_1, \eta_2, \dots$ are supposed to be real valued in paper No. 328, this supposition is nowhere used; the proofs are valid for abstract valued random variables, as well. A subtle point is, however, that if the densities f_1 and f_2 vanish on different sets, the function (2.7) is not continuous at the endpoints of the interval $[0, 1]$ and the minimum in (2.8) need

not be achieved; in this case the proofs of (2.11) and (2.17) break down and even a counterexample exists, see Hellman and Raviv [9]. This point is elaborated by Vajda [8]. It should be noted that the exponential rate of convergence is not affected, see Chernoff's classical paper, referred to in No. 231.

If the parameter θ has more than two but finitely many possible values θ_i , we have $\lim_{n \rightarrow \infty} \sqrt[n]{e(\Delta_n)} = \lim_{n \rightarrow \infty} \sqrt[n]{R(\theta | \xi^{(n)})} = \max_{i \neq k} \lambda_{ik}$ where $\lambda_{ik} = \inf_{0 \leq t \leq 1} \int f_i^t(x) f_k^{1-t}(x) \mu(dx)$, $f_i(x)$ being the conditional μ -density of the η 's given $\theta = \theta_i$.

This is an easy consequence of Rényi's results and was independently obtained by Vajda [7]; it also follows from Theorem 5 of Shannon, Gallager and Berlekamp [4]. Quite new problems arise if θ has a continuous distribution. The information in the sample concerning the parameter can be defined in that case, too, but it goes to infinity as $n \rightarrow \infty$. The problem is, how fast, and which statistic (if any) gives asymptotically the same amount of information as the whole sample. In this direction, very interesting results were obtained by Pinsker (1972).

The second inequality of Theorem 1 of No. 288 is a particular case of Fano's inequality, referred to in No. 285, while the first one holds even if the left hand side is multiplied by 4, as shown in No. 285. This first inequality was also proved by Kovalevsky [2] and Baladová [3]; Vajda [6] gives another proof, through a related inequality for a generalized information measure. Results of Perez [5] and Arimoto [10] also show that in certain cases the error probability can be better estimated in terms of some generalized information measure. Arimoto, in particular, has given the analogues of the known inequalities between error probability and missing information (in both directions) for the generalized information measures introduced by him.

Though the amount of information with respect to θ is mathematically meaningful only if θ is a random variable, nevertheless, information-theoretic methods can be effectively used in non-Bayesian statistics, too; see Kullback [1]. A general class of measures of informativity of statistical experiments has been suggested by Csiszár [12]. These informativity measures, useful both for the Bayesian and the non-Bayesian approach, are related to those of Arimoto [10]. An interesting new model of statistical decision problems of Nemetz [13] has also been motivated to a great extent by Rényi's information-theoretic approach to statistics.

Section 5 of No. 288 shows an interesting connection between the main results of the paper and a measure theoretic theorem of Kakutani. In the notation of the paper Theorem 3.1 asserts that $\prod_{k=1}^{\infty} \lambda_k = 0$ implies that μ and ν

are orthogonal. It is also possible to show in a direct way that $\prod_{k=1}^{\infty} \lambda_k > 0$ implies that μ and ν are equivalent, which amounts to a new proof of Kakutani's theorem, see Nemetz [11]. (I. Cs.)

REFERENCES

- [1] Kullback, S.: *Information theory and statistics*. Wiley, New York, (1959).
- [2] Ковалевский, В. А.: *Задача распознавания образовточкой с зрения тематической*

статистики. Читающие автоматы и распознавание образов. Киев, Наукова думка. (1965).

- [3] Baladová, L.: Minimum of average conditional entropy for given minimum probability of error. *Kybernetika*, 2 (1966), 416—422.
- [4] Shannon, C. E., Gallager, R. G. and Berlekamp, E. R.: Lower bounds to error probability for coding on discrete memoryless channels, II. *Information and Control*, 10 (1967), 522—552.
- [5] Perez, A.: Risk estimates in term of generalized f -entropies. *Proceedings of the Colloquium on Information Theory* held at Debrecen, 1967, published by the Bolyai Mathematical Society, Budapest, 1968, 299—316.
- [6] Вайда, И.: Оценка минимальной вероятности ошибки при проверке конечного или счетного числа гипотезов. *Проблемы Передачи Информации*, 4 (1968), 9—19.
- [7] Vajda, I.: On the convergence of information contained in a sequence of observations. *Proceedings of the Colloquium on Information Theory*, Debrecen, 1967, 489—501.
- [8] Vajda, I.: On the amount of information contained in a sequence of independent observations. *Kybernetika*, 6 (1970), 306—323.
- [9] Hellman, M. E. and Raviv, J.: Probability of error, equivocation, and the Chernoff bound. *IEEE Transactions IT*—16, (1970), 368—372.
- [10] Arimoto, S.: Information-theoretical considerations of estimation problems. *Information and Control*, 19 (1971), 181—194.
- [11] Nemetz, T.: Information theoretic methods in statistic (in Hungarian) Thesis submitted to the Hung. Acad. of Sci. in partial fulfilment of the requirements for the academic degree of "Candidate of Math. Sci." (1972).
- [12] Csizsár, I.: A class of measure of informativity of observation channels. *Periodica Math. Hung.*, 2 (1972), 191—213.
- [13] Nemetz, T.: On a finite decision model. Lecture, presented on the 7th Prague Conference on Information Theory, (1974). (See also Nemetz (1972).) [11]

ON THE ENUMERATION OF TREES

A. RÉNYI

§ 1. INTRODUCTION

The aim of this paper is to give another proof for the famous formula of Cayley, according to which denoting by T_n the total number of trees having n labelled vertices, one has

$$(1) \quad T_n = n^{n-2}.$$

Cayley has stated formula (1) in 1889 (see [1]) without giving a full proof. As a matter of fact, Cayley has formulated in his paper the following more general formula:

$$(2) \quad \sum_T x_1^{v_1(T)-1} x_2^{v_2(T)-1} \dots x_n^{v_n(T)-1} = (x_1 + x_2 + \dots + x_n)^{n-2}$$

where the summation is to be extended over all trees T having n vertices labelled by the numbers $1, 2, \dots, n$ and $v_k(T)$ denotes the degree (valency) of the point labelled by k in the tree T . Clearly for $x_1 = x_2 = \dots = x_n = 1$ formula (2) reduces to (1). Cayley has verified (2) for $n = 6$ by exhibiting all possible trees; after this he remarked that "it will be at once seen that the proof given for this particular case is applicable for any value whatever of n ". We shall show in what follows that (2) can in fact be proved by induction very easily: it is not impossible that what Cayley had in mind was essentially the proof given below, or some variant thereof.

Several proofs for Cayley's formula (1) have been given. In his excellent paper J. W. Moon [2] outlines nine proofs of (1), which he attributes to Prüfer, Clarke, Rényi, Dziobek, Katz, Göbel, Moon, Kirchhoff and Pólya. Prüfer's proof can be formulated so that it gives the more general formula (2); the proof which Moon attributes to Kirchhoff leads to a formula which is even more general than (2): we shall return to this question in § 3 of this paper. The other seven proofs do not lead, without essential modification, to a proof of (2). It should be emphasized that (2) gives much more information on the family of trees having n labelled vertices than (1): for example it follows immediately from (2) that the number of trees with n labelled vertices in which the k th point has degree v_k ($k = 1, 2, \dots, n$) is equal to

$$(3) \quad T_n(v_1, v_2, \dots, v_n) = \frac{(n-2)!}{(v_1-1)! (v_2-1)! \dots (v_n-1)!} \text{ if } \sum_{k=1}^m v_k = 2n-2.$$

Let us mention that Prüfer's proof leads immediately to (3), from which (2) follows.

In what follows we shall call the sum on the right hand side of (2) *Cayley's polynomial of order n* , and denote it by

$$(4) \quad C_n(x_1, x_2, \dots, x_n) = \sum_T x_1^{v_1(T)-1} x_2^{v_2(T)-1} \dots x_n^{v_n(T)-1}.$$

With this notation (2) can be written in the following form:

$$(5) \quad C_n(x_1, x_2, \dots, x_n) = (x_1 + x_2 + \dots + x_n)^{n-2}.$$

§ 2. PROOF OF CAYLEY'S FORMULA

Our aim is to prove formula (5) where the polynomial $C_n(x_1, x_2, \dots, x_n)$ is defined by (4). Evidently Cayley's polynomial $C_n(x_1, x_2, \dots, x_n)$ is a *symmetric* polynomial of its variables, and it is *homogeneous of degree $n-2$* ; the second statement follows from the remark that the degree of each term of Cayley's polynomial is $\left(\sum_{k=1}^n v_k\right) - n$, and in every graph the sum of the degrees of the points equals twice the number of edges: as a tree with n points has $n-1$ edges it follows that $\left(\sum_{k=1}^n v_k\right) - n = 2(n-1) - n = n-2$.

Evidently (5) holds for $n=2$, because there is only one tree with two vertices and in this both points have degree 1. Let us suppose that (5) holds for $n-1$ instead of n : we shall prove that this implies that it holds for n too.

If T is a tree with n labelled vertices, let us call the product $\prod_{k=1}^n x_k^{v_k(T)-1}$ in which $v_k(T)$ denotes the degree of the point labelled by the number k , the *profile* of the tree T . Clearly in the profile of a tree T the variable x_k occurs with a positive exponent if and only if the point labelled by the number k is not an end-point of T ; thus we have

$$(6) \quad C_n(x_1, \dots, x_{n-1}, 0) = \sum' x_1^{v_1(T)-1} \cdot x_2^{v_2(T)-1} \cdot \dots \cdot x_{n-1}^{v_{n-1}(T)-1}$$

where the dash after the sign Σ indicates that the summation has to be extended over those and only those trees T in which the point labelled by the number n is an endpoint. If T is such a tree that the point labelled by the number n is an endpoint of T , then removing from T this point together with the unique edge connecting it with an other point of T there remains a tree T' having $n-1$ points labelled by the numbers $1, 2, \dots, n-1$. The profile of such a tree T is equal to the profile of the tree T' multiplied by x_k provided that the point labelled by n was connected in T with the point labelled by k . It follows that

$$(7) \quad C_n(x_1, x_2, \dots, x_{n-1}, 0) = (x_1 + x_2 + \dots + x_{n-1}) C_{n-1}(x_1, x_2, \dots, x_{n-1})$$

and as by the induction hypothesis

$$(8) \quad C_{n-1}(x_1, x_2, \dots, x_{n-1}) = (x_1 + x_2 + \dots + x_{n-1})^{n-3}$$

we get

$$(9) \quad C_n(x_1, x_2, \dots, x_{n-1}, 0) = (x_1 + x_2 + \dots + x_{n-1})^{n-2}.$$

Let us call the terms $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ and $x_1^{h_1} x_2^{h_2} \dots x_n^{h_n}$ *similar*, if the sequence $(h_1, h_2, \dots, h_n)$ is a rearrangement of the sequence $(k_1, k_2, \dots, k_n)$. As $C_n(x_1, x_2, \dots, x_n)$ is a symmetric polynomial, similar terms of $C_n(x_1, x_2, \dots, x_n)$ have equal coefficients. From (9) we get the coefficients of all terms in which x_n

is missing; however as $C_n(x_1, \dots, x_n)$ is homogeneous of degree $n - 2$, in each term of this polynomial at least two variables are missing; thus to every term there can be found a similar term in which x_n is missing. Thus from (9) we can get the coefficients of all terms of the Cayley-polynomial $C_n(x_1, x_2, \dots, x_n)$. Expressed in another way, $C_n(x_1, x_2, \dots, x_n)$ is the unique polynomial which is symmetric and homogeneous of degree $n - 2$ for which (9) holds. As however the polynomial $(x_1 + x_2 + \dots + x_n)^{n-2}$ reduces to $(x_1 + x_2 + \dots + x_{n-1})^{n-2}$ if $x_n = 0$, it follows that $(x_1 + x_2 + \dots + x_n)^{n-2}$ is equal to the Cayley polynomial of order n , i.e. that (5) holds. This completes the proof of (5).

§ 3. SOME FURTHER REMARKS

In the last step of the proof of (5) given in § 2, we have used the following fact: if $P(x_1, x_2, \dots, x_n)$ is a symmetric polynomial of its n variables, and it is homogeneous of degree $< n$ then $P(x_1, x_2, \dots, x_n)$ is uniquely determined by $P(x_1, x_2, \dots, x_{n-1}, 0)$. Of course $P(x_1, x_2, \dots, x_n)$ can be expressed by a formula, the right hand side of which can be evaluated provided that $P(x_1, \dots, x_{n-1}, 0)$ is given. To express this formula in a compact form, let us denote by S_k the operator which applied to any polynomial $P(x_1, x_2, \dots, x_n)$ ($n > k$) substitutes 0 for x_k , i.e.

$$(10) \quad S_k P(x_1, \dots, x_n) = P(x_1, \dots, x_{k-1}, 0, x_{k+1}, \dots, x_n).$$

Let us consider the operator

$$(11) \quad \Delta_n = \prod_{k=1}^n (I - S_k)$$

where I is the identity operator. It follows by the inclusion-exclusion principle that if P is any polynomial of n variables, then $\Delta_n P$ is equal to the sum of those terms of P in which every one of the variables $x_1, x_2, \dots, x_n$ occurs with a positive exponent. In particular if P is such a polynomial which does not contain any term in which all the n variables occur effectively, then we have

$$(12) \quad \Delta_n P = 0.$$

Thus in particular if P is homogeneous of degree $< n$, then (12) holds.

Let us consider now the following generalization of Cayley's polynomials. Let G be any graph having n labelled vertices and let us put

$$(13) \quad C_n(G; x_1, \dots, x_n) = \sum_T x_1^{v_1(T)-1} x_2^{v_2(T)-1} \dots x_n^{v_n(T)-1}$$

where the summation has to be extended over all *spanning trees* T of the graph G , i.e. over all trees having the same n vertices as G and which are subgraphs of G , i.e. consist only of edges belonging to the graph G . We shall call $C_n(G; x_1, \dots, x_n)$ the *Cayley-polynomial of the graph* G . Evidently the Cayley-polynomial $C_n(x_1, \dots, x_n)$ considered in the previous §§ is the Cayley polynomial of the complete graph of order n .

Of course the Cayley polynomial of a graph G is in general not symmetric: however it is homogeneous of degree $n-2$, and thus the formula (12) can be

applied. This leads to a proof of the following formula: If G is an arbitrary graph having n labelled points, then we have

$$(14) \quad x_1 x_2 \dots x_n C_n(G; x_1, x_2, \dots, x_n) = |A|$$

where $|A|$ denotes the determinant of the $(n-1)$ by $(n-1)$ matrix $A = (a_{jk})$ defined as follows:

$$(15) \quad a_{kk} = x_k \left(\sum_{(j,k) \in G} x_j \right)$$

where the summation has to be extended over those values of j for which the j th point is connected with the k th point in G , and

$$(16) \quad a_{jk} = \begin{cases} -x_j x_k & \text{if the } j\text{-th and } k\text{th points are connected in } G \\ 0 & \text{otherwise.} \end{cases}$$

Formula (14) is a particular case of a more general formula called in electrical engineering Maxwell's rule, which is closely related to Kirchhoff's rule (see [3], p. 131; for a simple proof see [4]). (14) is obtained from Maxwell's rule if the impedance e_{jk} of the edge connecting the j th and k th point is taken to be equal to $x_j x_k$.

My thanks are due to Prof. P. R. Bryant and Prof. H. Sachs for the above mentioned references concerning Maxwell's rule.

REFERENCES

- [1] Cayley, A.: A theorem on trees. *Quarterly Jour. Math.*, **23** (1889), 376—378.
- [2] Moon, J. W.: Various proofs of Cayley's formula for counting trees. In: *Seminar of Graph Theory*, (ed.) F. Harary, 70—78.
- [3] Bryant, P. R.: Graph theory applied to electrical networks. In: *Graph Theory and Theoretical Physics*, (ed.) F. Harary, Academic Press 1967, 111—137.
- [4] Hutschenreuther, H.: Einfacher Beweis des "Matrix-Gerüst-Satzes" der Netzwerktheorie. *Wissenschaftliche Zeitschrift der Technischen Hochschule Ilmenau*, **13** (1967), 403—404.

341. *Vorträge der II. Ungarischen Biometrischen Konferenz* (Budapest, von 19. bis 22. März 1968) Akadémiai Kiadó, Budapest, 1970; pp. 27–33.

STOCHASTISCHE PROZESSE IN DER BIOLOGIE

von

A. RÉNYI

Mathematisches Forschungsinstitut der Ungarischen Akademie der Wissenschaften,
Budapest, Ungarn

MATHEMATISCHE MODELLE DES WACHSTUMS BIOLOGISCHER POPULATIONEN

Das Wachstum biologischer Populationen kann durch verschiedenartige mathematische Modelle beschrieben werden. Es gibt einerseits deterministische Modelle, die den Prozeß als durch die Anfangsbedingungen eindeutig bestimmt auffassen.

Je nachdem, ob das Modell die Zeit und die Populationsgröße in kontinuierlichen oder diskreten Größen betrachtet, führt so ein Modell zu einer Differentialgleichung bzw. einer Differenzengleichung. Die deterministischen Modelle sind sehr nützlich, um eine klare Übersicht über die Grundtendenzen des Wachstums zu geben, aber sie geben ein zu vereinfachtes Bild des wirklichen Prozesses, da sie die zufälligen Schwankungen (die bei biologischen Wachstumsprozessen im allgemeinen von großer Bedeutung sind) völlig außer acht lassen.

Die stochastischen Modelle, die den Wachstumsprozeß als einen stochastischen Prozeß auffassen, geben ein die Wirklichkeit viel getreuer widerspiegelndes Bild des wirklichen Ablaufs des Wachstums der betrachteten Population. Die stochastischen Modelle fassen die Zeit meistens als kontinuierliche Veränderliche auf, aber die Größe der betrachteten Population wird durch die Anzahl der Mitglieder der Population beschrieben, also — der Wirklichkeit gemäß — als diskrete Größe behandelt. Solche stochastische Modelle führen im allgemeinen auf Differentialgleichungssysteme (bzw. Integrodifferentialgleichungssysteme) für die Glieder der Wahrscheinlichkeitsverteilung der zufälligen Anzahl der Mitglieder der Population, die als zufällige Funktion der Zeit aufgefaßt wird. Diese Gleichungssysteme können meistens in Form einer einzigen Differentialgleichung (bzw. Integrodifferentialgleichung) für die erzeugende Funktion der Wahrscheinlichkeitsverteilung aufgeschrieben werden. Aus dieser Gleichung kann man im allgemeinen eine einfachere Gleichung für den Erwartungswert der Größe der Population als Funktion der Zeit erhalten, die meistens mit der durch das entsprechende deterministische Modell gelieferten Gleichung übereinstimmt oder jedenfalls sich nur wenig davon unterscheidet.

Wenn man also anstatt eines deterministischen Modells das entsprechende stochastische Modell betrachtet, verliert man nichts; falls man nur einen Überblick über die Entwicklungstendenz der Population im Großen gewinnen will, geht man einfach zur Betrachtung der Erwartungswerte über. Die wirkliche Bedeutung des deterministischen Modells wird eben dadurch klar, daß so ein Modell sich eigentlich immer auf den Erwartungswert der Größe der Population bezieht. Dadurch wird auch klar, warum man die Größe einer Population als kontinuierliche Größe auffassen darf: Die wirkliche Größe ist zwar immer eine ganze Zahl, aber eine zufällige ganze Zahl, deren Erwartungswert als Funktion

der Zeit sich stetig (z. B. nach einem Exponentialgesetz) ändert. Das stochastische Modell gibt aber — im Gegensatz zum deterministischen Modell — auch Aufschluß über die Größenordnung der zufälligen Schwankungen um den Erwartungswert.

Die stochastischen Modelle haben aber den Nachteil, daß sie mathematisch meistens etwas schwieriger sind. Das ist ja eben der Preis, den man für die tiefere Einsicht in die Gesetzmäßigkeiten des Prozesses zahlen muß. Falls die mathematischen Schwierigkeiten unüberwindbar groß sind, kann man meistens einen Mittelweg einschlagen, indem man ein teilweise stochastisches, teilweise deterministisches Modell wählt. Dies bedeutet, daß man nur diejenigen Größen als stochastisch betrachtet, bei denen die zufälligen Schwankungen von großer Bedeutung sind, und solche Größen, die zwar in Wirklichkeit auch zufällig sind, aber deren Schwankungen von sekundärer Bedeutung sind, als eindeutige Funktionen der Zeit behandelt. Solche Modelle nenne ich im folgenden der Kürze halber »halbstochastisch«. Zur Erhaltung solcher Modelle, die die miteinander scheinbar unvereinbaren Forderungen nach der Realitätstreue einerseits und nach der Vermeidung unüberwindbarer mathematischer Schwierigkeiten andererseits gleichzeitig erfüllen, ist es auch oft nützlich, wirkliche biologische Prozesse in zwei oder mehrere Phasen zu teilen, und diese Phasen mit Hilfe verschiedener mathematischer Modelle zu beschreiben.

Diese Möglichkeiten werde ich im folgenden Abschnitt anhand eines konkreten Beispiels, der Reproduktion des Poliovirus, veranschaulichen.

MATHEMATISCHE MODELLE DER REPRODUKTION DES POLIOVIRUS

Die mathematischen Modelle zur Beschreibung des Reproduktionszyklus des Poliovirus, die ich jetzt erörtern werde, sind in Zusammenarbeit mit Herrn Dr. A. Koch* entstanden; ich bin Herrn Dr. Koch für die biologische Problemstellung und für die wertvollen Auskünfte über den Ablauf der Reproduktion des Poliovirus sehr dankbar.

Diesen Prozeß kann man sich folgendermaßen vorstellen: Ein Virion besteht aus einer ikosaederförmigen Hülle aus Protein, in deren Innern sich das aus RNS bestehende eigentliche Virus befindet. Falls ein Virion in das Innere einer lebendigen Zelle eindringt (die Versuche wurden mit Nierenzellen von Affen ausgeführt), so wird nach einer kurzen Zeit die Hülle aufgelöst, und das Virus wird frei. Nach einer kurzen Periode von etwa 10–15 Minuten werden die meisten Lebensfunktionen der Zelle lahmgelegt, und es beginnt der eigentliche Reproduktionsprozeß des Virus, der ungefähr 6 Stunden dauert. Während der ersten 3 Stunden produziert die Zelle — dem RNS-Code des Virus entsprechend — gewisse Enzyme, die in der zweiten Phase des Zyklus die Reproduktion des Virus katalysieren. In dem einfachsten Fall vereinigen sich diese Replikaseenzyme zu zweien zu Dimeren, und nur diese Dimere sind zur Katalysierung der Reproduktion des Virus fähig. Während der zweiten 3 Stunden des Zyklus entsteht eine große Anzahl von Kopien des Virus, ferner das Protein zur Bildung der Hüllen, und am Ende des

* Staatliches Institut für Gesundheitswesen, Abteilung für Virologie, Budapest.

Zyklus sind etwa 1000 fertige Virionen vorhanden, die aus der zerfallenden Zelle freierwerden.

Die mathematische Beschreibung des Prozesses muß also folgende empirische Tatsachen widerspiegeln:

Bis zum Ende der dritten Stunde werden hauptsächlich nur Enzyme produziert. Die Dimerbildung beginnt nur, wenn die Enzymkonzentration genügend hoch ist, und die eigentliche Reproduktion nur, wenn die Dimerkonzentration eine gewisse Höhe erreicht. Bis dahin ist nur das ursprüngliche Virus vorhanden, in der zweiten Hälfte des Zyklus aber reproduziert sich das Virus mit exponentieller Geschwindigkeit.

EIN DETERMINISTISCHES MODELL

Als erste Annäherung geben wir ein deterministisches Modell an, das die Dimerbildung noch nicht zu beschreiben beabsichtigt, nur die Bildung der Enzyme und die Virusreproduktion. Es bedeute $V(t)$ bzw. $E(t)$ die Anzahl der zur Zeit t in der Zelle anwesenden Viren bzw. Enzyme. Dann gilt das Differentialgleichungssystem

$$(1) \quad V'(t) = f(E) \cdot V(t),$$

$$(2) \quad E'(t) = \lambda V(t).$$

Gleichung (1) bedeutet, daß die Geschwindigkeit der Virusreproduktion mit der Anzahl der schon gebildeten Viren proportional ist, und der Faktor hängt nur von der Enzymkonzentration ab. Die Funktion $f(E)$ muß jedenfalls für $0 \leq E < +\infty$ stetig und monoton wachsend sein und die Bedingungen

$$f(0) = 0, \quad f(+\infty) = \mu > 0$$

erfüllen.

Gleichung (2) bedeutet, daß die Geschwindigkeit der Enzymbildung der Anzahl der anwesenden Viren proportional ist, wobei der Proportionalitätsfaktor λ konstant bleibt. Die Anfangsbedingungen sind offenbar

$$V(0) = 1, \quad E(0) = 0.$$

Das Gleichungssystem (1) bis (2) hat eine eindeutig bestimmte, diesen Anfangsbedingungen genügende Lösung. Falls man z. B.

$$(3) \quad f(E) = \frac{\mu^2 E}{\sqrt{\lambda^2 + \mu^2 E^2}}$$

setzt, wo die Wahl von $f(E)$ den genannten Bedingungen genügt, so kann die Lösung explizit angegeben werden; es ist nämlich

$$(4) \quad V(t) = \operatorname{ch} \mu t,$$

$$(5) \quad E(t) = \frac{\lambda}{\mu} \operatorname{sh} \mu t.$$

Da die Funktion $\text{ch}\mu t$ den Wert 2 für $t = \frac{\ln(2 + \sqrt{3})}{\mu}$ erreicht, so muß man (falls t die Zeit in Stunden bedeutet) den Wert von μ für etwa $\frac{\ln(2 + \sqrt{3})}{3}$

nehmen. Den Wert von λ könnte man daraus bestimmen, wenn die Anzahl $E(3)$ der vorhandenen Enzyme nach ungefähr 3 Stunden bekannt wäre; denn es ist $E(3) = \frac{\lambda}{\mu} \sqrt{3}$, also $\lambda = \frac{\mu E(3)}{\sqrt{3}}$.

Das Gleichungssystem (1) bis (2) ist nichtlinear; falls also die Anfangsbedingungen z. B. $V(0) = 2$, $E(0) = 0$ sind, so verändern sich die Funktionen $V(t)$ und $E(t)$ wesentlich (anstatt sich zu verdoppeln). Aber dies geschieht bekanntlich praktisch nie: falls ein Virus in die Zelle eindringt, läßt die Zellenwand ein zweites Virus praktisch nicht mehr durch.

Die Funktion $E(t) = \frac{\lambda}{\mu} \text{sh}\mu t$ wächst für kleine Werte von t fast linear, annähert so wie λt . Wenn man in (3) einfach $E(t) = \lambda t$ einsetzt, so erhält man für $V(t)$ aus (1)

$$(1') \quad V'(t) = V(t) \frac{\mu^2 t}{\sqrt{1 + \mu^2 t^2}},$$

dessen der Anfangsbedingung $V(0) = 1$ genügende Lösung

$$(4') \quad V(t) = \exp[\sqrt{1 + \mu^2 t^2} - 1]$$

ist.

Die Funktion (4) bzw. (4') ändert sich für kleine Werte von t nur sehr langsam, aber für größere Werte von t wachsen beide annähernd wie $e^{\mu t}$.

EIN HALBSTOCHASTISCHES MODELL

Ein vollständig stochastisches Modell des Reproduktionszyklus des Poliovirus ist mathematisch ziemlich kompliziert. Man kann aber ein ziemlich einfaches halb-stochastisches Modell bekommen, wenn man $E(t)$ als deterministisch behandelt [z. B. wenn man annimmt, daß für $E(t)$ die aus dem deterministischen Modell erhaltene Formel (5) gilt] und nur die Virusanzahl als stochastisch betrachtet. Dies führt zu einem einfachen Markowschen Prozeß vom Yuleschen Typ* (reiner Geburtsprozeß), der aber zeitlich inhomogen ist. Durch eine nichtlineare Transformation der Zeitskala kann aber dieser Prozeß auf den homogenen Fall zurückgeführt werden. Somit erhalten wir, falls $P_n(t)$ die Wahrscheinlichkeit bezeichnet, daß zur Zeit t genau n Viren in der Zelle vorhanden sind:

$$(6) \quad P_n(t) = \frac{1}{\text{ch}\mu t} \cdot \left(1 - \frac{1}{\text{ch}\mu t}\right)^{n-1} \quad (n = 1, 2, \dots),$$

* Siehe Th. E. HARRIS: The theory of branching processes. Springer, 1963.

also hat die Virusanzahl eine negative binomiale Verteilung. Für den Erwartungswert $M(t)$ der Verteilung (6), also für

$$(7) \quad M(t) = \sum_{n=1}^{\infty} n P_n(t)$$

erhält man

$$(8) \quad M(t) = \operatorname{ch} \mu t;$$

d. h. also, der Erwartungswert der Anzahl der Viren ist mit der aus dem deterministischen Modell erhaltenen Funktion $V(t)$ gleich. Für die Streuung $D(t)$ der Verteilung (6) erhält man

$$(9) \quad D(t) = \operatorname{ch} \mu t \cdot \sqrt{1 - \frac{1}{\operatorname{ch} \mu t}}.$$

Also für große Werte von t ist die relative Streuung der Virusanzahl nahezu 1.

EIN DETERMINISTISCHES MODELL FÜR DIE DIMERBILDUNG

Bisher haben wir die Tatsache vernachlässigt, daß die Enzyme zuerst paarweise Dimere bilden müssen, um als Katalysatoren bei der Virusreplikation dienen zu können. Nun betrachten wir diese Phase des Virusreproduktionszyklus, u. zw. zuerst deterministisch. Falls $Y(t)$ die Anzahl der zur Zeit t vorhandenen Dimere bezeichnet, so gilt offenbar (falls man annimmt, daß die Geschwindigkeit der Bildung neuerer Dimere mit der Anzahl der vorhandenen Paare von Enzymen proportional ist)

$$(10) \quad Y'(t) = v[E(t) - 2Y(t)]^2,$$

wobei die Anfangsbedingung $Y(0) = 0$ erfüllt sein muß und $v > 0$ eine Konstante ist. Falls wir in (10) als erste Annäherung $E(t) = \lambda t$ setzen, erhalten wir als Lösung der nichtlinearen Differentialgleichung (10)

$$(11) \quad Y(t) = \frac{1}{2} \left\{ \lambda t - \sqrt{\frac{\lambda}{2v}} \left(\frac{e^{2\sqrt{2\lambda v} \cdot t} - 1}{e^{2\sqrt{2\lambda v} \cdot t} + 1} \right) \right\}.$$

Das bedeutet, daß $Y(t)$ für kleine Werte von t sehr langsam wächst, es ist nämlich für kleine t -Werte annähernd

$$(12) \quad Y(t) \sim \frac{2\lambda^2 v t^3}{3},$$

aber für große Werte von t unterscheidet sich $Y(t)$ von $\frac{\lambda t}{2} = \frac{E(t)}{2}$ nur sehr wenig, denn es strebt nach (11) $E(t) - 2Y(t)$ (also die Anzahl der freien monomeren Enzyme) gegen die Konstante $\sqrt{\frac{\lambda}{2v}}$, es ist also

$$(13) \quad Y(t) = \frac{E(t) - \sqrt{\frac{\lambda}{2v}}}{2} + o(1).$$

Das bedeutet, daß für vernünftige, nicht zu kleine Werte von v (genau gesagt, falls $\sqrt{\lambda v}$ mindestens so groß ist wie μ) zum Zeitpunkt, wo die Virusreplikation wirklich anfängt, bereits der größte Teil aller bis dahin entstandenen Enzyme Dimere bildet; dies beweist, daß die Vernachlässigung der Dimerbildung bei den Modellen A und B berechtigt ist.

EIN STOCHASTISCHES MODELL FÜR DIE DIMERBILDUNG

Nehmen wir an, daß die Zeitpunkte der Entstehung neuer Enzyme einen Poissonschen Prozeß mit der Ereignisdichte $\frac{\lambda}{2}$ bilden und jedes Ereignis die Bildung 2 neuer Enzyme bedeutet. (Die Annahme der paarweisen Entstehung der Enzyme ist nur dazu nötig, um gewisse Paritätsschwierigkeiten auszuschalten.) Nehmen wir ferner an, daß, falls $2k$ freie, d. h. noch nicht zu Dimeren vereinigte Enzyme (Monomere) vorhanden sind, die Ereignisdichte der Entstehung eines neuen Dimers gleich $v \binom{2k}{2}$ ist. Falls $Q_k(t)$ die Wahrscheinlichkeit davon bedeutet, daß zur Zeit t genau $2k$ freie Enzyme vorhanden sind, und falls wir annehmen, daß der Prozeß Markowschen Typs ist, erhalten wir für die $Q_k(t)$ das Differentialgleichungssystem

$$(14) \quad \begin{aligned} 2Q'_k(t) &= \lambda(Q_{k-1}(t) - Q_k(t)) \\ &+ v[(2k+2)(2k+1)Q_{k+1}(t) - 2k(2k-1)Q_k(t)]. \end{aligned}$$

Unser Prozeß ist ein Geburts- und Todesprozeß, und es kann die allgemeine Theorie von S. KARLIN und J. MCGREGOR* angewendet werden. Es folgt, daß es eine stationäre Grenzverteilung der Anzahl der freien Enzyme gibt, u. zw. ist, wenn wir

$$\lim_{t \rightarrow +\infty} Q_k(t) = Q_k$$

setzen,

$$(15) \quad Q_k = \frac{\left(\frac{\lambda}{v}\right)^{2k}}{(2k)!} \cdot \frac{1}{\cos \sqrt{\frac{\lambda}{v}}} \quad (k = 0, 1, \dots).$$

Die Verteilung (15) kann als eine bedingte Poissonsche Verteilung interpretiert werden mit der Bedingung, daß die betrachtete Anzahl gerade ist. Der Erwartungswert der Verteilung (15) ist

$$(16) \quad \sum_{k=1}^{\infty} 2k Q_k = \sqrt{\frac{\lambda}{v}} \cdot \operatorname{th} \sqrt{\frac{\lambda}{v}},$$

* Siehe S. KARLIN und J. MCGREGOR: The classification of birth and death processes. Transactions Amer. Math. Soc. 86 (1957) 366—400.

also falls $\sqrt{\frac{\lambda}{v}}$ eine große Zahl ist, was angenommen werden kann, so ist der Erwartungswert der Anzahl der freien (monomeren) Enzyme ungefähr gleich $\sqrt{\frac{\lambda}{v}}$, im vollen Einklang mit dem deterministischen Modell *C*. Dadurch werden unsere Schlußfolgerungen bezüglich Modell *C* und also auch bezüglich der Modelle *A* und *B* unterstützt.

ON A NEW LAW OF LARGE NUMBERS

By

PAUL ERDÖS AND ALFRED RÉNYI

in Budapest, Hungary

§1. Introduction

We shall prove first (in §2) the new law of large numbers for the simplest special case, that is for independent repetitions of a fair game. For this special case the theorem can be stated as follows: if the game is played N times, the maximal average gain of a player over $[C \log_2 N]$ consecutive games* ($C \geq 1$), tends with probability one to the limit α , where α is the only solution in the interval $0 < \alpha \leq 1$ of the equation

$$\frac{1}{C} = 1 - \left(\frac{1+\alpha}{2} \right) \log_2 \left(\frac{2}{1+\alpha} \right) - \left(\frac{1-\alpha}{2} \right) \log_2 \left(\frac{2}{1-\alpha} \right).$$

In §3 we generalize this result to an arbitrary sequence η_n ($n = 1, 2, \dots$) of independent, identically distributed random variables with expectation 0, the common distribution of which satisfies the condition, that its moment-generating function $\phi(t) = E(e^{t\eta_n})$ exists in an open interval around the origin. We prove that for every α in a certain interval $0 < \alpha < \alpha_0$ one has

$$(1.1) \quad P \left(\lim_{N \rightarrow +\infty} \max_{0 \leq n \leq N - [C \log N]} \frac{\eta_{n+1} + \eta_{n+2} + \dots + \eta_{n+[C \log N]}}{[C \log N]} = \alpha \right) = 1,$$

where $C = C(\alpha)$ is defined by the equation

$$(1.2) \quad e^{-(1/C)} = \min_t \phi(t) e^{-\alpha t}.$$

* Here and in what follows $[x]$ denotes the integral part of x .

In §4 we discuss the special case of Gaussian random variables, in which case our result is essentially equivalent to a previous result of *Paul Lévy* about the Brownian movement process.

In §5 we give as an application of the result of §3, a new proof of the theorem of *P. Bártfai* on the "stochastic geyser problem", using the fact that the functional dependence between C and α in (1.1) determines the distribution of the variables uniquely (Theorem 3). The result of §2 can also be applied in probabilistic number theory; as a matter of fact it was such an application which led the first named author to raise the problem which is solved in the present paper.

§2. The maximal average gain of a player over a short period.

Let $\xi_1, \xi_2, \dots, \xi_n, \dots$ be a sequence of independent random variables, each taking on the values ± 1 with probability $1/2$. We may interpret ξ_n as the gain of one of the players in the n^{th} repetition of a fair game. Let us put $S_0 = 0$,

$$(2.1) \quad S_n = \xi_1 + \xi_2 + \dots + \xi_n \quad (n = 1, 2, \dots)$$

and

$$(2.2) \quad \vartheta(N, K) = \max_{0 \leq n \leq N-K} \frac{S_{n+K} - S_n}{K}.$$

Let us introduce the notation

$$(2.3) \quad h(x) = x \log_2 \frac{1}{x} + (1-x) \log_2 \frac{1}{1-x} \quad \text{for } 0 < x < 1;$$

i.e. $h(x)$ is the entropy of the probability distribution $(x, 1-x)$. We shall prove the following

Theorem 1. *For every fixed $c \geq 1$ we have**

$$(2.4) \quad P(\lim_{N \rightarrow +\infty} \vartheta(N, [c \log_2 N]) = \alpha) = 1,$$

* Here and what follows $P(\dots)$ denotes the probability of the event in the brackets.

where $\alpha = \alpha(c)$ is the only solution with $0 < \alpha \leq 1$ of the equation

$$(2.5) \quad \frac{1}{c} = 1 - h\left(\frac{1+\alpha}{2}\right).$$

Remark. It is easy to see that $\alpha(c)$ is a decreasing function of c , further $\alpha(1) = 1$ and $\lim_{c \rightarrow +\infty} \alpha(c) = 0$.

Proof of Theorem 1. We shall use the following estimates, which follow immediately from Stirling's formula: If $\frac{1}{2} \leq \gamma < 1$

$$(2.6) \quad A_1 \cdot n^{-1/2} \cdot 2^{n(h(\gamma)-1)} \leq 2^{-n} \sum_{n\gamma \leq K \leq n} \binom{n}{K} \leq B_1 \cdot n^{-1/2} \cdot 2^{n(h(\gamma)-1)}$$

where A_1 and B_1 are positive constants, depending only on γ . Let $c \geq 1$ be fixed, and let α be the unique solution of the equation (2.5) with $0 < \alpha \leq 1$. Let ε be an arbitrary small positive number and put $\alpha' = \alpha + \varepsilon$. It follows from (2.6) that

$$(2.7) \quad P(\vartheta(N, [c \log_2 N]) \geq \alpha') \leq B_1 N^{-\delta_1}$$

where δ_1 is a positive number, depending only on α and ε . Thus the series

$$(2.8) \quad \sum_{j=1}^{+\infty} P(\vartheta(2^{(j+1)/c} - 1, j) \geq \alpha')$$

is convergent, and therefore by the Borel-Cantelli lemma one has

$$(2.9) \quad \vartheta(2^{(j+1)/c} - 1, j) < \alpha'$$

with probability 1 for all but a finite number of values of j . As however

$$(2.10) \quad \vartheta(N, [c \log_2 N]) \leq \vartheta(2^{(j+1)/c} - 1, j) \text{ for } 2^{j/c} \leq N \leq 2^{(j+1)/c} - 1,$$

it follows that with probability one, for all but a finite number of values of N one has

$$(2.11) \quad \vartheta(N, [c \log_2 N]) < \alpha'.$$

As $\varepsilon > 0$ is arbitrary, we obtain

$$(2.12) \quad P(\limsup_{N \rightarrow +\infty} \vartheta(N, [c \log_2 N]) \leq \alpha) = 1.$$

Now let again ε be an arbitrary small positive number, $0 < \varepsilon < \alpha$ and put $\alpha'' = \alpha - \varepsilon$. As

$$(2.13) \quad P(\vartheta(N, K) \leq \alpha'') \leq P\left(\frac{S_{(r+1)K} - S_{rK}}{K} \leq \alpha'', 0 \leq r \leq \frac{N}{K} - 1\right)$$

and because of the independence of the random variables $S_{(r+1)K} - S_{rK}$ ($r = 0, 1, \dots$) it follows that

$$(2.14) \quad P(\vartheta(N, [c \log_2 N]) \leq \alpha'') \leq \left(1 - \frac{A_1 N^{\delta_2}}{N}\right)^{N/([c \log_2 N]) - 1} \leq e^{-(A_2 N^{\delta_2})/\log N}$$

where A_2 and δ_2 are positive constants. Thus the series

$$(2.15) \quad \sum_{N=1}^{\infty} P(\vartheta(N, [c \log_2 N]) \leq \alpha'')$$

is convergent and using again the Borel-Cantelli lemma we get

$$(2.16) \quad P \liminf_{N \rightarrow +\infty} \vartheta(N, [c \log_2 N]) \geq \alpha = 1.$$

As (2.12) and (2.16) imply (2.4), Theorem 1 is proved.

It should be remarked, that the same argument as that used to prove (2.12) can be used to show that if $K(N)$ is an integer-valued function of N such that $\frac{K(N)}{\log N} \rightarrow +\infty$ we have

$$(2.17) \quad P\left(\lim_{N \rightarrow +\infty} \vartheta(N, K(N)) = 0\right) = 1.$$

This result can be interpreted as follows: if $K(N)$ grows faster than $\log N$, then the ordinary law of large numbers applies. On the other hand if $K(N) \leq c \log_2 N$ with $0 < c < 1$ then with probability 1 for all except for a

finite number of values of N there exists at least one $n \leq N - K(N)$ such that $\xi_{n+1} = \xi_{n+2} = \dots = \xi_{n+K(N)} = 1$, which of course implies $\vartheta(N, K(N)) = 1$. Thus the case of real interest is just when $K(N) \sim c \log_2 N$ with $c \geq 1$, and Theorem 1 gives an answer to the question what happens in this case.

§3. The general case.

We shall prove now the following

Theorem 2. *Let $\eta_1, \eta_2, \dots, \eta_n, \dots$, be a sequence of independent, identically distributed nondegenerate random variables. We suppose that the moment generating function*

$$(3.1) \quad \phi(t) = E(e^{t\eta_n})$$

of the common distribution of the η_n exists for $t \in I$ where I is an open interval** containing $t = 0$. Let us suppose that*

$$(3.2) \quad E(\eta_n) = 0.$$

Let α be any positive number such that the function $\phi(t)e^{-\alpha t}$ takes on its minimum in some point in the open interval I and let us put

$$(3.3) \quad \min_{t \in I} \phi(t)e^{-\alpha t} = \phi(\tau)e^{-\alpha\tau} = e^{-(1/C)}.$$

Then $C > 0$ and putting $S_0 = 0$,

$$(3.4) \quad S_n = \eta_1 + \eta_2 + \dots + \eta_n \quad \text{for } n \geq 1$$

and

$$(3.5) \quad \vartheta(N, K) = \max_{0 \leq n \leq N-K} \frac{S_{n+K} - S_n}{K} \quad (1 \leq K \leq N),$$

*we have****

$$(3.6) \quad P\left(\lim_{N \rightarrow +\infty} \vartheta(N, [C \log N]) = \alpha\right) = 1.$$

* $E(\dots)$ denotes the expectation of the random variable in the brackets.

** We suppose that I is the *largest* open interval in which $\phi(t)$ exists.

*** In this and the following §§ $\log N$ denotes the natural logarithm of N .

Proof of Theorem 2. Let us notice first that $\psi(t) = \phi(t)e^{-\alpha t}$ is a strictly convex function: thus τ in (3.3) is determined uniquely. As clearly $\psi(0) = 1$ and in view of (3.2) $\psi'(0) = -\alpha < 0$ it follows that $\tau > 0$ and $\psi(\tau) < 1$ and thus $C > 0$. Let us mention that the condition that $\psi(t)$ takes on its minimum in the interval I is satisfied if for instance $P(\eta_n > \alpha) > 0$ because in this case $\psi(t)$ tends to $+\infty$ if t tends to the upper endpoint of I (which may be the point $+\infty$). We have evidently

$$\frac{\phi'(\tau)}{\phi(\tau)} = \alpha.$$

The proof of Theorem 2 follows exactly that of Theorem 1, only instead of (2.6) we have to use the following result, which under some restrictions is due to *H. Cramér* (see [1]), and in the form needed for our purpose is due to *R. R. Bahadur* and *R. Ranga Rao* (see [2], Theorem 1):

$$(3.7) \quad P(S_n > \alpha n) = \frac{e^{-(n/C)}}{\sqrt{2\pi n}} b_n \cdot (1 + o(1))$$

where b_n is a sequence of positive numbers such that $0 < b \leq b_n \leq B$; if the η_n are not lattice variables, b_n does not depend on n .

Remark. In the special case when $P(\eta_n = \pm 1) = 1/2$, we have $\phi(t) = \frac{1}{2}(e^t + e^{-t})$ therefore if $0 < \alpha < 1$ $\tau = \frac{1}{2} \log \frac{1+\alpha}{1-\alpha}$ and $\frac{1}{C} = \frac{1+\alpha}{2} \log(1+\alpha) + \frac{1-\alpha}{2} \log(1-\alpha)$. Passing to logarithms with base 2 it is easily seen that $e^{-(1/C)} = 2^{h((1+\alpha)/2)-1} = 2^{-(1/c)}$ i.e. $c = C \log 2$. Thus the statement of Theorem 1 for $c > 1$ is contained as a special case in Theorem 2.

§4. The Gaussian case.

Let us consider the special case in which the random variables have a normal distribution with mean 0 and variance 1. (In this case of course S_n is also normally distributed and we do not even need the result (3.7).) As regards the connection between C and α this can be explicitly determined in this special

case: we have evidently for every $\alpha > 0$ $C = \frac{2}{\alpha^2}$, and thus we get from (3.6)

$$(4.1) \quad P(\lim_{N \rightarrow +\infty} \vartheta(N, [C \log N]) = \sqrt{\frac{2}{C}} = 1 \text{ for every } C > 0).$$

From (4.1) one can deduce the following remarkable theorem, due to *P. Lévy* (see [3]): Let $x(t)$ be a Brownian movement process, then

$$(4.2) \quad \lim_{h \rightarrow 0} P\left(|x(t+h) - x(t)| < \lambda \sqrt{2h \log \frac{1}{h}} \text{ for } 0 \leq t \leq 1-h\right) = \begin{cases} 1 & \text{if } \lambda > 1 \\ 0 & \text{if } \lambda < 1. \end{cases}$$

Notice that if the variance of the random variables η_n is equal to 1 then we have in general for $\alpha \rightarrow 0$ $C \sim 2/\alpha^2$; as a matter of fact we have for $t \rightarrow 0$ $\phi'(t) \sim t$ and thus for $\alpha \rightarrow 0$ we get $\tau \sim \alpha$ and therefore $C \sim 2/\alpha^2$. Thus for very small values of α the relation between α and C in Theorem 2 becomes in the limit independent from the distribution of the variables η_n ; however for a fixed not too small value of α the functional relation between α and C depends essentially on the distribution of the random variables η_n . Clearly the reason why the relation between α and C in Theorem 2 depends on the distribution of the variables η_n , is that Theorem 2 is a theorem about big deviations, while the reason for the disappearance of this dependence in the limit if $\alpha \rightarrow 0$ is that if α is decreasing we approach the domain of validity of the central limit theorem.

§5. An application.

Let η_n ($n = 1, 2, \dots$) be a sequence of independent and identically distributed random variables and let $F(x)$ denote their common distribution function. Let us put

$$(5.1) \quad \xi_n = S_n + r_n$$

where S_n is defined by (3.4) and r_n ($n = 1, 2, \dots$) is an arbitrary sequence of bounded random variables such that

$$(5.2) \quad |r_n| \leq R_n \quad \text{where} \quad R_n = o(\log n)$$

(Nothing is supposed concerning the dependence between the variables S_n and r_n). P. Bártfai has proved (see [4]) that if the moment generating function

$$(5.3) \quad \phi(t) = \int_{-\infty}^{+\infty} e^{tx} dF(x)$$

of the variables η_n exists in a neighbourhood of $t = 0$, then given the values ξ_n ($n = 1, 2, \dots$) the distribution function $F(x)$ is thereby uniquely determined with probability one. A new proof of this result of Bártfai can be obtained from Theorem 2 as follows: We may suppose without restricting the generality that $E(\eta_n) = 0$; in this case all conditions of Theorem 2 are satisfied and thus it follows that for $0 < \alpha < a$ where a is a sufficiently small positive number we have (in view of (5.2)) with probability one

$$(5.4) \quad \lim_{N \rightarrow +\infty} \left(\max_{0 \leq n \leq N - [c \log N]} \frac{\xi_{n+[c \log N]} - \xi_n}{[c \log N]} \right) = \alpha.$$

Thus knowing the sequence ξ_n we can determine the functional dependence between α and c .

To prove Bártfai's theorem we shall need the following

Theorem 3. *The functional dependence between α and $c = c(\alpha)$ in Theorem 2 determines the distribution of the random variables η_n uniquely.*

Proof. If the function $c = c(\alpha)$ is given for $0 < \alpha < a$, we can determine the function

$$(5.5) \quad \lambda(\alpha) = e^{-(1/c(\alpha))}$$

and thus also the function

$$(5.6) \quad \frac{\lambda'(\alpha)}{\lambda(\alpha)} = -\tau.$$

As clearly $\tau = \tau(\alpha)$ is an increasing function of α , its inverse function $\alpha = \alpha(\tau)$ can also be determined. This means however that we can determine the function

$$(5.7) \quad \phi(\tau) = \alpha(\alpha(\tau))e^{\tau\alpha(\tau)}$$

in some interval $0 \leq \tau \leq \tau_0$. As it is well known that the moment-generating function $\phi(t)$ determines the distribution function $F(x)$ uniquely, (even if $\phi(t)$ is given only in some interval, it being an analytic function if it exists), the statement of Theorem 3 follows.

It follows from Theorem 3 that in the stochastic geyser problem if we know a single realization of the sequence ζ_n ($n = 1, 2, \dots$) we can determine the distribution function $F(x)$ with probability one; this proves *Bárfai's* theorem.

REFERENCES

1. H. Cramér, *Sur un nouveau théorème-limite de la théorie des probabilités*. Actualités Scientifiques et Industrielles, No 736, Hermann et Cie, Paris, 1938.
2. R. R. Bahadur and R. Ranga Rao, On deviations of the sample mean, *Annals of Mathematical Statistics*, 31 (1960), 1015–1027.
3. P. Lévy, *Théorie de l'addition des variables aléatoires indépendantes*, Paris, Gauthier-Villars.
4. P. Bárfai, Die Bestimmung der zu einem wiederkehrenden Prozess gehörenden Verteilungsfunktion aus den mit Fehlern behafteten Daten einer einzigen Realisation. *Studia Scientiarum Mathematicarum Hungarica*, 1 (1966), 161–168.

NOTE

First of all we make some remarks to the paper itself.

(1) In the proof of Theorem 2 the theorem of Chernoff can be applied instead of the theorem of Bahadur and Rao, therefore condition (3.3) can be replaced by the following weaker one: Let α be any positive number with the property $P(\eta_1 \geq \alpha) > 0$ and put

$$C = \frac{1}{\log \frac{1}{\varrho(\alpha)}}$$

where $\varrho(\alpha) = \inf_{t \in I} e^{-\alpha t} \Phi(t)$. (The remark in the proof that $P(\eta_1 > \alpha) > 0$ ensures the validity of condition (3.3), is evidently false.)

(2) As a matter of fact Rényi proved a slightly sharpened version of Bárfai's theorem, namely, the boundedness of r_n in condition (5.2) is superfluous. (See also the comment to No. 355.)

(3) Theorem 3 can be proved also by the inversion formula

$$\Phi(t) = \sup_x e^{tx} \varrho(x)$$

(see [1]). (P. B.)

In [2] Komlós and Tusnády determined the limit distribution of $\vartheta(N, K)$ and analyzed the index process $\left\{n : \frac{S_{n+K} - S_n}{K}\right\}$ with $K \sim C \log n$. (P. B.)

REFERENCES

- [1] Bártfai, P.: Connection between the convex analysis and the theory of large deviations. *Z. Wahrscheinlichkeitstheorie* (to appear).
- [2] Komlós, J. and Tusnády, G.: On the "pure heads". *Annals of Probability* (to appear).
- [3] Book, S. A.: The Erdős - Rényi new law of large numbers for weighted sums. *Proc. Amer. Math. Soc.*, **38** (1973), 165 - 171.

The Prüfer code for k -trees

by

C. Rényi and A. Rényi

Budapest, Hungary

§ 1. INTRODUCTION

The notion of k -trees (k -dimensional trees) for $k \geq 2$, which is a natural generalization of the notion of an ordinary (one-dimensional) tree (a "1-tree"), has been introduced by F. HARARY and E. M. PALMER [1]. A k -tree can be defined either as a k -dimensional simplicial complex with certain properties, or as a graph; in what follows, we take the second point of view.

The simplest way to define a k -tree of order n ($k = 1, 2, \dots; n \geq k+1$)

The results of this paper have been obtained during June and July 1969. The results of § 2 - on which everything else in this paper is based - are due almost exclusively to Catherine Rényi. Alas, Catherine Rényi died on August 23, 1969. It remained the duty of the author named second to prepare the final text of the present paper; thus all possible shortcomings of the paper are his responsibility.

is to do this recursively. A k -tree of order $k+1$ is a complete graph of order $k+1$. A k -tree $G_{n+1}^{(k)}$ of order $n+1$ ($n \geq k+1$) is obtained by taking an arbitrary k -tree $G_n^{(k)}$ of order n and selecting any of its points which form a complete k -graph in $G_n^{(k)}$ and by connecting these k points with a new point*. Thus a k -tree of order n is a graph having n points, $\binom{k+1}{2} + k(n-k-1)$ edges and, in general, for every j with $1 \leq j \leq k+1$ containing $\binom{k+1}{j} + (n-k-1) \cdot \binom{k}{j-1}$ complete j -graphs: thus in particular it contains $n-k$ complete $(k+1)$ -graphs and $k(n-k)+1$ complete k -graphs.

A point of a k -tree is called an endpoint if it belongs only to a single complete $(k+1)$ -graph of the k -tree. Clearly each of the $k+1$ points of a k -tree of order $k+1$ is an endpoint. It is easy to see that every k -tree of order $n \geq k+2$ contains at least 2 and at most $n-k$ endpoints; this follows immediately from the recursive definition, because a k -tree of order $k+2$ contains evidently 2 endpoints, and by forming from a given k -tree $G_n^{(k)}$ of order n , a k -tree of order $n+1$ by adding to $G_n^{(k)}$ a new point, and joining it to the points of a complete k -graph in $G_n^{(k)}$, the number of endpoints is never decreased.

In what follows we shall consider labelled k -trees, i.e. we suppose that the n points of a k -tree of order n are labelled by the numbers $1, 2, \dots, n$. For the sake of brevity we shall call the point labelled by the number j "the point j ". We shall deal mainly with rooted k -trees; a k -tree of order n is called rooted at the root $(\varphi_1, \varphi_2, \dots, \varphi_k)$ where $(\varphi_1, \varphi_2, \dots, \varphi_k)$ is an unordered k -tuple of different integers chosen from the integers $1, 2, \dots, n$, if the complete k -graph consisting of the points $\varphi_1, \dots, \varphi_k$ is contained in the k -tree in question. Notice that a 1-tree is rooted at any one of its points; however a k -tree with $k \geq 2$ is rooted only at $k(n-k)+1$ k -tuples among the possible $\binom{n}{k}$ k -tuples which can be formed from the integers $1, 2, \dots, n$. In the case $k=1$ the only consequence of looking at a 1-tree as rooted at one of

* In [1] a complete k -graph is called a k -tree of order k ; we found it more convenient not to consider such a graph as a k -tree, i.e. to define k -trees of order n only for $n > k+1$.

its points, say q , is that the root q is not considered as an endpoint, even if it is connected with a single point. Similarly for $k \geq 2$ the k points belonging to the root are not considered as endpoints even if they belong to a single complete $(k+1)$ -graph.

Notice that every rooted k -tree contains at least one endpoint (not belonging to the root). This is trivial for $k = 1$ because every 1-tree contains at least 2 endpoints, of which at least one is different from the root. For $k \geq 2$, the statement follows from the remark (proved easily by induction) that every tree contains at least two endpoints which are not contained in the same complete k -graph, and thus if the k -tree is rooted, at least one of them does not belong to the root.

The aim of the present paper is to extend to k -trees the method by which A. PRÜFER [2] has coded 1-trees. In what follows we shall define the Prüfer code of a 1-tree of order n for 1-trees rooted at some selected point: for the sake of simplicity we suppose that the tree is rooted at the point n .

Prüfer's code is defined for labelled 1-trees of order n (the n points of which are labelled by the numbers $1, 2, \dots, n$) as follows: we remove from the tree the endpoint which is labelled by the least number among all endpoints of the tree, and write down the number by which the unique point of the tree, to which the removed endpoint was connected, is labelled; we repeat the same procedure with the remaining 1-tree of order $n-1$, and continue this process until there remains only a single edge (a 1-tree of order 2). In this way we obtain a sequence of length $n-2$, each element of which is one of the numbers $1, 2, \dots, n$. It can be shown that each of such n^{n-2} sequences is the Prüfer codeword of a tree of order n , and this tree can be reconstructed, given the codeword. In the case $k \geq 2$ the Prüfer code of a labelled k -tree of order n (the points of which are labelled by the numbers $1, 2, \dots, n$) and rooted at a given k -tuple $(q_1, q_2, \dots, q_k)$ is defined similarly: we remove from the k -tree that endpoint which is labelled by the least number among all endpoints of the k -tree, and write down the (unordered) k -tuple of those numbers by

which the k points connected to the removed endpoint are labelled. We repeat the same procedure with the remaining k -tree of order $n-1$, and continue this process until there remains only a complete $(k+1)$ -graph (i.e. a k -tree of order $k+1$). In this way we obtain a sequence of $n-k-1$ unordered k -tuples of the numbers $1, 2, \dots, n$; however, if $k \geq 2$, not all such sequences are the codewords of a k -tree of order n , but only those which satisfy certain conditions of admissibility. The problem to be solved consists just in finding these conditions, i.e. in characterizing those sequences of $n-k-1$ unordered k -tuples, formed from the numbers $1, 2, \dots, n$, which are the Prüfer codewords of a k -tree of order n ; the solution of this characterization problem will lead also to a decoding procedure by which the k -tree can be reconstructed from its Prüfer codeword.

While the coding procedure can be generalized in a straightforward way, it will be seen that the characterization of those sequences which are the codewords of a k -tree, and the decoding procedure are much more involved for $k \geq 2$. It appeared that to solve this problem, a much more thorough study of the original Prüfer code in the case $k=1$ was needed than was done previously. This study involved a certain coding of permutations which seems not to have been used before. In § 2 we start by discussing this coding of permutations; § 3 contains a detailed study of the Prüfer code for ordinary trees, based on the introduction of the notion of the "redundant Prüfer code" of a k -tree. In § 4 it will be shown that generalizing for any $k \geq 2$ for (rooted) k -trees the notion of the redundant Prüfer code the problem of characterization as well as of decoding are solved without encountering any further difficulty. In § 5 we show how the Prüfer code can be used for counting all labelled k -trees of order n as well as for enumerating k -trees of order n satisfying certain conditions.

§ 2. CODING OF PERMUTATIONS

Let $\pi_n = (\alpha_1, \alpha_2, \dots, \alpha_n)$ be a permutation of the numbers

$1, 2, \dots, n$. We call an element a_{k+1} of the permutation π_n ($1 \leq k \leq n-1$) a weak element, if it is preceded by a larger number, i.e. if $\max_{1 \leq j \leq k} a_j > a_{k+1}$; otherwise we call a_{k+1} a strong element of the permutation π_n ; a_1 is always a strong element.*

Let $e_k(\pi_n)$ denote the number of elements a_j ($j = 1, 2, \dots, k$) which are larger than a_{k+1} ($k = 1, 2, \dots, n-1$); thus for any permutation π_n of order n we have $0 \leq e_k(\pi_n) \leq k$ and a_{k+1} is a weak element if and only if $e_k(\pi_n) \neq 0$. We now shall prove a series of lemmas.

LEMMA 1. To every sequence $e_1, e_2, \dots, e_{n-1}$ of integers for which $0 \leq e_k \leq k$ ($k = 1, 2, \dots, n-1$) there corresponds a uniquely determined permutation π_n of integers $1, 2, \dots, n$ such that $e_k(\pi_n) = e_k$ ($k = 1, 2, \dots, n-1$).

PROOF. The permutation π_n in question can be successively constructed starting from its last element and working successively backwards. As a matter of fact, as a_n has to be preceded by e_{n-1} larger numbers, evidently $a_n = n - e_{n-1}$. Let us now omit a_n from the sequence $1, 2, \dots, n$; evidently a_{n-1} is obtained by taking the element having the rank $n-1 - e_{n-2}$ in the remaining sequence; similarly, if we have already determined $a_n, a_{n-1}, \dots, a_{k+2}$, let us omit these numbers from the sequence $1, 2, \dots, n$; a_{k+1} ($1 \leq k \leq n-1$) will be equal to the element having the rank $k+1 - e_k$ in the remaining sequence, while a_1 will be the unique number of the sequence $1, 2, \dots, n$ which remains after removing $a_n, a_{n-1}, \dots, a_2$.

Thus we obtained that any permutation π_n of the elements $1, 2, \dots, n$ can be coded by the sequence $e_k(\pi_n)$ ($k = 1, 2, \dots, n-1$).

Let this code be called in what follows the CR-code of the permutation π_n . This code is closely related to another code, due to M. HALL (see [4]), which is defined as follows: Let $u_k(\pi_n)$ denote the number of those numbers less than $k+1$ which follow the number $k+1$ in π_n ; then we have

* A strong element is sometimes called an upper record, see e.g. [3].

$0 \leq u_k(\pi_n) \leq k$ and the permutation π_n is uniquely determined by the codeword $u_1(\pi_n), u_2(\pi_n), \dots, u_{n-1}(\pi_n)$; we shall call this coding the MH-code.

It is easy to show that the CR code of a permutation π_n is equal to the MH code of its conjugate permutation π_n^* ; as a matter of fact if in π_n $a_{k+1} = j$, then in π_n^* $a_j^* = k+1$ and if there are in π_n e_k numbers greater than $a_{k+1} = j$ among the numbers $a_1, a_2, \dots, a_k$, then in π_n^* there are e_k numbers less than $k+1$ among the numbers $a_{j+1}^*, \dots, a_n^*$.

It is pointed out in [4] that the coding of permutations is of importance in computer programming.

Now we prove

LEMMA 2. The number of those permutations $(a_1, a_2, \dots, a_n)$ of the numbers $1, 2, \dots, n$ in which the elements a_{h_i+1} ($i = 1, 2, \dots, r$; $1 \leq h_1 < h_2 < \dots < h_r < n$) are weak and all others strong ($r \leq n-1$) is equal to $h_1 h_2 \dots h_r$.

PROOF of LEMMA 2. Let $(e_1, e_2, \dots, e_{n-1})$ be the CR codeword of a permutation satisfying the requirements of Lemma 2. Then clearly $1 \leq e_{h_i} \leq h_i$ ($i = 1, 2, \dots, r$) while if j does not belong to the sequence $h_1, h_2, \dots, h_r$ then $e_j = 0$. Thus the total number of such permutations is equal to the number of ways in which the numbers $e_{h_1}, e_{h_2}, \dots, e_{h_r}$ can be chosen, i.e. is equal to $h_1 h_2 \dots h_r$ which was to be proved.

REMARK 1. Let us consider the trivial identity

$$(2.1) \quad n! = \prod_{h=1}^{n-1} (h+1) = \sum_{1 \leq h_1 < h_2 < \dots < h_r \leq n-1} h_1 h_2 \dots h_r$$

Lemma 2 furnishes a combinatorial interpretation of the identity (2.1): the left-hand side is equal to the total number of permutations of the elements $1, 2, \dots, n$ while the term $h_1 h_2 \dots h_r$ on the right-hand side gives

the number of those permutations in which the elements α_{h_i+1} ($i = 1, 2, \dots, r$), and only these, are weak.

REMARK 2. It follows from the proof of Lemma 1, that if we want to list all permutations satisfying the requirements of Lemma 2, we may proceed as follows: α_{h_r+1} can take the values $1, 2, \dots, h_r$. If the value of α_{h_r+1} is fixed, remove this value from the sequence $1, 2, \dots, n$; $\alpha_{h_{r-1}+1}$ can be equal to any of the first h_{r-1} elements of the remaining sequence; in general if the values of $\alpha_{h_r+1}, \dots, \alpha_{h_i+1}$ ($1 \leq i \leq r-1$) are already fixed, remove these from the sequence $1, 2, \dots, n$, and take α_{h_i+1} to be any one of the first h_i terms of the remaining sequence. Thus working backwards we find all possible choices of the weak elements. The strong elements are then uniquely determined, as they are equal to the remaining $n-r$ numbers in natural order.

REMARK 3. Let us choose at random with uniform distribution one of the $n!$ permutations of the numbers $1, 2, \dots, n$; let this permutation be $\pi_n = (\alpha_1, \alpha_2, \dots, \alpha_n)$. Let $P(n; m_1, m_2, \dots, m_s)$ denote the probability that $\alpha_1, \alpha_{m_1+1}, \dots, \alpha_{m_s+1}$ ($1 \leq m_1 < m_2 < \dots < m_s \leq n-1$) and only these, are the strong elements (upper records) of the random permutation π_n . Denote by $h_1+1, \dots, h_r+1$ ($r = n-s-1$) those among the numbers $1, 2, \dots, n$ which are not contained in the sequence $1, m_1+1, \dots, m_s+1$. Then we have by Lemma 2,

$$(2.2) \quad P(n; m_1, m_2, \dots, m_s) = \frac{h_1 h_2 \dots h_r}{n!} = \frac{1}{n m_1 m_2 \dots m_s}$$

This formula can be found in DAVID and BARTON [3]; the proof given here by means of Lemma 2 is, however, much simpler than the proof in [3].

REMARK 4. The result of Lemma 2 can be also interpreted as follows: let us choose at random with uniform distribution one of the permutations of order n . Let this be $\pi_n = (\alpha_1, \alpha_2, \dots, \alpha_n)$.

Put $\varepsilon_h = 0$ if α_{h+1} is a weak element and $\varepsilon_h = 1$ if α_{h+1} is a strong element of π_n ($h = 0, 1, \dots, n-1$).

Then we have

$$(2.3) \quad P(\varepsilon_h = 1) = \frac{1}{h+1} \quad \text{and} \quad P(\varepsilon_h = 0) = \frac{h}{h+1}$$

($h = 0, 1, \dots, n-1$) and the random variables $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}$ are independent. It follows that putting $S_n = \varepsilon_0 + \varepsilon_1 + \dots + \varepsilon_{n-1}$ i.e. denoting by S_n the total number of strong elements of the random permutation π_n , we have, denoting by $E(\xi)$ the expectation and by $D^2(\xi)$ the variance of a random variable ξ , and by $P(A)$ the probability of an event A ,

$$(2.4) \quad E(S_n) = 1 + \frac{1}{2} + \dots + \frac{1}{n} \sim \log n$$

and

$$(2.5) \quad D^2(S_n) = \sum_{k=1}^n \left(\frac{1}{k} - \frac{1}{k^2} \right) \sim \log n$$

and it is easy to show that the distribution of $\frac{S_n - \log n}{\sqrt{\log n}}$ tends for $n \rightarrow +\infty$ to the standard normal distribution, i.e.

$$(2.6) \quad \lim_{n \rightarrow +\infty} P\left(\frac{S_n - \log n}{\sqrt{\log n}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du$$

It is interesting to compare this result with a related result on sequences of independent observations (see [5]).

§ 3. THE REDUNDANT PRÜFER CODE FOR 1-TREES

Let us consider a labelled 1-tree T_n of order n , rooted at n , and let us perform the process by which its Prüfer codeword is obtained as described in the introduction. Let the least endpoint of T_n be a_1 , and the point with which this endpoint is connected be b_1 ; after removing the point a_1 , let a_2 be the least endpoint of the remaining tree, and b_2 the point to which it is connected; in general, after removing $j-1$ points, let a_j be the least endpoint, and b_j the point with which a_j is connected ($1 \leq j \leq n-2$); after removing $n-2$ points only a single edge remains, one of the endpoints of which is the root n ; let a_{n-1} be its other endpoint and put $b_{n-1} = n$.

Let us consider the matrix consisting of two rows and $n-1$ columns

$$(3.1) \quad \begin{pmatrix} a_1, a_2, \dots, a_{n-1} \\ b_1, b_2, \dots, b_{n-1} \end{pmatrix}$$

We call the matrix (3.1) the redundant Prüfer codeword of the 1-tree T_n rooted at n , clearly $(b_1, b_2, \dots, b_{n-1})$ is the usual Prüfer codeword which we call the primitive Prüfer codeword of the tree T_n . We shall prove a series of lemmas about the redundant Prüfer code.

LEMMA 3. The redundant Prüfer codeword (3.1) is uniquely determined by the primitive Prüfer codeword $(b_1, b_2, \dots, b_{n-1})$ and can be obtained from the latter in the following way:

- 1) $b_{n-1} = n$,
- 2) a_1 is the least integer not contained in the sequence $b_1, b_2, \dots, b_{n-1}$
- 3) for every j with $1 \leq j \leq n-1$ a_j is the least integer not contained among the numbers $a_1, a_2, \dots, a_{j-1}, b_j, b_{j+1}, \dots, b_{n-1}$.

PROOF. Lemma 3 follows immediately from the rule of construction of the primitive Prüfer code and the definition of the redundant Prüfer code.

REMARK. Lemma 3 contains the rule for decoding the primitive Prüfer code, i.e. the algorithm for reconstructing the tree, given its primitive Prüfer code. We first construct the redundant Prüfer code according to Lemma 3; as clearly (a_j, b_j) ($j = 1, 2, \dots, n-1$) are all the edges of the tree in question, once the redundant Prüfer code is given, the tree can be immediately obtained from it.

As usual, we define the degree of a point of a graph as the number of other points of the graph to which it is connected by an edge. We prove now

LEMMA 4. Every number j ($1 \leq j \leq n$) occurs d_j times in the redundant Prüfer code of a tree, where d_j denotes the degree of the point in the tree. If $1 \leq j \leq n-1$ then j occurs just once in the upper row and d_j-1 times in the lower row, at places with indices less than the index of its occurrence in the upper row. The number n occurs d_n times in the lower row.

PROOF. Lemma 4 follows from Lemma 3, and from the definition of the redundant Prüfer code.

REMARK. As $b_{n-1} = n$, Lemma 3 implies the well known fact that every number j ($1 \leq j \leq n$) occurs d_j-1 times in the primitive Prüfer code $(b_1, b_2, \dots, b_{n-2})$.

LEMMA 5. The upper row $(a_1, a_2, \dots, a_{n-1})$ of the redundant Prüfer code of a 1-tree of order n rooted at the point n , is a permutation of the numbers $1, 2, \dots, n-1$. If a_{h+1} is a weak element of this permutation, then we have

$$(3.1) \quad b_h = a_{h+1} \quad (1 \leq h \leq n-2)$$

PROOF. The first statement of Lemma 5 follows immediately from Lemma 4. As regards the second statement let a_{h+1} be a weak element of the permutation $(a_1, a_2, \dots, a_{n-1})$ and let j be the largest natural number not exceeding h such that $a_j > a_{h+1}$. We shall prove the statement $a_{h+1} = b_h$

by induction on the value of $t = h+1-j$. If $t = 1$, i.e. if $a_h > a_{h+1}$, let us put $a_{h+1} = v$ and $a_h = u$.

According to Lemma 3, u is the least number not occurring among the numbers $a_1, a_2, \dots, a_{h+1}, b_h, b_{h+1}, \dots, b_{n-1}$; b_{n-1} ; and v the least number not occurring among $a_1, a_2, \dots, a_{h-1}, u, b_{h+1}, \dots, b_{n-1}$.

It follows that v occurs among the numbers $a_1, \dots, a_{h-1}, b_h, b_{h+1}, \dots, b_{n-1}$ but it does not occur among $a_1, \dots, a_{h-1}, b_{h+1}, \dots, b_{n-1}$;

this is possible only if $b_h = v = a_{h+1}$. Thus our statement holds for $t = 1$.

Suppose it holds for $t = 1, 2, \dots, m$; we shall show that it holds for $t = m+1$ too. Suppose that $a_{h-m} > a_{h+1}$ and $a_j < a_{h+1}$ for $j = h-m+1, \dots, h$.

It follows that $a_h, a_{h-1}, \dots, a_{h-m+1}$ are all weak elements of the permutation $(a_1, a_2, \dots, a_{n-1})$ and by the induction hypothesis it follows that $b_j = a_{j+1}$ for $j = h-1, \dots, h-m$. Now the value $a_{h+1} = v$ has to occur among the numbers $a_1, \dots, a_{h-m+1}, b_{h-m}, \dots, b_{n-1}$ because otherwise a_{h-m} would have the value v and not a larger value; as, however, the numbers a_i are all different, v can be equal only to b_h , i.e. $b_h = v = a_{h+1}$; this means that $b_h = a_{h+1}$ holds for $t = m+1$ too, and thus the second statement of Lemma 5 follows by induction.

REMARK 1. Notice that the converse of the second statement of Lemma 5 does not hold: $b_h = a_{h+1}$ does not imply that a_{n+1} is a weak element of the permutation $(a_1, a_2, \dots, a_{n-1})$.

REMARK 2. Clearly $a_{h+1} = j$ is a weak element of the permutation $(a_1, \dots, a_{n-1})$ if and only if there exists in the tree a path starting from the root, passing through the point j and arriving to a point $k > j$. In this case we call the point j a weak point of the tree.

Now we are in the position to prove

LEMMA 6. Let $\pi_{n-1} = (a_1, a_2, \dots, a_{n-1})$ be a permutation of the numbers $1, 2, \dots, n-1$. Let $\tau_1(n, \pi_{n-1})$ denote the number of those labelled 1-trees of order n , rooted at n , the upper row of the redundant Prüfer

codeword of which is equal to the sequence π_{n-1} . Let $a_{h_1+1}, a_{h_2+1}, \dots, a_{h_r+1}$ be the weak elements of the permutation π_{n-1} . Then we have

$$(3.2) \quad T_1(n, \pi_{n-1}) = \prod_{\substack{h=1 \\ h \neq h_i (1 \leq i \leq r)}}^{n-2} (n-h)$$

PROOF. According to Lemma 5 we have $b_{h_i} = a_{h_i+1}$ for $i = 1, 2, \dots, r$ further we have by definition $b_{n-1} = n$.

If h ($1 \leq h \leq n-2$) is not one of the numbers $h_1, \dots, h_r$ then b_h can take on any value different from $a_1, a_2, \dots, a_h$ because according to Lemma 4 the value a_j can occur in the lower row of the redundant Prüfer code only at a place with index $h < j$, i.e. we have $b_h \neq a_j$ if $j < h$. Thus there are $n-h$ possible choices for the value of b_h if h is not one of the numbers $h_1, h_2, \dots, h_r$; this implies that (3.2) holds.

REMARK. Evidently one has, denoting by S_{n-1} the set of all $(n-1)!$ permutations of the numbers $1, 2, \dots, n-1$ and by $T_1(n)$ the total number of labelled 1-trees of order n ,

$$(3.3) \quad T_1(n) = \sum_{\pi_{n-1} \in S_{n-1}} T_1(n, \pi_{n-1}).$$

According to Lemma 2 the total number of permutations is $\pi_{n-1} \in S_{n-1}$ in which the weak elements are $a_{h_1+1}, \dots, a_{h_r+1}$ ($1 \leq h_1 < h_2 < \dots < h_r \leq n-2$) is $h_1 h_2 \dots h_r$. Thus it follows that

$$(3.4) \quad \begin{aligned} T_1(n) &= \sum_{1 \leq h_1 < h_2 < \dots < h_r \leq n-1} h_1 h_2 \dots h_r \prod_{\substack{h=1 \\ h \neq h_i (1 \leq i \leq r)}}^{n-2} (n-h) = \\ &= \prod_{h=1}^{n-2} (h+n-h) = n^{n-2}. \end{aligned}$$

i.e. we obtain in this way a proof of Cayley's well-known formula

$$(3.5) \quad T_1(n) = n^{n-2}$$

for the total number of labelled trees of order n . Of course, for 1-trees this proof of (3.5) is unnecessarily complicated, and it is much easier to enumerate trees of order n by remarking that each element of the primitive Prüfer codeword can be chosen in n ways, and thus there are n^{n-2} possibilities; however, it will be seen in § 4 that in counting k -trees of order n in the case $k \geq 2$ this simple method of counting cannot be easily generalized, while Lemma 6 can be easily generalized for k -trees for every k (see Lemma 6*), and this leads to a method for enumerating all k -trees of order n as well for counting the number of k -trees having certain prescribed properties.

From what has been said we get immediately the following result on the number of weak points of a random 1-tree. As usual, a random 1-tree of order n is defined as a 1-tree chosen at random, with uniform distribution, among the n^{n-2} possible labelled 1-trees of order n . (For the definition of weak points, see Remark 2 to Lemma 5.)

THEOREM 1. Let $W(n, r)$ denote the probability that a random labelled 1-tree of order n , rooted at the point n , should contain exactly r weak points; then we have

$$\sum_{r=0}^{n-2} W(n, r) x^r = \prod_{h=1}^{n-2} \left(1 + \frac{h}{n} (x-1) \right).$$

Thus if V_n is the number of weak points in a random labelled tree of order n we have

$$E(V_n) = \frac{n}{2} \left(1 - \frac{1}{n} \right) \left(1 - \frac{2}{n} \right)$$

$$D^2(V_n) = \frac{n}{6} \left(1 - \frac{1}{n} \right) \left(1 - \frac{2}{n} \right) \left(1 + \frac{3}{n} \right)$$

and

$$\lim_{n \rightarrow +\infty} P\left(\frac{\sqrt{n} - \frac{n}{2}}{\sqrt{\frac{n}{6}}} < x\right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du,$$

i.e. the number of weak points of a random 1-tree of order n (rooted at the point n) is for large n approximately normally distributed around $\frac{n}{2}$ with variance $\frac{n}{6}$.

REMARK 1. It is interesting to compare Theorem 1 with previous results on the number of inversions of a random 1-tree (see [8] and [9]). The points j_1 and j_2 of a random 1-tree are said to be in inversion if $j_1 < j_2$ and the path from the point j_2 to the point n passes through the point j_1 .

REMARK 2. Notice that an endpoint of a 1-tree is never weak. As it is known (see [10]) that the number of endpoints of a random 1-tree of order n is for large n approximately normally distributed with mean value $\frac{n}{e}$ and variance $\frac{n}{e} \left(1 - \frac{2}{e}\right)$, it follows e.g. that the expected number of points of a random 1-tree, which are neither endpoints nor weak points, is asymptotically equal to $n\left(\frac{1}{2} - \frac{1}{e}\right)$ for $n \rightarrow +\infty$.

§ 4. THE CHARACTERIZATION OF PRÜFER CODEWORDS FOR k -TREES

Let us now generalize the results of the previous § for k -trees with $k \geq 2$. We consider labelled k -trees of order n rooted at a given complete k -graph, which can be taken without restricting the generality as consisting of the points labelled by the numbers $n-k+1, n-k+2, \dots, n$. In other words, we consider the set of all k -trees of order n , the points of which are labelled by the numbers $1, 2, \dots, n$ and which contain the complete graph formed by the points $n-k+1, n-k+2, \dots, n$. First we define the redundant Prüfer codeword of such a tree. This codeword is a matrix

$$(4.1) \quad \begin{pmatrix} a_1, a_2, \dots, a_{n-k} \\ B_1, B_2, \dots, B_{n-k} \end{pmatrix}$$

where $(a_1, a_2, \dots, a_{n-k})$ is a permutation of the numbers $1, 2, \dots, n-k$, while B_i ($1 \leq i \leq n-k$) is a k -tuple of different integers taken from the numbers $1, 2, \dots, n$. The redundant Prüfer codeword of a k -tree T , rooted at the k -tuple $(n-k+1, n-k+2, \dots, n)$, is obtained as follows: a_1 is the least endpoint of the tree, and B_1 is the k -tuple of those points to which a_1 is connected; a_2 is the least endpoint of the tree $T^{(1)}$ obtained after removing from T the point a_1 (and of course all k edges connecting a_1 with a point belonging to B_1) and B_2 is the k -tuple of those points of $T^{(1)}$ which are connected in $T^{(1)}$ to a_2 ; in general a_{j+1} is the least endpoint of the tree $T^{(j)}$ obtained by removing from T the points $a_1, a_2, \dots, a_j$ and all edges starting at these points, while B_{j+1} is the k -tuple of those points in $T^{(j)}$ which are connected to a_{j+1} (in $T^{(j)}$) ($j = 1, 2, \dots, n-k+1$). (Remember that the points of the root are not endpoints.) It is easy to see that Lemmas 3, 4 and 5 can be generalized to k -trees for any k ; the corresponding statements are as follows:

Lemma 3*. The redundant Prüfer codeword (4.1) of a k -tree is uniquely determined by the primitive Prüfer codeword $(B_1, B_2, \dots, B_{n-k-1})$ and can be obtained from the latter in the following way:

- 1) B_{n-k} is the k -tuple $(n-k+1, n-k+2, \dots, n)$ (i.e. the root);
- 2) a_1 is the least integer not contained among the elements of the k -tuples B_i ($i = 1, 2, \dots, n-k$);
- 3) For every j , with $1 < j \leq n-k$, a_j is the least integer different from the numbers $a_1, a_2, \dots, a_{j-1}$ and not contained among the elements of the k -tuples $B_j, B_{j+1}, \dots, B_{n-k}$.

In the same way as in the special case $k=1$ Lemma 3* contains

the algorithm for decoding the primitive Prüfer code of a k -tree: first one has to construct from the primitive codeword the redundant codeword according to the rules laid down in Lemma 3*; if this is done, the k -tree in question is already defined because evidently the edges of the k -tree are those connecting two points belonging to at least one $(k+1)$ -tuple C_j where C_j consists of α_j and of the k points forming the k -tuple B_j ($j = 1, 2, \dots, n-k$). (Notice that the C_j ($j = 1, 2, \dots, n-k$) are all complete $(k+1)$ -graphs contained in the k -tree in question, and the same edge may belong to several of these complete $(k+1)$ -graphs.)

Before generalizing Lemma 4 for $k \geq 2$, we introduce a definition: the degree of a complete k -graph G formed by k of the points $1, 2, \dots, n$ in a k -tree T , is defined as the number of those complete $(k+1)$ -graphs contained in T which contain G .

Now we can formulate

Lemma 4*. Every k -tuple B of k of the integers $1, 2, \dots, n$ belongs to $d(B)$ of the $(k+1)$ -tuples $C_j = (\alpha_j, B_j)$ ($j = 1, 2, \dots, n-k$) where $d(B)$ is the degree of the complete k -graph consisting of the k points of B . The root $R = (n-k+1, n-k+2, \dots, n)$ occurs $d(R)$ times among the k -tuples $B_1, B_2, \dots, B_{n-k}$, while every other k -tuple B for which $d(B) \geq 1$ occurs just once as the subset of a $(k+1)$ -tuple $C_j = (\alpha_j, B_j)$ such that B is not identical with B_j (i.e. such that $\alpha_j \in B$), and B occurs $d(B) - 1$ times among the k -tuples B_i with $i < j$.

Finally the generalization of Lemma 5 for $k \geq 2$ is as follows:

Lemma 5*. The upper row $(\alpha_1, \alpha_2, \dots, \alpha_{n-k})$ of the redundant Prüfer codeword of a k -tree, rooted at the k -tuple $(n-k+1, \dots, n)$ is a permutation of the numbers $1, 2, \dots, n-k$. If α_{n+1} is a weak element of the permutation $(\alpha_1, \dots, \alpha_{n-k})$ then α_{n+1} is contained in the k -tuple B_h ($1 \leq h \leq n-k-1$).

The proofs of Lemmas 3*, 4*, 5* are almost word for word the

same in the case $k \geq 2$ as for $k=1$; therefore there is no need to go into details except for the second statement of Lemma 5*, the proof of which in the general case is slightly more involved. This proof is as follows: let α_{h+1} be a weak element of the permutation $(\alpha_1, \dots, \alpha_{n-k})$ and let j be the largest number not exceeding h such that $\alpha_j > \alpha_{h+1}$, and put $t = h+1-j$; we apply induction on t as we have done for the special case $k=1$. If $t=1$, i.e. if $\alpha_h > \alpha_{h+1}$ put $\alpha_{h+1} = v$ and $\alpha_h = u > v$. According to Lemma 3*, u is the least number different from $\alpha_1, \dots, \alpha_{h-1}$ and not belonging to any of the k -tuples $B_h, B_{h+1}, \dots, B_{n-k}$ and v the least number different from $\alpha_1, \alpha_2, \dots, \alpha_{h-1}, u$ and not occurring among the elements of the k -tuples $B_{h+1}, \dots, B_{n-k}$; as $v < u$ this is possible only if v belongs to B_h . Thus our statement holds for $t=1$. Suppose our statement holds for $t=1, 2, \dots, m$; we show that it holds for $t=m+1$ too. Suppose that $\alpha_{h-m} > \alpha_{h+1}$ and $\alpha_j < \alpha_{h+1}$ for $j = h-m+1, \dots, h$. It follows that $\alpha_h, \alpha_{h-1}, \dots, \alpha_{h-m+1}$ are all weak elements of the permutation $(\alpha_1, \alpha_2, \dots, \alpha_{n-k})$ and thus by the induction hypothesis it follows that $\alpha_{j+1} \in B_j$ for $j = h-1, \dots, h-m$.

Now the value $\alpha_{h+1} = v$ has to occur among the elements of at least one of the k -tuples $B_{h-m}, B_{h-m+1}, \dots, B_h$; let j be the largest integer such that $v \in B_j$ ($j \leq h$) if we would have $j \leq h-1$ then both α_{j+1} and v would belong to B_j . Now the k -tuple B_j has to occur in just one $(k+1)$ -tuple $C_i = (\alpha_i, B_i)$ ($i > j$) so that $B_j \neq B_i$, i.e. $\alpha_i \in B_j$; if this would happen for $i = h+1$ in which case $\alpha_i = \alpha_{h+1} = v$, we would have $\alpha_{j+1} \in B_{h+1}$ which is however impossible as α_{j+1} cannot be an element of B_{h+1} because $h+1 > j+1$; or we may have $i \leq h$ in which case $v \in B_i$ with $i > j$, but this again contradicts the definition of j as the largest index $\leq h$ such that $v \in B_j$; thus the supposition $j \leq h-1$ is impossible; thus $j = h$ that is, $v = \alpha_{h+1} \in B_h$, which was to be proved.

Lemmas 3*, 4*, 5* contain a complete characterization of those sequences $B_1, B_2, \dots, B_{n-k-1}$ of $n-k-1$ k -tuples, which are the primitive

Prüfer codewords of a k -tree rooted at the k -tuple $n-k+1, n-k+k, \dots, n$.

This characterization is as follows:

THEOREM 2. A sequence $(B_1, B_2, \dots, B_{n-k-1})$ of $n-k-1$ k -tuples from the integers $1, 2, \dots, n$ is the primitive Prüfer code of a k -tree of order n , labelled by the numbers $1, 2, \dots, n$ and rooted at the k -tuple $(n-k+1, \dots, n)$, if and only if it has the following properties:

a) Putting $B_{n-k} = (n-k+1, n-k+2, \dots, n)$, denoting by α_1 the least natural number not contained in any of the k -tuples $B_1, B_2, \dots, B_{n-k}$ and for every $j \leq n-k$ denoting by α_j the least natural number different from $\alpha_1, \dots, \alpha_{j-1}$ and not contained in any of the k -tuples $B_j, B_{j+1}, \dots, B_{n-k}$ the numbers $\alpha_1, \dots, \alpha_{n-k}$ form a permutation of the numbers $1, 2, \dots, n-k$.

b) Denoting by C_j the $(k+1)$ -tuple consisting of α_j and the k elements of the k -tuple B_j , each B_i is the subset of at least one C_j with $i < j \leq n-k$.

PROOF of THEOREM 2. The conditions a) and b) are necessary because of Lemmas 3*, 4* and 5*. To see that they are sufficient it is enough to point out that if these conditions are satisfied the corresponding k -tree can be recursively constructed starting from the complete $(k+1)$ -graph the points of which are the elements of C_{n-k} and working backwards: at the j -th step the new point is $\alpha_{n-k-j+1}$ and the k -tuple of points to which it is connected is $B_{n-k-j+1}$, this k -tuple being a subset of a $(k+1)$ -tuple C_i such that $i > n-k-j+1$ ($j = 1, 2, \dots, n-k$).

We give now some examples which may help to familiarize the reader with the meaning of Theorem 2.

EXAMPLE 1. Let us have $n=7, k=2$ and consider the sequence of $n-k-1=4$ pairs of the integers $1, 2, 3, 4, 5, 6, 7$;

$$(6, 7), (6, 7), (1, 6), (5, 6).$$

We shall verify that this is the primitive Prüfer codeword of a 2-

tree of order 7, rooted at the edge (6,7). As a matter of fact condition a) is satisfied with $\alpha_1 = 2, \alpha_2 = 3, \alpha_3 = 4, \alpha_4 = 1$ and $\alpha_5 = 5$. Further the matrix

$$\begin{pmatrix} 2 & 3 & 4 & 1 & 5 \\ (6,7) & (6,7) & (1,6) & (5,6) & (6,7) \end{pmatrix}$$

clearly satisfies condition b).

EXAMPLE 2. Let us have $n=5, k=2$. The sequence (1, 2), (4, 5) is not the primitive Prüfer codeword of a 2-tree of order 5 rooted at the edge (4, 5). As a matter of fact while condition a) is satisfied with $\alpha_1 = 3, \alpha_2 = 1, \alpha_3 = 2$ the matrix

$$\begin{pmatrix} 3 & 1 & 2 \\ (1,2) & (4,5) & (4,5) \end{pmatrix}$$

does not satisfy condition b) because the pair (1,2) is not a subset of either of the triples (1, 4, 5) and (2, 4, 5).

In connection with this example it should be pointed out that a sequence of $n-k-1$ k -tuples of the numbers $1, 2, \dots, n$ which satisfies condition a) but violates condition b) of Theorem 2 corresponds to a graph the edges of which are the edges of $n-k$ such complete $(k+1)$ -graphs which do not form a k -tree

REMARK. It is easy to obtain from Theorem 2 a characterization of the primitive Prüfer codewords of k -trees of order n rooted at any k -tuple. The obvious modification of Theorem 1 for this case is as follows:

THEOREM 2b. A sequence $(B_1, B_2, \dots, B_{n-k-1})$ of $n-k-1$ k -tuples of the integers $1, 2, \dots, n$ is the primitive Prüfer codeword of a k -tree of order n the points of which are labelled by the numbers $1, 2, \dots, n$ and which is rooted at some k -tuple B of the numbers $1, 2, \dots, n$ if it has the following properties:

a) Put $B_{n-k} = B$; let α_1 be the least natural number not contained in any of the k -tuples $B_1, B_2, \dots, B_{n-k}$ and for every j with $1 < j \leq n-k$; let α_j be the least natural number different from $\alpha_1, \dots, \alpha_{j-1}$ and not contained in any of the k -tuples $B_j, B_{j+1}, \dots, B_{n-k}$. Then $\alpha_1, \alpha_2, \dots, \alpha_{n-k}$ is a permutation of the $n-k$ numbers obtained by omitting from the sequence $1, 2, \dots, n$ the elements of the k -tuple B .

b) Denoting by C_j the $(k+1)$ -tuple consisting of α_j and the elements of the k -tuple B_j , each B_i ($1 \leq i \leq n-k-1$) is contained in at least one C_j with $i < j \leq n-k$.

REMARK. The same sequence $B_1, B_2, \dots, B_{n-k-1}$ may be the primitive Prüfer code of different k -trees rooted at different roots, as is shown by the following.

EXAMPLE 3. The sequence $(3, 4), (3, 5), (4, 5)$ is the primitive Prüfer code of a 2-tree of order 6, rooted at the edge $(4, 6)$, the corresponding redundant Prüfer code being

$$\begin{pmatrix} 1 & 2 & 3 & 5 \\ (3, 4) & (3, 5) & (4, 5) & (4, 6) \end{pmatrix}.$$

At the same time, the sequence $(3, 4), (3, 5), (4, 5)$ is also the primitive Prüfer code of an other 2-tree of order 6 rooted at the edge $(1, 5)$ the corresponding redundant Prüfer code being

$$\begin{pmatrix} 2 & 6 & 3 & 4 \\ (3, 4) & (3, 5) & (4, 5) & (1, 5) \end{pmatrix}.$$

§ 5. ENUMERATION OF k -TREES

We first prove the generalization of Lemma 6 to the case of k -trees for $k \geq 2$.

LEMMA 6.* Let $\pi_{n-k} = (\alpha_1, \alpha_2, \dots, \alpha_{n-k})$ be a permutation of

the numbers $1, 2, \dots, n-k$. Let $R_k(n, \pi_{n-k})$ denote the number of those labelled k -trees of order n , rooted at the k -tuple $(n-k+1, n-k+2, \dots, n)$, the upper row of the redundant Prüfer codeword of which is equal to the sequence π_{n-k} . Let $\alpha_{h_1+1}, \dots, \alpha_{h_r+1}$ be the weak elements of the permutation π_{n-k} . Then we have

$$(5.1) \quad R_k(n, \pi_{n-k}) = k^r \prod_{h=1}^{n-k-1} [k(n-k-h)+1] \\ h \neq h_i \quad (1 \leq i \leq r)$$

PROOF. According to Lemma 5* we have $\alpha_{h_i+1} \in B_{h_i}$ for $i = 1, 2, \dots, r$. As by Lemma 4*, B_{h_i} has to be a subset of some $(k+1)$ -tuple C_j with $j > h_i$, and α_{h_i+1} is not an element of C_j with $j > h_i+1$, it follows that B_{h_i} has to be a subset of C_{h_i+1} . As the number of k -tuples contained in the $(k+1)$ -tuple C_{h_i+1} and containing α_{h_i+1} is equal to k , the number of choices of B_{h_i} is equal to k . If h is not one of the numbers $h_1, h_2, \dots, h_r$ then the number of possible choices of B_h is equal to the number of all k -tuples contained in at least one of the $(k+1)$ -tuples C_j with $j > h$. It is easy to see that this number is equal to $k(n-k-h)+1$; this statement is most easily shown by induction on the value of $t = n-k-h$. If $t = 0$, i.e. if $h = n-k$, then $B_h = B_{n-k}$ is the root $(n-k+1, \dots, n)$, i.e. the number of choices is one. Suppose our statement holds for some value of $t = n-k-h$, i.e. we know already that the $(k+1)$ -tuples $C_{h+1}, \dots, C_{n-k}$ contain together $kt+1$ k -tuples. As B_h is one of these, C_h contains k such k -tuples which are not contained in any of the $(k+1)$ -tuples $C_{h+1}, \dots, C_{n-k}$ i.e. the number of choices for B_{h-1} is $k(t+1)+1 = k(n-k-(h-1))+1$, thus our statement is proved by induction. It follows that the total number of choices of the lower row of the redundant Prüfer codeword with the given upper row π_{n-k} is

$$(5.2) \quad R_k(n, \pi_{n-k}) = k^r \prod_{h=1}^{n-k-1} (k(n-k-h)+1) \\ h \neq h_i \quad (1 \leq i \leq r)$$

Thus Lemma 6* is proved.

We now deduce from Lemma 6 the following result which has been proved first by BEINEKE and PIPPERT [6] and also by MOON [7] ; our proof is essentially different from both of these proofs.

THEOREM 3. The total number $R_k(n)$ of labelled k -trees of order n rooted at a given k -tuple is given by the formula

$$(5.3) \quad R_k(n) = [k(n-k)+1]^{n-k-1},$$

while the total number $T_k(n)$ of labelled (unrooted) k -trees of order n is given by

$$(5.4) \quad T_k(n) = \binom{n}{k} [k(n-k)+1]^{n-k-2}$$

PROOF. In proving (5.3) we may suppose without restricting the generality that the k -trees in question are rooted at the k -tuple $(n-k+1, n-k+2, \dots, n)$. We have evidently

$$(5.5) \quad R_k(n) = \sum_{\pi_{n-k} \in S_{n-k}} R_k(n, \pi_{n-k})$$

where S_{n-k} denotes the set of all permutations of the numbers $1, 2, \dots, n-k$. Using Lemma 6* and Lemma 2 we obtain from (5.5)

$$(5.6) \quad R_k(n) = \sum_{1 \leq h_1 < h_2 < \dots < h_r \leq n-k-1} h_1 h_2 \dots h_r \cdot k^r \prod_{h=1}^{n-k-1} [k(n-k-h)+1] = [k(n-k)+1]^{n-k-1} \prod_{h \neq h_i (1 \leq i \leq r)}$$

Thus (5.3) is proved.

As has been remarked both in [6] and [7], knowing the total number $R_k(n)$ of rooted labelled k -trees of order n , it is very easy to get the total number $T_k(n)$ of labelled unrooted k -trees of order n , using the obvious identity

$$(5.7) \quad T_k(n) [k(n-k)+1] = \binom{n}{k} R_k(n)$$

(5.7) follows from the remark that every (unrooted) k -tree of order n contains $k(n-k)+1$ complete k -graphs and thus it can be rooted at any of these; on the other hand one can choose k points out of n in $\binom{n}{k}$ ways, and for each such choice by definition the total number of k -trees of order n rooted at this k -tuple is $R_k(n)$.

From (5.3.) and (5.7) we obtain immediately (5.4).

REMARK. Notice that $R_1(n) = T_1(n)$ and thus for $k=1$ both (5.3) and (5.4) reduce to Cayley's formula

In [7] MOON has also determined the number $R_{k,d}(n)$ of k -trees of order n in which a selected k -tuple of points has the degree d . We shall now deduce this result by our method, i.e. we prove

THEOREM 4. Denoting by $R_{k,d}(n)$ ($k \geq 1$, $n \geq k+1$, $d \geq 1$) the number of labelled k -trees of order n in which a selected k -tuple has the degree d , we have

$$(5.8) \quad R_{k,d}(n) = \binom{n-k-1}{d-1} [k(n-k)]^{n-k-d}$$

PROOF. It is no restriction to suppose that the selected k -tuple is

$B = (n-k+1, n-k+2, \dots, n)$. We consider the redundant Prüfer codewords of those k -trees which are rooted at B and in which B has the degree $d \geq 1$. Clearly B occurs in the lower row of the redundant Prüfer codeword d times, one of these being the last place. If the other $d-1$ places have the indices $j_1, j_2, \dots, j_{d-1}$ then clearly the elements α_{j_i+1} ($i = 1, 2, \dots, d-1$) of the permutation π_{n-k} in the upper row of the redundant Prüfer codeword cannot be weak. It follows in the same way as in the proof of Lemma 6* that if both the places $j_1, \dots, j_{d-1}$ and the weak elements $\alpha_{h_1+1}, \dots, \alpha_{h_r+1}$ of π_{n-k} are fixed, the total number of choices of the k -tuples in the lower row is equal to

$$(5.9) \quad k^r \prod_{h=1}^{n-k-1} (k(n-k-h))$$

$$h \neq j_\ell \quad (1 \leq \ell \leq d-1)$$

$$h \neq h_i \quad (1 \leq i \leq r)$$

(Notice that we had to replace $k(n-k-h)+1$ by $k(n-k-h)$ because B is now not an admissible choice for B_h if $h \neq j_\ell$ $j_\ell = 1, 2, \dots, d-1$, and $h \neq n-k$.)

Multiplying (5.9) by the number $h_1 h_2 \dots h_r$ of permutations π_{n-k} having their weak elements at the places with indices h_i+1 ($1 \leq i \leq r$) and by summation over all admissible choices of the indices $h_1, \dots, h_r$, we obtain that to any choice of the indices $j_1, \dots, j_{d-1}$ there correspond $[k(n-k)]^{n-k-d}$ k -trees; as the indices $j_1, \dots, j_{d-1}$ can be chosen in $\binom{n-k-1}{d-1}$ ways, (5.8) follows.

REMARK. Notice that

$$(5.10) \quad R_k(n) = \sum_{d=1}^{n-k} R_{k,d}(n)$$

thus (5.3) can be deduced from (5.8); as a matter of fact Moon proved (5.3) by proving first (5.8) - in a rather complicated way - and then carrying out the summation over d .

One can easily generalize Theorem 1 to k -trees for any $k \geq 2$.

We call the point $j \leq n-k$ of a labelled k -tree T of order n a weak point if there exists in T a point $h > j$ such that the unique "path" from the point h to the root (i.e. the shortest sequence of different complete $(k+1)$ -graphs $C_1, \dots, C_s$, the first of which contains the point h and the last the root, and the intersection of C_i and C_{i+1} is a complete k -graph) passes through the point j (i.e. j belongs to one of the $(k+1)$ -tuples $C_1, \dots, C_s$).

With this definition we obtain the following generalization of Theorem 1.

THEOREM 1*. Let $w_k(n, r)$ denote the probability that a random* labelled k -tree of order n , rooted at the k -tuple $(n-k+1, n-k+2, \dots, n)$ contains r weak points. We have

$$\sum_{r=0}^{n-k-1} w_k(n, r) x^r = \prod_{h=1}^{n-k-1} \left(1 - \frac{hk(x-1)}{k(n-k)+1} \right).$$

Thus if $V_n^{(k)}$ denotes the number of weak points of a random k -tree of order n , we have

$$E(V_n^{(k)}) = \frac{k(n-k)(n-k-1)}{2[k(n-k)+1]} \sim \frac{n}{2}$$

and

$$D^2(V_n^{(k)}) = \frac{k(n-k)(n-k-1)[k(n-k+1)+3]}{6[k(n-k)+1]^2} \sim \frac{n}{6}$$

* A random k -tree of order n rooted at the k -tuple $n-k+1, \dots, n$ means a k -tree chosen at random, with uniform distribution among the $[k(n-k)+1]^{n-k-1}$ trees.

further

$$\lim_{n \rightarrow +\infty} P \left(\frac{V_n^{(k)} - \frac{n}{2}}{\sqrt{\frac{n}{6}}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{u^2}{2}} du.$$

REMARK. Notice that asymptotically the mean and variance of $V_n^{(k)}$ do not depend on k . It has been proved by the second author (see [11]) that the same is true as regards the number $\varepsilon_n^{(k)}$ of endpoints of a random k -tree of order n .

$$\frac{\varepsilon_n^{(k)} - \frac{n}{e}}{\sqrt{\frac{n}{e} \left(1 - \frac{2}{e}\right)}}$$

has in the limit for $n \rightarrow +\infty$ a standard normal distribution independently of the value of k . Thus it follows that for the majority of labelled k -trees of order n the number of points which are neither endpoints nor weak points is asymptotically equal to $n \left(\frac{1}{2} - \frac{1}{e} \right)$.

Other enumeration problems concerning k -trees can also be solved by the method of the present paper.

REFERENCES

- [1] F. HARARY-E.M. PALMER, On acyclic simplicial complexes, *Mathematika* 15 (1968) 115-122.
- [2] A. PRÜFER, Neuer Beweis eines Satzes über Permutationen. *Archiv der Mathematik und Physik* 27 (1918) 142-144.
- [3] F.N. DAVID-D.E. BARTON, *Combinatorial chance*, Griffin, London 1962, p. 181-182.
- [4] See D.H. LEHMER, The machine tools of combinatorics, Chapter 1, in *Applied Combinatorial Analysis*, edited by F. Beckenbach, Wiley, New York, 1964, see p.20.
- [5] A. RÉNYI, Théorie des éléments saillants d'une suite d'observations, *Annales de la Faculté des Sciences de l'Université de Clermont-Ferrand*, 8 (1962) 7-13.

- [6] L.W. BEINEKE-R.E. PIPPERT, The number of labelled k -dimensional trees, *Journal of Combinatorial Theory*, 6 (1969) 200-205.
- [7] J.W. MOON, The number of labelled k -trees, *Journal of Combinatorial Theory*, 6 (1969) 196-199.
- [8] C.L. MALLOWS-J.RIORDAN, The inversion enumerator for labelled trees, *Bulletin of the American Math. Soc.* 74 (1968) 92-94.
- [9] J.W. MOON, Counting labelled trees: a survey of methods and results. (Lecture notes.) Biennial Seminar of the Canadian Mathematical Congress, Vancouver, 1968.
- [10] A. RÉNYI, Some remarks on the theory of trees, *Publications of the Math Inst. of the Hung. Acad. of Sci.* 4 (1959) 385-388.
- [11] A. RÉNYI, On the number of endpoints of a k -tree, *Studia Scientiarum Mathematicarum Hungarica* (in print).

163, 167, 332, 347

NOTES

A. Rényi dealt with one and more dimensional mathematical trees in his papers No. 163, 167, 332, 347, als in C. Rényi and A. Rényi No. 343.

1. The first question concerning trees was that how many different trees exist with a given number of points.

Let $T(n)$ be the number of trees with n labelled points.

One of the earliest results in enumerative graph theory was the Cayley formula:

$$(1) \quad T(n) = n^{n-2}.$$

Several proofs of this have been given since it was first stated by Cayley, in [4]. Cayley did not give a proof of formula (1) for general case, only for $n = 5$ and $n = 6$. The first (and most elegant) proof is due to Prüfer [22] using the so-called "Prüfer code". Moon [16] reports on the outlines of nine different proofs.

Let $F(n, k)$ denote the number of forests with n labelled points that consist of k disjoint trees such that k fixed points belong to different trees.

It was also Cayley, who gave the following formula without proof (see Cayley [4]).

$$(2) \quad F(n, k) = k \cdot n^{n-k-1}.$$

Rényi was the first, who proved formula (2), in his first papers on trees (see Rényi No. 163). Here Rényi used Dziobek's method (see Dziobek [6]) of proving formula (1).

Also in this paper Rényi determines the number of forests that consists of k disjoint trees (without k fixed roots) and gives an asymptotical formula of it, too.

Let $T(n, r)$ denote the number of trees with n labelled points in which exactly r points are of degree 1 (namely they have r endpoints).

In the second part of this paper Rényi, applying Prüfer code, determines the number

$$(3) \quad T(n, r) = \frac{n!}{r!} \mathfrak{S}_{n-2}^{n-r}$$

where $\mathfrak{S}_n^m$ denote the Stirling numbers of second kind.

Additionally he mentions that the next recursion formula holds for $T(n, r)$:

$$(4) \quad \frac{r}{n} T(n, r) = r T(n-1, r) + (n-r) T(n-1, r-1).$$

Formula (3) can be considered as a proof of formula (1), because:

$$(4a) \quad T(n) = \sum_{r=2}^n T(n, r) = \sum_{r=2}^n \frac{n!}{r!} \mathfrak{S}_{n-2}^{n-r} = \sum_{l=1}^{n-2} \mathfrak{S}_{n-2}^l n(n-1) \dots (n-l+1) = n^{n-2}.$$

Here Rényi also shows, that the number of endpoints has asymptotically a normal distribution with mean value $\frac{n}{e}$ and variance $\frac{n}{e} \left(1 - \frac{2}{e}\right)$.

Meir and Moon [13] generalize Rényi's result of $T(n, r)$ (see formula (3)) in such a way, that they determine the number of trees with n labelled points in which r points are of degree two. After that they show, that the number of points of degree two has also a normal distribution with mean value $\frac{n}{e}$, but the

variance is $\frac{n}{e} \left(1 - \frac{1}{e}\right)$. They give a general formula of the mean value (M_v) and the variance (σ_v^2) for an arbitrary degree v without proof.

$$M_v = \frac{n}{e} \cdot \frac{1}{(v-1)!}$$

$$\sigma_v^2 = \frac{n}{e} \cdot \left[1 - \frac{1}{e} \cdot \frac{1 + (v-2)^2}{(v-1)!} \right] \cdot \frac{1}{(v-1)!}.$$

Harary and Mowshowitz [8] use Rényi's formula on $T(n, r)$. In structural diagrams of chemical compounds the symbol H for hydrogen is always an endpoint of the diagram. This suggests the problem of enumeration of labelled trees with unlabelled endpoints ($T^*(n, r)$). They start with the formula:

$$T^*(n, r) = \sum_{i=2}^n \binom{n-i-1}{r-i} T(n-r, i) \quad r = 2, 3, \dots, n-1; \quad n = 3, 4, 5, \dots$$

The further generalization of the previous result on $T^*(n, r)$ can be found in Moon [17]. Using the result of Harary and Mowshowitz, he determines the number of connected graphs with unlabelled endpoints.

Beineke and Moon [1] use Rényi's method of determining the number $T(n, r)$ to determine the number of 2 dimensional trees, $T_2(n)$. (See Proof IV in Beineke and Moon [1].) They establish a recursion formula for $T_2(n)$ (comp. formula (4)), and use the numbers $M(s, r)$, which are defined by the relation

$$(2x + 1)^s = \sum_{r=0}^s M(s, r) \cdot x \cdot (x - 1) \dots (x - r + 1).$$

Meir and Moon [15] apply Rényi's result concerning the counting of forests (see formula (2)) to determine the mean value and variance of the number of edges chosen at random, that must be removed from a random rooted forest before isolating its roots.

It was Rényi's idea to use Prüfer's method for solving some enumeration problems concerning trees of coloured point. This idea was worked out by G. Oláh [20], [21].

2. Let $D(n, k)$ denote the number of connected graphs with n points and n edges in which the single cycle is of length k .

Katz proved in [10] that

$$D(n, k) = \frac{1}{2} n \cdot (n - 1) \dots (n - k + 1) \cdot n^{n-k-1}.$$

Similar result was obtained by Rényi No. 167 in his second paper on trees.

Let $C(n, m)$ denote the number of graphs with n labelled points and m edges. Rényi shows, that

$$C(n, n) = \frac{n^{n-1}}{2} \sum_{k=3}^n \binom{n}{k} \frac{k!}{n^k}.$$

In the proof he uses his own result on $F(n, k)$. (See Rényi No. 163.)

Observe that

$$\sum_{k=3}^n D(n, k) = C(n, n).$$

Katz [10] and Rényi No. 167 showed, that $C(n, n)$ is asymptotically equal to $\left(\frac{\pi}{8}\right)^{1/2} \cdot n^{n-1/2}$, if $n \rightarrow \infty$ and the distribution of the length of the cycle in

these graphs is asymptotically normal with mean value $\left(\frac{2n}{\pi}\right)^{1/2}$

The arguments used in Meir and Moon [14] are related to arguments, that Rényi No. 167 has used in studying the distribution of $C(n, n)$. (See also Katz [10].) In this paper Meir and Moon show among other things that the mean value of the number of points in the path joining two arbitrary points in a random tree T_n with n labelled points is $\left(\frac{n\pi}{2}\right)^{1/2}$ and the mean value (M_p) of the number of path of length $k - 1$ in T_n is:

$$M_p = \frac{k \cdot n}{2} \cdot \binom{n}{k} \frac{k!}{n^k}.$$

Let f denote a function that maps $\{1, 2, \dots, n\}$ into $\{1, 2, \dots, n\}$. (Each function f determines a directed graph with n points and n edges.) The results of Katz [10] and Rényi No. 167 are used at studying the distribution of some parameters (the number of connected f , the probability that f is connected, the number of components of f and so on) associated with functions f . (See section 7.1 "Random Mapping Functions" in Moon's book [19].)

3. Cayley [4] has formulated the following more general formula than formula (1):

$$(5) \quad \sum_T x_1^{v_1-1} \cdot x_2^{v_2-1} \dots x_n^{v_n-1} = (x_1 + x_2 + \dots + x)^{n-2}$$

where the summation is taken over all trees T with n labelled points and v_k denotes the degree of the k th point of T . Cayley also didn't give a full proof of this formula, only for the case $n = 5, n = 6$.

Let $T_n(v_1, v_2, \dots, v_n)$ be the number of trees with n labelled points in which the k th point has degree v_k . Then the next formula follows from Prüfer's method, as Moon [16] reported:

$$(6) \quad T_n(v_1, v_2, \dots, v_n) = \frac{(n-2)!}{(v_1-1)!(v_2-1)! \dots (v_n-1)!}$$

Rényi No. 332 was the first, who gave a correct proof for formula (5), by applying induction, and appealing to the fact, that the Cayley polynomial is a symmetric polynomial in its n variables, and is homogeneous of degree $n - 2$. (The Cayley polynomial is the left side of formula (5).)

Naturally, it is also considered as a new proof of formula (1).

It is also mentioned in this paper, that formula (6) follows from formula (5).

Several people have proved the following two theorems, which came from electrical network theory. The first is due to Kirchoff [11], the second one is frequently called Maxwell's rule. (See Maxwell [12].)

Matrix-tree theorem I: If A is the reduced incidence matrix of a rooted graph G , then the number of spanning trees of G equals the determinant of the matrix $A \cdot A^T$.

Matrix-tree theorem II: Let the variables $y_1, y_2, \dots, y_m$ be associated with the edges of the connected rooted graph G , and let $\pi(T)$ be the product of variables associated with the edges of a spanning tree T of the graph G , then

$$\det(A \cdot Y \cdot A^T) = \sum \pi(T)$$

where the summation is taken over all spanning trees of G , and $Y = \langle y_i \rangle$ is a diagonal matrix.

(The expression $\sum \pi(T)$ is sometimes called tree-polynomial.)

Some other properties of rooted graphs and the matrix $A \cdot Y \cdot A^T$ are investigated in Rupp [24].

After having generalized the Cayley polynomial for graphs, Rényi No. 332 shows, that the two matrix-tree theorems can be proved by applying Cayley-polynomial.

The Matrix-tree Theorem I also gives a proof of the Cayley formula (1), if the graph G is the complete graph.

Matrix-tree theorems are applied to obtain formulae for the number of spanning trees in special graphs. (See section 5.4 "Applications" in Moon [19].)

Let $W_1(n, k)$ denote the number of spanning trees of a graph obtained from the complete n -graph by removing k edges no two of which have a point in common, then:

$$W_1(n, k) = (n - 2)^k \cdot n^{n-k-2} \quad (0 \leq 2k \leq n)$$

and let $W_2(n, k)$ denote ones, if the k edges are incident with a fixed point, then:

$$W_2(n, k) = (n - k - 1)(n - 1)^{k-1} n^{n-k-2} \quad (0 \leq k \leq n - 1).$$

4. The notion of k -tree was introduced by Harary and Palmer [9].

Several proofs of the number of labelled 2-trees have given. (See Beineke and Moon [1]). One of them is based on Rényi's method for determining of the number $T(n, r)$. (See point 1.)

Beineke and Pippert [2] were the first, who determined the number of k -trees with n labelled points, and later Moon [18] found another method.

They obtained the formula:

$$(7) \quad T_k(n) = \binom{n}{k} [k(n - k) + 1]^{n-k-2}.$$

The proofs of Beineke and Pippert are based on Dziobek's proof of Cayley formula (1); Moon's proof is based on Clarke's proof of Cayley formula (1). (See Dziobek [6] and Clarke [5].)

Rényi determines the number of trees with r endpoints not only for 1-trees, but for k -trees ($T_k(n, r)$) too. (See Rényi No. 347.) A recursion formula holds for $T_k(n, r)$, too, (comp. formula (4)) and Stirling numbers also are used in the proof. Rényi's result on $T_k(n, r)$ gives a proof of formula (7). (Comp. formula (4a).)

In this paper Rényi shows, that the number of endpoints of a k -tree has also a normal distribution with mean value $\frac{n}{e}$ and variance $\frac{n}{e} \left(1 - \frac{2}{e}\right)$. It is very interesting, that the mean value and variance do not depend on k .

5. After having introduced the notion of the redundant Prüfer code, C. Rényi and A. Rényi No. 343 determine the number of k -trees with n labelled points (formula (7)), in such a way, that they define the Prüfer code for k -trees.

It is also mentioned in this paper, that the next formula also can be proved with Prüfer's method:

$$R_{k,d}(n) = \binom{n - k - 1}{d - 1} [k(n - k)]^{n-k-d}$$

where $R_{k,d}(n)$ denotes the number of k -trees with n labelled points in which a fixed k -tuple has the degree d . This formula was proved by Clarke [5] for the case $k = 1$ and by Moon [18] for an arbitrary k .

Foata [7] knowing the methods of Beineke and Pippert [2], Moon [18] and C. Rényi—A. Rényi No. 343 gives a further proof of formula (7). He enumerates the "acyclic functions", which are readily enumerated, and shows, that the rooted k -trees are special acyclic functions.

Beineke and Pippert [2] determine the number of unlabelled k -trees with n points, which are embeddable in k dimensional space.

Finally, we mention, that similarly to 1-trees, k -trees also are applied in the study of sparse linear systems. (See Rose [23].) (Gy. K.)

REFERENCES

- [1] Beineke, L. W. and Moon, J. W.: Several proofs of labelled 2 dimensional trees. In "Proof Techniques in Graph Theory" (F. Harary, editor) New York, Academic Press, (1969), 11–20.
- [2] Beineke, L. W. and Pippert, R. E.: The number of labelled k dimensional trees. *Journal of Combinatorial Theory*, **6** (1969), 200–205.
- [3] Beineke, L. W. and Pippert, R. E.: The number of labelled dissections of a k -ball. *Mathematische Annalen*, **191** (1971), 87–98.
- [4] Cayley, A.: A theorem on trees. *Quarterly Journal of Mathematics*, **23**, 376–378. *Collected Papers*, Cambridge, 13 (1889), (1897), 26–28.
- [5] Clarke, L. E.: On Cayley's formula for counting trees. *Journal of the London Mathematical Society*, **33** (1958), 471–474.
- [6] Dziobek, O.: Eine Formel der Substitutionstheorie. *Sitzungsberichte der Berliner Mathematischen Gesellschaft*, **17** (1947), 64–67.
- [7] Foata, D.: Enumerating k -trees. *Discrete Mathematics*, **1** (1971), 181–186.
- [8] Harary, F. and Mowshowitz, M.: Labelled trees with unlabelled end-points. *Journal of Combinatorial Theory*, **6** (1969), 60–64.
- [9] Harary, F. and Palmer, E. M.: On acyclic simplicial complexes. *Mathematika*, **15** (1968), 115–122.
- [10] Katz, L.: Probability of indecomposability of a random mapping function. *Annals of Mathematical Statistics*, **26** (1955), 512–517.
- [11] Kirchhoff, G.: Über die Auflösung der Gleichungen, auf welche man bei der Untersuchung der linearen Verteilung galvanischer Ströme geführt wird. *Annalen der Physik und Chemie*, **72** (1847), 497–508.
- [12] Maxwell, J. C.: *A Treatise on Electricity and Magnetism*, 1, 3rd edition. Oxford, Clarendon Press, (1892), 403–410.
- [13] Meir, A. and Moon, J. W.: On nodes of degree two in random trees. *Mathematika*, **15** (1968), 188–192.
- [14] Meir, A. and Moon, J. W.: The distance between points in random trees. *Journal of Combinatorial Theory*, **8** (1970), 99–103.
- [15] Meir, A. and Moon, J. W.: Cutting down random trees. *Journal of the Australian Mathematical Society*, **11** (1970), 311–324.
- [16] Moon, J. W.: Various proofs of Cayley's formula for counting trees. In "A Seminar on Graph Theory" (F. Harary, editor). London, Academic Press, (1967), 261–272.
- [17] Moon, J. W.: Connected graphs with unlabelled end-points. *Journal of Combinatorial Theory*, **6** (1969), 65–66.
- [18] Moon, J. W.: The number of balled k -trees. *Journal of Combinatorial Theory*, **6** (1969), 196–199.
- [19] Moon, J. W.: Counting labelled trees. *Canadian Mathematical Congress*, (1970).
- [20] Oláh, G.: A problem on enumeration at certain trees. (In Russian with English abstracts.) *Studia Sci. Math. Hung.*, **3** (1968), 71–80.
- [21] Oláh, G.: Enumeration problems concerning trees. (In Hungarian with English abstracts.) *Matematikai Lapok*, **21** (1970), 1–2, 103–142.
- [22] Prüfer, H.: Neuer Beweis eines Satzes über Permutationen. *Archiv für Mathematik und Physik*, **27** (1918), 142–144.
- [23] Rose, D. J.: On simple characterizations of k -trees. *Discrete Mathematics*, **7** (1974), 317–322.
- [24] Rupp, M.: Sparse matrix inversion by graphs. (In Hungarian with English abstract.) *Matematikai Lapok*, **23** (1972), 1–2; 163–171.

ON THE ENUMERATION OF SEARCH-CODES

By

A. RÉNYI (Budapest), member of the Academy*Dedicated to Professor G. ALEXITS at the occasion of his 70th birthday*

§ 1. Definition of search-codes

Any finite sequence of nonnegative integers is called a *codeword*. If $a = (a_1, a_2, \dots, a_s)$ is a codeword, we call s the *length* of the codeword a and put $|a| = s$. The empty sequence (of length 0) is considered as a codeword too. We denote by Z the set of all codewords. If $a = (a_1, a_2, \dots, a_r)$ and $b = (b_1, b_2, \dots, b_s)$ are any two codewords, we define the codeword ab as $ab = (a_1, a_2, \dots, a_r, b_1, b_2, \dots, b_s)$. Clearly $|ab| = |a| + |b|$, and Z is a semigroup with respect to the multiplication defined above. Denoting by e the empty codeword, e is the unit element of the semigroup Z . A codeword a is called a *prefix* of the codeword b if there exists a codeword c such that $b = ac$; in this case c is called a *suffix* of b . If $a = (a_1, \dots, a_s)$, $a_1, \dots, a_s$ are called the *letters* of a .

Any finite set $C = \{c_1, c_2, \dots, c_n\}$ of different codewords $c_j = (c_{j,1}, c_{j,2}, \dots, c_{j,l_j})$ is called a *code*. It is convenient to consider the empty set also as a code: we call it *the empty code*. The code consisting of the single codeword e , where e is the empty codeword is a nonempty code, which will be called *the trivial code*.

If C is a code and a any codeword (not necessarily in C) we denote by C_a the set of those codewords $b \in Z$ for which $ab \in C$. In other words C_a is obtained by taking all those codewords c of C of which a is a prefix and removing from these codewords the prefix a , i.e. preserving only the suffix of c following a . Evidently $C_e = C$, and $(C_a)_b = C_{ab}$. Of course for certain $a \in Z$ (in fact for all but a finite number of $a \in Z$) C_a is the empty code. If $a = c \in C$ then C_c is not empty, as it contains certainly the empty codeword e , but C_c may be the trivial code: if C_c is for every $c \in C$ the trivial code, C is called a *prefix code*. Thus a code C is a prefix code if none of its codewords is the prefix of another codeword in C .

If C is a code, we shall denote by $N(C)$ the number of elements of C , and we shall call $N(C)$ the *size* of C .

We shall call a code C *well-branched*, if one of the following three cases takes place: 1. C is the empty code; 2. C is the trivial code; 3. C does not contain the empty codeword e and there exists an integer $b(C)$ — called *the branching number* of C — such that $b(C) \geq 2$ and denoting by $\{k\}$ the codeword of length 1, consisting of the single letter k ($k = 0, 1, \dots$) the code $C_{\{k\}}$ is not empty if $k < b(C)$ and $C_{\{k\}}$ is empty if $k \geq b(C)$. If C is the empty code we put $b(C) = 0$ while if C is the trivial code we put $b(C) = 1$; thus the branching number $b(C)$ is defined for every well-branched code.

We call a code C a *search code* if C_a is a well-branched code for every $a \in Z$. Clearly if C is a search code, then C is necessarily a prefix code. As a matter of fact if $c \in C$ the code C_c has to be a well branched code, and as it contains the empty codeword e , C_c has to be the trivial code: thus C is a prefix code. However, not every

prefix code is a search-code: for instance the code consisting of a single codeword, which is different from the empty codeword c , is a prefix code, but not a search code.

If C is a search code, we call those $a \in Z$ for which $b(C_a) \geq 2$, the *branching points* of C . We shall denote the total number of branching points of C by $B(C)$.

A search code C is called *regular of degree q* ($q \geq 2$), if each of its branching points has the branching number q , i.e. if for each $a \in Z$ such that $b(C_a) \geq 2$, one has $b(C_a) = q$. The trivial code is by definition regular of every degree $q \geq 2$.

The study of search codes is motivated by the connection of search-codes with the *mathematical theory of search* (see e.g. [1]). Let us consider a simple search process in which we want to identify an unknown element x of a finite set S . Suppose that we can not observe x directly, however we may choose some functions $f_1, f_2, \dots, f_N$ from a given set F of nonnegative integer valued functions f defined on the set S , and observe the values $f_1(x), f_2(x), \dots, f_N(x)$ of these functions at the unknown point x . A method for choosing the functions f_k , one after the other, from the set F (so that the choice of f_k may depend on the previously observed values $f_1(x), \dots, f_{k-1}(x)$) so that after a finite number N of steps ($N = N(x)$ may depend on x) the unknown x is uniquely determined by the sequence $f_1(x), f_2(x), \dots, f_N(x)$, is called a *strategy of search*. Clearly each strategy defines a code, the codewords of which are the sequences $(f_1(x), f_2(x), \dots, f_{N(x)}(x))$ ($x \in S$). A strategy is called *irreducible*, if none of the observations prescribed by the strategy is unnecessary. It is easy to see that the codes corresponding to irreducible strategies of search are just the search-codes defined above, provided that for every possible sequence $f_1(x), \dots, f_{k-1}(x)$, if n is a possible value of $f_k(x)$, then so is every $m < n$, as well.

To every search-code there corresponds a rooted tree, defined as follows: the root of the tree corresponds to the empty code word, the branching points of the tree correspond to the branching points of the code, and the endpoints of the tree correspond to codewords belonging to the code. Two vertices of the tree are connected by an edge if the two corresponding codewords a and b are such that a is a prefix of b and $|b| - |a| = 1$.

In what follows we shall count search codes satisfying certain conditions. We shall use throughout the paper the method of generating functions. An other way to solve these problems is by means of the mentioned correspondence between codes and trees, making use of the methods of the theory of trees. However, this approach has the disadvantage, that to different codes there may correspond the same tree. In dealing with regular codes this does not cause any difficulty, but in the general case the counting of trees is somewhat more involved: as a matter of fact for some types of codes in the present paper, we get explicit formulae for the total number of codes, while for the number of the corresponding trees we were able to get explicit formulas only for the corresponding generating functions. In view of this we do not deal here at all with the counting of trees corresponding to the search-codes considered. However, we intend to return to these questions elsewhere.

§ 2. Enumeration of regular search-codes

Let C be a regular search code of degree $q \geq 2$. First we prove the following

LEMMA. *If C is a regular search-code of degree q then the size $N(C)$ of the code C satisfies the following congruence relation:*

$$(2.1) \quad N(C) \equiv 1 \pmod{q-1}.$$

Conversely, if n is a natural number such that $n-1$ is divisible by $q-1$, then there exist regular search codes of degree q and size n .

PROOF. Let $E(C)$ denote the number of pairs (a, b) of code-words, such that both C_a and C_b are different from the empty code, further a is a prefix of b and $|b| - |a| = 1$. To determine $E(C)$ we may first fix a and count in how many ways b can be chosen, or conversely, fix b and consider in how many ways a can be chosen. Thus we obtain two expressions, and equating these we shall get (2.1). Evidently a can be chosen as one of the branching points of C , i.e. in $B(C)$ ways, and if a is fixed, by definition b can be chosen in $b(C_a) = q$ ways; thus

$$(2.2) \quad E(C) = q \cdot B(C).$$

On the other hand, b can be chosen in $B(C) + N(C) - 1$ ways,* and to every b there corresponds a uniquely determined a , obtained by omitting the last letter of b . Thus

$$(2.3) \quad E(C) = B(C) + N(C) - 1.$$

Comparing (2.2) and (2.3) we get

$$(2.4) \quad N(C) = B(C)(q-1) + 1$$

which proves (2.1).

REMARK. $E(C)$ is equal to the number of edges of the tree corresponding to the code C .

The second statement of the lemma can be proved by induction as follows: If $n=1$, there exists a (unique) regular code of degree q and size $N(C)=1$, namely the trivial code. Suppose we have already constructed a regular search code of degree q and having size $N(C)=n$, where $n-1$ is divisible by $q-1$. Take any one of the codewords c belonging to the code C , omit c from C and add to C the q code-words obtained by adding to the end of c the suffix of length 1 consisting of the single letter k , where k is any one of the numbers $0, 1, \dots, q-1$. In this way we obtain a code C' which is regular of degree q and has size $N(C') = n + q - 1$. This proves Lemma 1.

We shall determine now the total number $C_q(n)$ of regular search codes of degree q and size n , where of course $n \equiv 1 \pmod{q-1}$. We shall prove the following

THEOREM 1. *For every natural number n of the form $n = k(q-1) + 1$ ($k=0, 1, \dots$) one has*

$$(2.5) \quad C_q(n) = \frac{(kq)!}{k! \cdot n!}.$$

* We can namely choose for b any codeword belonging to C and any branching point of C , except e .

PROOF. Clearly $C_q(1)=1$, and for every $n = k(q-1)+1$ with $k \geq 1$ we have the recursion formula

$$(2.6) \quad C_q(n) = \sum_{n_1+n_2+\dots+n_q=n} C_q(n_1)C_q(n_2)\dots C_q(n_q),$$

where the summation has to be extended only over those values of n_j for which $C_q(n_j)$ is defined i.e. for $n_j \equiv 1 \pmod{q-1}$.

Let us put

$$(2.7) \quad G_q(y) = \sum_{n \equiv 1 \pmod{q-1}} C_q(n) x^n.$$

We get from (2.6)

$$(2.8) \quad G_q(y) = y + (G_q(y))^q.$$

From (2.8) one can deduce, by the Bürmann—Lagrange formula for the power series of the inverse function of a given function, that

$$(2.9) \quad G_q(y) = \sum_{k=0}^{\infty} \frac{(kq)!}{k!(k(q-1)+1)!} y^{k(q-1)+1},$$

i.e. that (2.5) holds.

REMARK. The power series expansion (2.9) can be interpreted as the power series of that real root x of the trinomial equation $x - x^q = y$, which reduces to 0 for $y=0$. It is easy to see that the power series (2.9) is convergent for $|y| \leq \frac{q-1}{q^{q-1}}$ and thus (2.9) solves the equation $x - x^q = y$ for a given value of y if $|y| \leq \frac{q-1}{q^{q-1}} = R_q$. Notice that R_q tends increasingly to 1 for $q \rightarrow +\infty$.

We want to add some remarks on the special case $q=2$, i.e. the case of *binary search codes*. If $q=2$, then by Lemma 1 $N(C) = B(C) + 1$ i.e. there exist regular binary search codes of any size $n \geq 1$, and we get from (2.5) that their total number is

$$(2.10) \quad C_2(n) = \frac{\binom{2n-1}{n}}{(2n-1)} = \frac{(2n-3)!! 2^{n-1}}{n!}.$$

This formula has been known already to A. CAYLEY (see [2] and [3]), who solved the corresponding problem for counting trees. Cayley pointed out also that $C_2(n)$ is equal to the number of possible interpretations of a „product” of n factors with respect to a nonassociative operation, i.e. $C_2(n)$ is equal to the possible bracketings of such a „product”.

Thus Theorem 1 is a straightforward generalization of Cayley's classical results. It seems improbable that this generalization has not been made previously, but I did not find it in the literature.

Let us notice that for $q=2$ we get from (2.8) the explicit formula

$$(2.11) \quad G_2(y) = \frac{1 - \sqrt{1-4y}}{2}.$$

§ 3. Enumeration of all search codes of given size

Let $D(n, k)$ denote the total number of search codes of size n and having k branching points. Evidently $k \leq n-1$, as for a given size the number of branching points is maximal if the code is binary. It is easy to see that $D(1, 0) = 1$, $D(n, 0) = 0$ if $n \geq 2$, and for $n \geq 2$ the following recursion formula holds:

$$(3.1) \quad D(n, k) = \sum_{l=2}^n \sum_{\substack{n_1+n_2+\dots+n_l=n \\ k_1+k_2+\dots+k_l=k-1}} D(n_1, k_1) D(n_2, k_2) \dots D(n_l, k_l).$$

Let us put

$$(3.2) \quad \sum_{n=1}^{\infty} \sum_{k=0}^{\infty} D(n, k) x^n y^k = d(x, y).$$

It follows that

$$(3.3) \quad d(x, y) = x + \frac{y d^2(x, y)}{1 - d(x, y)}.$$

Thus we get

$$(3.4) \quad d(x, y) = \frac{1+x - \sqrt{(1+x)^2 - 4x(y+1)}}{2(y+1)}.$$

Let us denote now by $D(n)$ the total number of search codes of size n . It follows, putting

$$(3.5) \quad \delta(x) = \sum_{n=1}^{\infty} D(n) x^n,$$

that

$$(3.6) \quad \delta(x) = d(x, 1) = \frac{1+x - \sqrt{1-6x+x^2}}{4}.$$

From (3.4) and (3.6) we can get explicit formulae for $D(n, k)$ and $D(n)$, respectively. By some easy calculations we get

$$(3.7) \quad D(n, k) = \frac{1}{n} \binom{n-2}{k-1} \binom{n+k-1}{k} \quad (n \geq 2, k \geq 1)$$

and thus

$$(3.8) \quad D(n) = \frac{1}{n} \sum_{k=1}^{n-1} \binom{n-2}{k-1} \binom{n+k-1}{k} \quad (n \geq 2).$$

From (3.6) we obtain for $D(n)$ the asymptotic formula

$$(3.9) \quad D(n) \sim \frac{\sqrt{3-2\sqrt{2}}}{4\sqrt{\pi}} \frac{(3+2\sqrt{2})^n}{n^{3/2}}.$$

The first values of $D(n)$ are $D(2)=1$, $D(3)=3$, $D(4)=11$, $D(5)=45$, and $D(6)=197$.

We consider now the following enumeration problem: let $D_*(n)$ denote the total number of search codes of size n consisting of codewords all having length

$\leq r$ ($r=1, 2, \dots$). By the same type of argument which led us to (3.3) we obtain, putting

$$(3.10) \quad \delta_r(x) = \sum_{n=1}^{\infty} D_r(n) x^n$$

that

$$(3.11) \quad \delta_r(x) = x + \frac{\delta_{r-1}^2(x)}{1 - \delta_{r-1}(x)}.$$

Thus we get successively

$$\delta_1(x) = \frac{x}{1-x},$$

$$\delta_2(x) = x + \frac{x^2}{(1-x)(1-2x)},$$

$$\delta_3(x) = x + \frac{x^2(1-2x+2x^2)^2}{(1-x)(1-2x)(1-4x+4x^2-2x^3)},$$

etc.

Evidently

$$(3.12) \quad \lim_{r \rightarrow +\infty} \delta_r(x) = \delta(x).$$

One can determine similarly the generating functions of the total number of *regular* search codes of degree q and size n , consisting of codewords all having the length $\leq r$. If the number of such codes is denoted by $B_q(n, r)$, and we put

$$(3.13) \quad \beta_q(r, x) = \sum_{\substack{n=1 \\ n \equiv 1 \pmod{q-1}}}^{\infty} B_q(n, r) x^n$$

we obtain $\beta_q(0, x) = x$ and

$$(3.14) \quad \beta_q(r, x) = x + [\beta_q(r-1, x)]^q \quad (r=1, 2, \dots).$$

Especially we get for the binary case $\beta_2(0, x) = x$ and

$$(3.15) \quad \beta_2(r, x) = x + \beta_2^2(r-1, x) \quad \text{for } r \geq 1.$$

Thus we get successively the polynomials

$$\beta_2(1, x) = x + x^2,$$

$$\beta_2(2, x) = x + (x + x^2)^2,$$

$$\beta_2(3, x) = x + [x + (x + x^2)^2]^2,$$

etc.

Let $B_2(r)$ denote the total number of binary search codes, consisting of codewords all having length $\leq r$, irrespectively of the number of codewords in the code. As clearly

$$(3.16) \quad B_2(r) = \sum_{n=1}^{\infty} B_2(n, r) = \beta_2(r, 1),$$

we get the recursion formula

$$(3.17) \quad \begin{aligned} B_2(0) &= 1, \\ B_2(r+1) &= 1 + B_2^2(r) \quad \text{for } r \geq 0 \end{aligned}$$

from which one can calculate successively the values of $B(r)$. We have $B_2(1)=2$, $B_2(2)=5$, $B_2(3)=26$, $B_2(4)=677$, $B_2(5)=458330$. (Notice that the trivial code is counted here as the unique binary code consisting of a single codeword of length 0.) If $b(r)$ denotes the total number of binary search codes such that the length of the longest codeword of the code is equal to r , then $b_2(r) = B_2(r) - B_2(r-1)$; thus we have $b_2(1)=1$, $b_2(2)=3$, $b_2(3)=21$, $b_2(4)=651$ etc.

One can get from (3.17) also asymptotic formulae for the sequences $B_2(r)$ resp. $b_2(r)$ for $r \rightarrow +\infty$.

References

- [1] A. RÉNYI, Lectures on the mathematical theory of search, *Department of Statistics of the University of North Carolina*. (In print.)
- [2] A. CAYLEY, On the theory of the analytical forms called trees. I—II, *Philosophical Magazine*, **13** (1857), pp. 172—176 and **18** (1859), pp. 347—378.
- [3] A. CAYLEY, A theorem on trees, *Quarterly Journal of Pure and Applied Mathematics*, **23** (1889) pp. 376—378.

182, 187, 192, 193, 213, 249, 256, 320, 340

NOTE

In papers Nos. 182, 187, 192, 193, 213, 249, 256, 320, 344 Rényi developed a theory of search. His interest in search theory was aroused, as he often said, by an event when a mechanic did not find an electrical trouble of his car and he had to help him. His results belong mostly to random search, but he raised personally a lot of problems in non-random search.

In paper No. 193 he proved (Theorem 2a), that if we choose the subsets randomly in such a way that the average size of the subsets is pn (n is the total number of elements, $0 < p < 1$), then we need not much more, than $\log n/I_1(p, 1-p)$ questions to identify the unknown element. He put the question in his seminary on search theory: what is the situation if we use non-random search but the size of the subsets is fixed ($l = [pn]$). Suppose, on the other hand, that the next question cannot depend on the answers of the previous questions. Next week B. Bollobás, J. Galambos, G. O. H. Katona, T. O. H. Nemetz and D. O. H. Szász had independently a partial solution: If $n \geq \frac{l(l+1)}{2} + 1$,

then there is a family of $\left\{ 2 \frac{n-1}{l+1} \right\}$ ($\{x\}$ is the least integer $\geq x$) subsets identifying the unknown element, and this is the smallest possible number. The result is a little bit disappointing; we could expect the number $\log n/I_1\left(\frac{l}{n}, \frac{n-l}{n}\right)$, however in this case $l \sim \sqrt{n}$, that is, $l/n \sim 0$; this formula cannot work.

However for larger l we can have something similar. Katona proved [1] that for the smallest number m of subsets the following inequalities hold:

$$\frac{\log n}{\log \frac{en}{l}} \cdot \frac{n}{l} \leq \frac{\log n}{I_1\left(\frac{l}{n}, \frac{n-l}{n}\right)} \leq m \leq \left\lceil \frac{\log 2n}{\log n/l} \right\rceil \frac{n}{l} \left(l \leq \frac{n}{2} \right),$$

and it is easy to see (it is not done in the paper) that in the case $n \rightarrow \infty$ $l/n \rightarrow p$

$$m \sim \frac{\log n}{I_1(p, 1-p)}$$

holds.

If we do not have any restriction on the size of the subsets, then the minimal m does not depend on whether the questions cannot depend on the previous answers or they can. Here, the situation is different. For the latter case the exact minimum of the maximal number of questions is determined [2]:

$$\left\lceil \frac{n}{l} \right\rceil - 2 + \left\lceil \log \left(n - \left(\left\lceil \frac{n}{l} \right\rceil - 2 \right) \right) \right\rceil.$$

The optimal strategy is the following: We choose disjoint l -tuples $A_1, \dots, A_{\left\lceil \frac{n}{l} \right\rceil - 2}$ and ask whether the unknown element is contained in $A_1, \dots, A_{\left\lceil \frac{n}{l} \right\rceil - 2}$. After $\left\lceil \frac{n}{l} \right\rceil - 2$ questions we know that the unknown element is either in one of the A_i 's or in the set B of the remaining elements. The number of elements of B is $n - l \left(\left\lceil \frac{n}{l} \right\rceil - 2 \right)$, where $l < n - l \left(\left\lceil \frac{n}{l} \right\rceil - 2 \right) \leq 2l$. Now we can use the simple halving in at most $\left\lceil \log \left(n - l \left(\left\lceil \frac{n}{l} \right\rceil - 2 \right) \right) \right\rceil$ steps.

Theorem 2b of paper No. 193 generalizes the statement of theorem 2a for general classifications (when one question divides the set into r disjoint ($r \geq 2$) parts). Then we need somewhat more than $\log n / I_1(p_1, \dots, p_r)$ random subsets if the sizes of the subsets are in average $p_1 n, \dots, p_r n$. The corresponding question for non-random search is solved by Zs. Baranyai [3]: If one question divides the set into disjoint subsets of $l_1, l_2, \dots, l_r$ ($l_1 + \dots + l_r = n$) elements, respectively, and the questions cannot depend on the previous answers, then for the minimal number m of questions the inequality

$$\frac{\log n}{I_1\left(\frac{l_1}{n}, \dots, \frac{l_r}{n}\right)} \leq m \leq \frac{\log n + \log \frac{n}{l_1} + \dots + \log \frac{n - l_1 - \dots - l_{r-2}}{l_{r-1}}}{\frac{l_1}{n} \log \frac{n}{l_1} + \dots + \frac{l_{r-1}}{n} \log \frac{n - l_1 - \dots - l_{r-2}}{l_{r-1}}}$$

holds ($l_1 \leq \dots \leq l_r$).

On the other hand, if $n \rightarrow \infty$, $l_i/n \rightarrow p_i$ ($1 \leq i \leq r$) then

$$m \sim \frac{\log n}{I(p_1, \dots, p_r)}$$

Another interesting question arises in paper No. 193. In theorem 2b we want to determine only one unknown element by random subsets. The necessary number of subsets is about $\log n/I_1(p_1, \dots, p_r)$. The problem, when l unknown elements are given at the same time and we want to identify them simultaneously, is solved (Theorem 3b) for $l = n$ only. In this case, the necessary number of questions is about $\log n/I_2(p_1, \dots, p_r)$, where $I_2(p_1, \dots, p_r)$ is the entropy of order 2 (see papers Nos. 143 and 180). What kind of entropy plays a role for general l 's?

In paper No. 344 several formulas are given for the sizes of certain classes of search codes. Chorneyko and Mohanty [4] have new results on this subject. Let us order the codewords of a code C in lexicographic order, and order the branching points in that order. Denote by $S(q_1, \dots, q_k)$ ($q_i \geq 2$, $i = 1, \dots, k$) the codes having branching numbers $q_1, \dots, q_k$ in this order. A *lattice path* to the point (m, n) ($m, n \geq 0$ integers) is a path in the two-dimensional lattice from $(0, 0)$ to (m, n) consisting of unit horizontal and vertical steps. It is well known that such a path can be uniquely represented by a vector $(x_1, \dots, x_n)$ ($0 \leq x_1 \leq \dots \leq x_n \leq m$) where x_i is the horizontal distance from the point $(m, n - i)$ to the path. A lattice path l corresponding to the vector $(x_1, \dots, x_n)$ *dominates* the lattice path l' corresponding to the vector $(x'_1, \dots, x'_n)$, if and only if $x'_i \leq x_i$ ($i = 1, \dots, n$). Let $L(q_1, \dots, q_k)$ denote the set of all lattice paths to the point $a_k = \left(\sum_{i=1}^k q_i - k + 1, k \right)$ beginning with a unit horizontal step, and ending with a unit vertical step, which are dominated by the lattice path corresponding to the vector $(0, a_1, \dots, a_{k-1})$ where $a_j = \sum_{i=1}^j q_i - j$ ($j = 1, 2, \dots, k - 1$). The authors prove a one to one correspondence between $S(q_1, \dots, q_n)$ and $L(q_1, \dots, q_n)$. Using this fact it is proved that the number of elements of $S(q_1, \dots, q_n)$ is $\det (a_{ij})_{(k-1) \times (k-1)}$, where

$$a_{ij} = \begin{cases} 0 & \text{if } i > j + 1 \\ \binom{a_{k-j} + 1}{j - i + 1} & \text{otherwise.} \end{cases}$$

Some of Rényi's results can be deduced from this one.

In 1969 Prof. Rényi had a seminar on search theory at Chapel Hill (see paper No. 320). J. N. Srivastava, who is an expert of statistical designs, attended a few of these lectures. He started to think about the connections of search and statistical designs and created the concept of "search designs" [5]. Let $T = (t_{ij})$ be an $N \times m$ 0 - 1 matrix. Then the $N \times 2^m$ matrix $A(T) = (a_{iS})$ ($1 \leq i \leq N$, S is a subset of $\{1, 2, \dots, m\}$) is defined by $a_{iS} = \prod_{j \in S} (2t_{ij} - 1)$. T is a *search*

design of resolving power k , if any $2k$ columns of $A(T)$ are independent. Such designs can be used in statistical situations, when v parameters ($v \gg k$) are given, only k of them are nonnegligible, and we want to search the k non-negligible ones and estimate them. Theorems for $k = 1$ and 2 are given in [5]. In a forthcoming paper of J. N. Srivastava there are results concerning the case $k = 3$.

The results of paper No. 213 are generalized by Lindström ([6], [7], [8]). In [6] the conjectures of Erdős and Rényi are proved:

$$\lim_{n \rightarrow \infty} \frac{A(n) \log_2 n}{n} = \lim_{n \rightarrow \infty} \frac{B(n) \log_2 n}{n} = 2.$$

In [7] the problem is generalized. Let M be a finite set of the real numbers. An $m \times n$ matrix A with entries from M is called a detecting matrix if the vectors Ax are different for different column-vectors with entries from M . For fixed n $f_M(n)$ is the minimal number of rows (m) of detecting matrices. It is easy to see, that $f_{\{0,1\}}(n) = A(n)$ and $f_{\{-1,1\}}(n) = B(n)$.

Let r be the rank of M , that is the minimal integer such that every element of M can be written in the form $\sum_{i=1}^r a_i e_i$, where e_i 's are fixed real and a_i 's are rational numbers. If for any element $\sum_{i=1}^r a_i e_i$ of M $\sum a_i = 1$ holds, then $d = r - 1$, otherwise $d = r$ is the *detecting rank* of M . It is independent of the particular basis chosen. It is proved in [7], that

$$\lim_{n \rightarrow \infty} \frac{f_M(n) \log_2 n}{n} = \frac{2}{d}.$$

The best result for $M = \{0, 1\}$ is

$$f_M(n) = \frac{2n}{\log n} + o\left(\frac{n \log \log n}{\log^2 n}\right).$$

It is proved by D. G. Cantor and W. H. Mills [9].

Another generalized version of the problem: M is a set of integers, the $m \times n$ matrix A has entries from M , the vectors x have entries $0, 1, \dots, k-1$, ($k \geq 2$) and Ax have to be different for different x 's. $f_{k,M}(n)$ is the minimum number of rows of A under this condition. In [8] the statement

$$\lim_{n \rightarrow \infty} \frac{f_{k,M}(n) \log_2 n}{n} = 2$$

is proved.

As regards random search (No. 249) an interesting generalization is given by Vajda [10]. He considered the case, when the i th question is a set of conditional probabilities $P_i(m | x)$ where $m \in \{1, 2, \dots, M\}$ is the answer and x is the unknown element. In Rényi's case in paper No. 249 $P_i(m | x)$ is always 0 or 1. On the other hand, in paper No. 187 $M = 2$ and $P_i(1 | x) = 1 - \beta$, $P_i(0 | x) = \beta$ for $x \in A_i$ and $P_i(1 | x) = \beta$, $P_i(0 | x) = 1 - \beta$ otherwise. Vajda considers random choice of questions and he has similar results to Rényi's one, but in the results Chernoff's information measure appears. (Gy. K.)

REFERENCES

- [1] Katona, G. O. H.: On separating systems of a finite set. *Journal of Combinatorial Theory*, 1 (1966), 174–194.
- [2] Katona, G. O. H.: Combinatorial search problems. *A survey of combinatorial theory*. Ed. by J. N. Srivastava, North-Holland Publishing Co., Amsterdam, 285–308.
- [3] Baranyai, Zs.: On a search problem of G. O. H. Katona (submitted to *Studia Sci. Math. Hung.*).

- [4] Chorneyko, I. Z. and Mohanty, S. G.: On the enumeration of pseudosearch codes. *Studia Sci. Math. Hung.*, 7 (1972), 47—54.
- [5] Srivastava, J. N.: Designs for searching non-negligible effects (to be published later).
- [6] Lindström, B.: On a combinatorial detection problem I. *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, Ser. A, 9 (1964), 195—206.
- [7] Lindström, B.: On a combinatorial detection problem II, *Studia Sci. Math. Hung.*, 1 (1966), 353—361.
- [8] Lindström, B.: On a combinatorial problem in number theory. *Canad. Math. Bull.*, 8 (1965), 477—490.
- [9] Cantor, D. G. and Mills, W. H.: Determination of a subset from certain combinatorial properties. *Canadian Journ. Math.*, 18 (1966), 42—48.
- [10] Вайда, И.: О случайном планировании экспериментов. *Проблемы передачи Информации*, 4 (1968), (4) 26—36.

ON THE NUMBER OF ENDPOINTS OF A k -TREEby
A. RÉNYI

§ 1. Definitions

A k -tree ($k=1, 2, 3, \dots$) is the natural generalization to k dimensions of an ordinary (i.e. one-dimensional) tree (see [1], [2], [3], [4]). A k -tree can be considered either as a k -dimensional simplicial complex with certain properties, or as a graph. We shall take the second point of view.

A k -tree can be most conveniently defined inductively as follows: A k -tree of order $k+1$ is a complete $(k+1)$ -graph. A k -tree $t_{n+1}^{(k)}$ of order $n+1$ ($n \geq k+1$) is obtained by choosing an arbitrary k -tree $t_n^{(k)}$ of order n , and adding a new vertex, joining it to k such points of $t_n^{(k)}$ which form a complete graph in $t_n^{(k)}$, i.e. to the points of a $(k-1)$ -cell of $t_n^{(k)}$. Thus a k -tree of order n contains n points (vertices), $n-k$ k -cells (i.e. complete subgraphs of order $k+1$) and $k(n-k)+1$ $(k-1)$ -cells (i.e. complete subgraphs of order k).

A point of a k -tree of order n ($n \geq k+1$) is called an *endpoint* if it belongs to a single k -cell of the k -tree.

It is easy to see by induction that the number of endpoints of a k -tree of order $n \geq k+1$ is at least 2 and at most $n-k$.

As a matter of fact two endpoints can not belong to the same $(k-1)$ -cell if $n \geq k+2$; thus if we take a k -tree $t_n^{(k)}$ of order $n \geq k+2$ and form a k -tree $t_{n+1}^{(k)}$ of order $n+1$ by adding to $t_n^{(k)}$ a new point (joining it with the points of a $(k-1)$ -cell of $t_n^{(k)}$) then the new point will be an endpoint, of $t_{n+1}^{(k)}$ and among the endpoints of $t_n^{(k)}$ at most one will not be an endpoint of $t_{n+1}^{(k)}$, thus the number of endpoints is either unchanged, or is increased by one; as a k -tree of order $k+2$ consists of two k -cells which have a $(k-1)$ -cell in common and thus it contains exactly 2 endpoints, it follows that any k -tree of order $n \geq k+2$ contains at least 2 and at most $n-k$ endpoints.

In this paper we consider *labeled*, more exactly: point-labeled k -trees, i.e. such k -trees of order n , the points of which are labeled by the numbers $1, 2, \dots, n$. It has been shown (see [2] and [3]) that denoting by $T_k(n)$ the total number of labeled k -trees of order n , one has

$$(1) \quad T_k(n) = \binom{n}{k} [k(n-k)+1]^{n-k-2} \quad (k=1, 2, \dots).$$

The aim of the present paper is to determine the number $T_k(n, r)$ of labeled k -trees of order n having r endpoints ($2 \leq r \leq n-k$). The corresponding problem for 1-trees has been solved in [5].

§ 2. Exact formulae

We prove first the following recursion formula

$$(2) \quad T_k(n+1, r) = (n+1)[(k(n-k-r+1)+1)T_k(n, r-1) + rkT_k(n, r)]$$

where $2 \leq r \leq n+1-k$, $n \geq k+2$.

To prove (2) let us mention that if we take any k -tree $t_n^{(k)}$ of order n having r endpoints, and join a new point to one of the $(k-1)$ -cells of $t_n^{(k)}$ containing an endpoint of $t_n^{(k)}$, we get a k -tree $t_{n+1}^{(k)}$ of order $n+1$ with r endpoints, because one endpoint of $t_n^{(k)}$ disappears and one new endpoint is created. On the other hand if we take a k -tree $t_n^{(k)}$ of order n having $r-1$ endpoints and join a new point to one of the $(k-1)$ -cells not containing any of the endpoints of $t_n^{(k)}$, we get a k -tree $t_{n+1}^{(k)}$ of order $n+1$ having r endpoints, because all the $r-1$ endpoints of $t_n^{(k)}$ will be endpoints of $t_{n+1}^{(k)}$, and the new point will also be an endpoint of $t_{n+1}^{(k)}$. If we do this with all k -trees of order n labeled by the numbers $1, 2, \dots, n+1$ except j (where $j = 1, 2, \dots, n+1$), we get all possible k -trees of order $n+1$ having r endpoints, each exactly r times; taking into account that each endpoint of a k -tree of order $n \geq k+2$ belongs to k of its $k(n-k)+1$ $(k-1)$ -cells, (2) follows.

Let us put now

$$(3) \quad t_k(n, s) = \frac{T_k(n, n-s)}{\binom{n}{s}}.$$

It follows that

$$(4) \quad t_k(n+1, s) = [k(s-k)+1] \cdot t_k(n, s) + ks t_k(n, s-1) \quad \text{for } k \leq s \leq n-1,$$

where $t_k(k+1, k) = 0$.

Thus, putting

$$(5) \quad G_k(z, s) = \sum_{n=s+2}^{+\infty} t_k(n, s) z^{n-s-2} \quad (s = k, k+1, \dots)$$

we obtain

$$(6) \quad G_k(z, s) = \frac{ks G_k(z, s-1)}{1 - z[k(s-k)+1]}.$$

As however $T_k(n, n-k) = \binom{n}{k}$ if $n \geq k+2$, we have

$$(7) \quad G_k(z, k) = \frac{1}{1-z}.$$

Thus it follows from (6) that

$$(8) \quad G_k(z, s) = \frac{s! k^{s-k}}{k! \prod_{j=0}^{s-k} (1 - z(jk+1))}.$$

It follows in particular for $k=1$ that

$$(9) \quad G_1(z, s) = \frac{s!}{\prod_{h=1}^s (1-hz)}.$$

Now it is known (see [5]) that for $k=1$

$$(10) \quad T_1(n, n-s) = S(n-2, s) s! \binom{n}{s}$$

where $S(m, s)$ are the Stirling numbers of the second type, defined by

$$(11) \quad y^m = \sum_{s=1}^m S(m, s) y(y-1) \dots (y-s+1).$$

From (10) we can deduce (9) directly as follows.

It follows from (11) that

$$(12) \quad \sum_{m=s}^{\infty} \frac{S(m, s) z^m}{m!} = \frac{(e^z - 1)^s}{s!}$$

and thus for $|z| < \frac{1}{s}$

$$(13) \quad \sum_{m=s}^{\infty} S(m, s) z^m = \sum_{m=s}^{\infty} \frac{S(m, s) z^m}{m!} \int_0^{\infty} y^m e^{-y} dy = \int_0^{\infty} \frac{(e^{zy} - 1)^s}{s!} e^{-y} dy.$$

It follows by partial integration that

$$(14) \quad \sum_{m=s}^{\infty} S(m, s) z^m = \frac{z^s}{\prod_{h=1}^s (1-hz)}$$

i. e.

$$(15) \quad G_1(z, s) = s! \sum_{m=s}^{\infty} S(m, s) z^{m-s} = \frac{s!}{\prod_{h=1}^s (1-hz)}$$

in accordance with (9).

To get an explicit expression for $T_k(n, r)$ we need the following identity

$$(16) \quad \frac{1}{\prod_{j=0}^m [1 - z(jk+1)]} = \frac{1}{m! k^m} \sum_{j=0}^m \binom{m}{j} \frac{(-1)^{m-j} (jk+1)^m}{1 - z(jk+1)}$$

which can be proved e.g. by elementary function theory.

It follows from (8) and (16)

$$(17) \quad G_k(z, s) = \binom{s}{k} \sum_{j=0}^{s-k} \binom{s-k}{j} \frac{(-1)^{s-k-j} (jk+1)^{s-k}}{1 - z(jk+1)}$$

and thus

$$(18) \quad t_k(n, s) = \frac{T_k(n, n-s)}{\binom{n}{s}} = \binom{s}{k} \sum_{j=0}^{s-k} \binom{s-k}{j} (-1)^{s-k-j} (jk+1)^{n-k-2}.$$

Thus we obtain finally

$$(19) \quad T_k(n, n-s) = \binom{n}{s} \binom{s}{k} \sum_{j=0}^{s-k} \binom{s-k}{j} (-1)^{s-k-j} (jk+1)^{n-k-2}.$$

By adding the values of $T_k(n, n-s)$ for $s = k, k+1, \dots, n-2$ we must of course get the known formula (1) (see [2], [3]) for the total number $T_k(n)$ of k -trees of order n . As a matter of fact we get from (19)

$$(20) \quad T_k(n) = \sum_{s=k}^{n-2} T_k(n, n-s) = \binom{n}{k} \sum_{j=0}^{n-k-2} \binom{n-k}{j} (jk+1)^{n-k-2} (n-k-j-1) (-1)^{n-k-j}.$$

Taking into account that

$$\begin{aligned} & \sum_{j=0}^{n-k-2} \binom{n-k}{j} (jk+1)^{n-k-2} (n-k-j-1) = \\ &= \frac{1}{k} [(k(n-k-1)+1)H^{(n-k-2)}(0) - H^{(n-k-1)}(0)] \end{aligned}$$

where

$$H(x) = e^x [(e^{kx} - 1)^{n-k} + (n-k)e^{k(n-k-1)x} - e^{k(n-k)x}]$$

and we have

$$H^{(n-k-2)}(0) = (n-k)[k(n-k-1)+1]^{n-k-2} - [k(n-k)+1]^{n-k-2}$$

and

$$H^{(n-k-1)}(0) = (n-k)[k(n-k-1)+1]^{n-k-1} - [k(n-k)+1]^{n-k-1}$$

and thus

$$\frac{1}{k} [(k(n-k-1)+1)H^{(n-k-2)}(0) - H^{(n-k-1)}(0)] = [k(n-k)+1]^{n-k-2}$$

it follows that (1) holds.

Thus as a by-product we obtained another proof of the formula (1). Notice that for $k=1$ (1) reduces to CAYLEY's celebrated formula $T_1(n) = n^{n-2}$ for the total number of ordinary (one-dimensional) trees of order n . (For other proofs of this formula see [6] and [7].)

§ 3. The moments of the distribution of the number of endpoints

Let us first consider the mean value and the variance of the number of endpoints of a k -tree of order n . For the mean value

$$(21) \quad M_k(n) = \frac{1}{T_k(n)} \sum_{r=2}^{n-k} r T_k(n, r)$$

we get from the recursion formula (2) immediately

$$(22) \quad M_k(n) = \frac{n T_k(n-1)}{T_k(n)} [k(n-k-1) + 1]$$

and thus

$$(23) \quad M_k(n) = \frac{n-k}{\left(1 + \frac{k}{k(n-k-1)+1}\right)^{n-k-2}}.$$

Thus we have

$$(24) \quad \lim_{n \rightarrow +\infty} \frac{M_k(n)}{n} = \frac{1}{e} \quad \text{for } k = 1, 2, 3, \dots$$

Similarly we get from (2) for the variance

$$(25) \quad D_k^2(n) = \frac{1}{T_k(n)} \sum_{r=2}^{n-k} [r - M_k(n)]^2 T_k(n, r)$$

$$(26) \quad D_k^2(n) = \frac{(n-k-1)(n-k)[(n-k-2)k+1]^{n-k-3}}{[k(n-k)+1]^{n-k-2}} + \\ + \frac{(n-k)[k(n-k-1)+1]^{n-k-3}}{[k(n-k)+1]^{n-k-2}} - \frac{(n-k)^2[k(n-k-1)+1]^{2n-2k-6}}{[k(n-k)+1]^{2n-2k-4}}$$

and thus

$$(2.7) \quad \lim_{n \rightarrow +\infty} \frac{D_k^2(n)}{n} = \frac{1}{e} \left(1 - \frac{2}{e}\right) \quad (k = 1, 2, \dots).$$

It is remarkable that the asymptotic formulae for $M_k(n)$ and $D_k^2(n)$ do not depend on k , i.e. are the same as those obtained in [5] for $k=1$.

In [5] we have proved that if we choose at random one of the n^{n-2} labeled trees of order n , so that any one of these is chosen with the same probability, then denoting by v_n the number of endpoints of this random tree, the distribution of the random variable $\frac{v_n - M_1(n)}{D_1(n)}$ tends for $n \rightarrow +\infty$ to the standard normal distribution. By considering moments of every order one can prove that the same holds for every k , i.e. if we choose at random, with uniform distribution one of the $T_k(n)$ labeled k -trees of order n , and denote the number of its endpoints by $v_n^{(k)}$, then the distribution of $\frac{v_n^{(k)} - M_k(n)}{D_k(n)}$ tends for $n \rightarrow +\infty$ to the standard normal distribution.

REFERENCES

- [1] HARARY, F. and PALMER, E. M.: On Acyclic simplicial complexes; *Mathematika* **15** (1968) 115—122.
- [2] BEINEKE, L. W. and PIPPERT, R. E.: The number of labeled k -dimensional trees, *Journal of Combinatorial Theory* **6** (1969) 200—205.
- [3] MOON, J. W.: The number of labeled k -trees, *Journal of Combinatorial Theory* **6** (1969) 196—199.
- [4] PALMER, E. M.: On the number of labeled 2-trees, *Journal of Combinatorial Theory* **4** (1969) 206—207.
- [5] RÉNYI, A.: Some remarks on the theory of trees, *Publ. Math. Inst. Hung. Acad. Sci.* **4** (1959) 73—85.
- [6] MOON, J. W.: *Various proofs of Cayley's formula for counting trees*, Seminar on Graph Theory, ed. by F. Harary.
- [7] RÉNYI, A.: On Cayley's polynomials for counting trees, *Proc. of the Calgary Int. Conference on Combinatorial Structures and their Applications* (in print).

163, 167, 332, **343**

Applications of probability theory to other areas of mathematics

Alfred Rényi

Mathematical Institute
Hungarian Academy of Sciences

0. Introduction. Probability theory was created for a definite purpose: for the mathematical investigation of random mass phenomena. However, after probability theory became an exact mathematical theory, its results can be applied in quite different fields, thus also to purely mathematical problems which have nothing to do with chance. This has in fact been done in several areas, and this led to the solution of many important problems, most of which could not be attacked by traditional methods of the area in question or by any other nonprobabilistic method. In what follows we shall discuss some selected typical applications of probability theory to number theory, algebra, combinatorial mathematics, geometry and several examples of such applications to analysis.

1. Number theory. Among those areas of mathematics in which probability theory has been successfully applied, *number theory* has to be mentioned at the first place, as probabilistic number theory has been much studied, since Gauss realized that the distribution of prime numbers is so irregular that only statistical statements make sense.

Among the most recent results I want to mention only one on the distribution of the numbers prime to n . Let $a_{n,1} < a_{n,2} < \dots < a_{n,k} < \dots$ denote all natural numbers which are prime to n . Let $\phi(n)$ denote Euler's function, i.e. put

$$(1.1) \quad \phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where p runs over all prime divisors of n . As is well known $\phi(n)$ is the number of natural numbers less than n and prime to n . Let us consider the intervals $[r, r + \lambda \cdot n/\phi(n))$ ($r = 1, 2, \dots, n$) where $\lambda > 0$ is any fixed number, and let $Q_n(\lambda, k)$ denote the number of those among these intervals which contain exactly k of the numbers $a_{n,j}$ ($1 \leq j \leq \phi(n)$) where k is any fixed nonnegative integer. Using the results of C. Hooley [1] I have recently proved [2] that if n tends to infinity through such values that $n/\phi(n) \rightarrow +\infty$, then we have

$$(1.2) \quad \lim_{n \rightarrow +\infty; n/\phi(n) \rightarrow +\infty} \frac{Q_n(\lambda, k)}{n} = \frac{\lambda^k e^{-\lambda}}{k!} \quad (k = 0, 1, \dots).$$

Thus we get in the limit a Poisson distribution. Still more is true: the distribution of the numbers $< n$ and prime to n resembles the Poisson process in every respect, including the independence-property. One can state this result also as follows: the strictly determined numbers $a_{n,1}, a_{n,2}, \dots, a_{n,\phi(n)}$ are distributed in the interval $[1, n)$ approximately as if they would have been chosen completely at random, if $\phi(n)/n$ is very small.

This theorem exemplifies that often probabilistic laws are inherent in the structure of nonrandom mathematical objects.

Probabilistic number theory is rich with results of this type. (See e.g. [3], [4], [5], [6]; in these further references can be found.)

2. Combinatorial problems. Let $A_n = (a_{j,k})$ ($1 \leq j \leq n; 1 \leq k \leq n$) be an n by n matrix each element of which is equal to $+1$ or -1 . Let $\varepsilon = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$ be a sequence with elements ± 1 . We consider the expression

$$(2.1) \quad M(A_n) = \min_{(\varepsilon)} \max_{1 \leq j \leq n} \left| \sum_{k=1}^n a_{j,k} \varepsilon_k \right|.$$

Recently P. Erdős and J. Komlós have proved¹ that there exists for every $n \geq 3$ a matrix A_n for which $M(A_n) > c\sqrt{n}$ where $c > 0$ is a constant, not depending on n . Their proof is an excellent example for such an application of probability theory where there is no hidden probabilistic law to be discovered: the apparatus of probability theory is introduced as an artifice to prove the existence of a combinatorial object, for which no method of construction is known. As a matter of fact in the given problem one can prove that for the majority of all n by n matrices with elements ± 1 one has $M(A_n) > c\sqrt{n}$ if c is such a number that

$$(2.2) \quad \frac{1}{(2\pi)^{1/2}} \int_c^{+\infty} e^{-x^2/2} dx > \frac{1}{4}$$

¹ My thanks are due to P. Erdős and J. Komlós for their kind permission to include this unpublished result in this paper.

and if $n \geq n_0(c)$; in other words if we choose the matrix A_n at random (with uniform distribution) among the 2^n n by n matrices with elements ± 1 , then, if n is sufficiently large, the probability will be near to 1 that for this random matrix we shall have $M(A_n) > c\sqrt{n}$. To show this let us first fix the values of $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$. Then for each j the random variable $s_j = \sum_{k=1}^n a_{jk}\varepsilon_k$ will have the distribution

$$(2.3) \quad P(s_j = k) = \binom{n}{(n+k)/2} \frac{1}{2^n}$$

if $k \equiv n \pmod{2}$ and $-n \leq k \leq +n$ and the random variables $s_1, \dots, s_n$ will be independent; this implies that

$$(2.4) \quad P\left(\max_{1 \leq j \leq n} |s_j| \leq c\sqrt{n}\right) = \left[\sum_{|k| \leq c\sqrt{n}} \binom{n}{(n+k)/2} \frac{1}{2^n} \right]^n.$$

By the de Moivre-Laplace theorem

$$(2.5) \quad \lim_{n \rightarrow +\infty} \sum_{|k| \leq c\sqrt{n}} \binom{n}{(n+k)/2} \frac{1}{2^n} = 1 - \frac{2}{(2\pi)^{1/2}} \int_c^\infty e^{-x^2/2} dx.$$

Putting

$$(2.6) \quad \alpha = 1 - \frac{2}{(2\pi)^{1/2}} \int_c^\infty e^{-x^2/2} dx,$$

we have by our supposition (2.2) $\alpha < \frac{1}{2}$. It follows that by choosing any number β such that $\alpha < \beta < \frac{1}{2}$, we have for sufficiently large values of n

$$P\left(\max_{1 \leq j \leq n} |s_j| \leq c\sqrt{n}\right) < \beta^n.$$

This means that among all 2^{n^2} matrices A_n there are at most $\beta^n \cdot 2^{n^2}$ exceptional matrices for which $\max |s_j| \leq c\sqrt{n}$ for any given choice of the values $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$. As the sequence $\varepsilon = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$ can be chosen in 2^n different ways, the number of matrices A_n which are exceptional for at least one choice of ε is at most $(2\beta)^n 2^{n^2}$. This implies that there are at least $(1 - (2\beta)^n) 2^{n^2}$ matrices A_n which are not exceptional for any ε , i.e. for which

$$(2.7) \quad M(A_n) > c\sqrt{n}.$$

As $2\beta < 1$, this means that such matrices exist if $n \geq n_0(c)$, in fact, (2.7) holds for the majority of n by n matrices A_n . Thus $\max M(A_n)/\sqrt{n}$ is bounded from below.

It should be added that an explicit example of a matrix A_n for which $M(A_n) > c\sqrt{n}$ is not known.² It is an open problem also whether $\text{Max } M(A_n)/\sqrt{n}$ is bounded from above.

As regards further applications of probability theory to the solution of combinatorial problems, see e.g. [7].

3. Statistical group theory. Let G_n be a finite Abelian group of order n . Let $b_1, b_2, \dots, b_k$ be k elements of G_n and let us consider the 2^k sums

$$(3.1) \quad \sum_{i=1}^k b_i \delta_i \quad \text{where } \delta_i = +1 \text{ or } \delta_i = 0 \text{ for } 1 \leq i \leq k.$$

Let $f(g)$ denote the number of representations of an element g of G_n in the form (3.1).

The following result has been proved by P. Erdős and A. Rényi [8]: For every $\varepsilon > 0$ there exists a number $c = c(\varepsilon)$ such that if

$$(3.2) \quad k > 2 \log n / \log 2 + c$$

then for almost all choices of the k elements $b_1, b_2, \dots, b_k$ we have

$$(3.3) \quad \frac{2^k}{n}(1 - \varepsilon) \leq f(g) \leq \frac{2^k}{n}(1 + \varepsilon)$$

for all $g \in G_n$.

The question whether the factor 2 of $\log n / \log 2$ in (3.2) can be replaced by a smaller number α ($1 < \alpha < 2$) for all Abelian groups G_n of order n , is open.

The proof of the above mentioned theorem depends on the evaluation of the mean value of

$$(3.4) \quad \sum_{g \in G_n} \left(f(g) - \frac{2^k}{n} \right)^2$$

for all possible choices of the k elements $b_1, b_2, \dots, b_k$; it turns out that this mean value is equal to $2^k(1 - 1/n)$, which implies that with probability $> 1 - \delta$,

$$\text{Max}_{g \in G_n} \left| f(g) - \frac{2^k}{n} \right| \leq \varepsilon \frac{2^k}{n} \quad \text{if } k > \frac{2 \log n + \log(1/\varepsilon\delta)}{\log 2}.$$

² Dr. R. Davidson has pointed out that any Hadamard matrix A_n of order n furnishes an example, such that $M(A_n) > \sqrt{n}$. This still leaves the question open for $n \not\equiv 0 \pmod{4}$ when no Hadamard matrix exists, and for those $n \equiv 0 \pmod{4}$ for which the existence of an Hadamard matrix is not known.

It is remarkable that the mean value of the second moment (3.4) does not depend on the structure of the group G_n . The same holds for the third moment but the mean value of the fourth moment

$$(3.5) \quad \sum_{g \in G_n} \left(f(g) - \frac{2^k}{n} \right)^4$$

depends already on the structure of G_n ; the mean value of (3.5) has been computed by J. Miech [9] and in a more explicit form—using the method of group-characters—by K. Bognár [10]; in this way it was possible to show that the factor 2 of $\log n / \log 2$ in (3.2) can be replaced by a smaller number for a large subclass of groups of order n .

As regards the applications of probabilistic methods to the theory of noncommutative finite groups, see the series of papers by P. Erdős and P. Turán [11] on statistical group theory.

4. Geometry. There is a whole chapter of geometry, which is based on the application of probabilistic ideas, namely integral geometry (see e.g. [12]). Some new results in probabilistic geometry have been obtained by A. Rényi and R. Sulanke [13], [14], [15].

Among these we mention only the following result: Let us choose at random and independently n straight lines $g_1, g_2, \dots, g_n$, cutting the unit circle C ; the random choice of g_k is done so that the distance of g_k from the center of C has a uniform distribution in the interval $(0, 1]$ and the direction of g_k is uniformly distributed in $[0, 2\pi)$ independently of ρ_k . Let H_k denote that half plane bounded by g_k which contains the center O of C ; then $\Pi_n = H_1 \cap H_2 \cap \dots \cap H_n$ is a convex polygon. Let v_n denote the number of sides of Π_n . It has been shown in [15] that the expectation of v_n tends to $\pi^2/2$.

It has been shown by W. Schmidt [16] that the limiting distribution

$$(4.1) \quad p_k = \lim_{n \rightarrow +\infty} P(v_n = k) \quad (k = 3, 4, 5, \dots)$$

exists; however, explicit expressions for p_k are not known.

5. Approximation of functions. Let ξ_n ($n = 1, 2, \dots$) be a sequence of random variables, converging in probability to a constant x . This implies that for every bounded and continuous function $f(x)$ one has³

$$(5.1) \quad \lim_{n \rightarrow +\infty} E(f(\xi_n)) = f(x).$$

³ If $\xi_n = \xi_n(x)$ converges in probability to x uniformly in x then the convergence in (5.1) is also uniform with respect to x .

The relation (5.1) is the source of a large number of theorems on the approximation of functions.

(a) Let first $n\xi_n$ have a binomial distribution of order n and parameter x ($0 < x < 1$) and let $f(x)$ be continuous in the closed interval $[0, 1]$. It follows from (5.1) that

$$(5.2) \quad \lim_{n \rightarrow +\infty} \sum_{k=0}^n f\left(\frac{k}{n}\right) \binom{n}{k} x^k (1-x)^{n-k} = f(x)$$

uniformly in x . This is Bernstein's classical probabilistic proof of the Weierstrass approximation theorem.

(b) Using instead of the binomial distribution a hypergeometric distribution, we get, putting $N_n = [n/\varepsilon] + 1$ where $0 < \varepsilon < \frac{1}{2}$,

$$(5.3) \quad \lim_{n \rightarrow +\infty} \sum_{k=0}^n f\left(\frac{k}{n}\right) \cdot \frac{\binom{N_n(\varepsilon + (1-2\varepsilon)x)}{k} \binom{N_n(1-\varepsilon - (1-2\varepsilon)x)}{n-k}}{\binom{N_n}{n}} = f(x)$$

uniformly in x ($0 \leq x \leq 1$); notice that (5.3) is also a statement about a sequence of polynomials converging to $f(x)$.

(c) If $n\xi_n$ has a Γ -distribution of order n and parameter n/t , we get from (5.1) that putting

$$(5.4) \quad g(s) = \int_0^{+\infty} e^{-sx} f(x) dx$$

we have

$$(5.5) \quad \lim_{n \rightarrow +\infty} \frac{\left(\frac{n}{t}\right)^n (-1)^{n-1} g^{(n-1)}\left(\frac{n}{t}\right)}{(n-1)!} = f(t)$$

i.e. the *Post-Widder inversion formula* for the Laplace transformation.

Another closely related inversion formula for the Laplace-Stieltjes transformation (see [36] and [37]) is obtained as follows: If

$$(5.4.b) \quad g(s) = \int_0^{+\infty} e^{-sx} dF(x)$$

where $F(x)$ is a function of bounded variation, it follows from the law of

large numbers applied to the Poisson distribution that

$$(5.5.b) \quad \lim_{\lambda \rightarrow +\infty} \sum_{0 \leq n \leq \lambda t} \frac{(-\lambda)^n g^{(n)}(\lambda)}{n!} = F(t) - F(0)$$

at every point of continuity t of $F(t)$.

Notice that it follows from (5.5.b) that if $(-1)^n g^{(n)}(\lambda) \geq 0$ for all n and for a sequence of values of λ tending to $+\infty$ then $F(t)$ is nondecreasing (compare with S. Bernstein's theorem mentioned in § 9).

(d) Let us choose for ξ_λ a random variable which has a Poisson distribution with parameter $\lambda > 0$. It follows from (5.1) that if $f(x)$ is bounded and continuous, and $t > 0$, then

$$(5.6) \quad \lim_{h \rightarrow 0} E(f(x + h\xi_{t/h})) = f(x + t)$$

uniformly in x , and thus if $F(t)$ is a distribution function on the interval $[0, +\infty)$, we have

$$(5.7) \quad \lim_{h \rightarrow 0} \int_0^{+\infty} E(f(x + h\xi_{t/h})) dF(t) = \int_0^{+\infty} f(x + t) dF(t).$$

Putting

$$(5.8) \quad g(s) = \int_0^{+\infty} e^{st} dF(t)$$

and supposing that $g(s)$ is analytic in some neighborhood of $s = 0$, we can write (5.7) in the form

$$\lim_{h \rightarrow 0} g(\Delta_h)f = g(D)f$$

where D stands for the operator of derivation, and Δ_h is the difference operator $\Delta_h f(x) = (f(x + h) - f(x))/h$. In particular, if $F(t) = 0$ for $0 \leq t \leq a$ and $F(t) = 1$ for $t > a$ in which case $g(s) = e^{as}$ we get as a particular case E. Hille's theorem

$$\lim_{h \rightarrow 0} e^{a\Delta_h} f(x) = e^{aD} f(x) = f(x + a).$$

Another interesting particular case is obtained if $F(t) = 1 - e^{-t}$ ($t \geq 0$), $g(s) = 1/(1 + s)$, which leads to

$$\lim_{h \rightarrow 0} h \sum_{k=0}^{\infty} \frac{f(x + kh)}{(1 + h)^k} = \int_0^{\infty} f(x + t) e^{-t} dt.$$

6. Entire functions. Let

$$(6.1) \quad f(z) = \sum_{n=0}^{\infty} a_n z^n$$

be an entire function, with nonnegative coefficients. Let us put

$$(6.2) \quad g(r) = \log f(e^r),$$

$$(6.3) \quad a(r) = g'(\log r)$$

and

$$(6.4) \quad b(r) = g''(\log r).$$

Let us suppose that

$$(6.5) \quad \lim_{r \rightarrow +\infty} b(r) = +\infty.$$

It has been shown by W. K. Hayman that under fairly general conditions on $f(z)$ the probability distribution $\{a_n r^n / f(r)\}$ (having mean value $a(r)$ and variance $b(r)$) can be approximated for $r \rightarrow +\infty$ by a normal distribution. It has been pointed out in [17] that for a fairly wide class of functions this follows from the central limit theorem of probability theory: for instance if $f(z)$ is a transcendental entire function of genus 0, and $f(0) = 1$, i.e., if $f(z)$ can be represented in the form

$$(6.6) \quad f(z) = \prod_{n=1}^{\infty} \left(1 - \frac{z}{z_n}\right)$$

and if all the roots z_n of $f(z)$ lie in the closed left half plane $\operatorname{Re}(z) \leq 0$ then it follows immediately from the central limit theorem that

$$(6.7) \quad \lim_{r \rightarrow +\infty} \frac{1}{f(r)} \sum_{n < a(r) + x(b(r))^{1/2}} a_n r^n = \frac{1}{(2\pi)^{1/2}} \int_{-\infty}^x e^{-u^2/2} du.$$

If one applies to the same problem the law of large numbers one is led to the beautiful probabilistic proof due to P. C. Rosenbloom of Wiman's following classical theorem: let (6.1) be an arbitrary entire function, and put

$$(6.6) \quad M(r) = \max_{|z|=r} |f(z)|$$

and

$$(6.9) \quad \mu(r) = \max_n |a_n| r^n.$$

Then for every $\varepsilon > 0$

$$(6.10) \quad M(r) < \mu(r)(\log \mu(r))^{1/2+\varepsilon}$$

for every $r > 1$ except for certain irregular values r belonging to a set E of finite logarithmic measure (i.e. such that $\int_E dr/r < +\infty$). The exponent $\frac{1}{2}$ in (6.10) is best possible for the class of all entire functions. However, recently we have proved with P. Erdős [19] (generalizing and sharpening similar previous results due to P. Lévy [20]) that if we assign random signs to the terms of the power series (6.1) then for almost all choices of these signs the exponent $\frac{1}{2}$ in (6.10) can be replaced by $\frac{1}{4}$; however, the set E of irregular values while being again (almost surely) of finite logarithmic measure, depends in general on the random choice of signs.

7. Power series with a finite radius of convergence. Let

$$(7.1) \quad f(z) = \sum_{n=0}^{+\infty} \alpha_n z^n$$

be a power series the coefficients α_n of which are independent random variables. Suppose that the power series (7.1) always has a finite radius of convergence. É. Borel [21] conjectured in 1896 that in this case the function $f(z)$ cannot be continued beyond its circle of convergence with probability 1. In the particular case when $|\alpha_n| > 0$ is a constant for each n , and the random variables $\alpha_n/|\alpha_n|$ are uniformly distributed over the unit circle, this conjecture has been verified by H. Steinhaus [22] in 1930, while for the case when $\alpha_n/|\alpha_n|$ is equal to $+1$ or -1 with probability $\frac{1}{2}$ the conjecture has been verified by Paley and Zygmund [23]. This last result leads immediately to a (probabilistic) proof of the following theorem of Hurwitz and G. Pólya [24]: given any power series with a finite positive radius of convergence, by changing the signs of certain well chosen terms, one can obtain a power series which cannot be continued beyond its circle of convergence. Borel's conjecture is not true without any further condition, as is shown by the example of the power series $\sum_{n=1}^{\infty} (1 \pm 1/2^n)z^n$. Blackwell modified Borel's conjecture in the following way: to every power series (7.1) with random coefficients α_n one can find appropriate constants b_n such that the radius of convergence of the series

$$(7.2) \quad \sum_{n=0}^{\infty} (\alpha_n - b_n)z^n$$

is not less than that of (7.1) and the series (7.2) cannot be continued with probability 1 beyond its circle of convergence. C. Ryll-Nardzewski [25] has proved that Blackwell's conjecture is in fact valid. J.-P. Kahane [26]

has shown that if the distribution of α_n is symmetric in the sense that α_n and $-\alpha_n$ have the same distribution, then Borel's conjectures are valid in the original formulation, i.e. b_n can be chosen equal to 0 in Ryll-Nardzewski's theorem; it has been later noticed by Kahane that from this special case the general theorem of Ryll-Nardzewski can be deduced (see also [17]).

As regards Kahane's result, this follows easily from Kolmogoroff's celebrated zero-one-law.

Several further results on power series with random coefficients have been recently proved by L. Arnold [27].

Similar methods can be applied to power series with several variables: Kahane has shown that in this way one obtains a surprisingly simple probabilistic proof for the important theorem of Cartan and Thullen according to which every domain of convergence is a domain of regularity.

Let us consider now a power series

$$(7.3) \quad f(z) = \sum_{n=0}^{\infty} a_n z^n$$

having the radius of convergence 1. If

$$(7.4) \quad \sum_{n=0}^{+\infty} |a_n| < +\infty$$

then the series (7.3) is uniformly convergent on the boundary of the unit circle. H. Bohr asked whether there exists a power series (7.3) which is uniformly but not absolutely convergent on the boundary of the unit circle (i.e. for which the condition (7.4) is not fulfilled). Examples of such functions have been given by L. Fejér, M. Riesz and G. H. Hardy. A. Zygmund has proved that if the series (7.3) has Hadamard gaps, i.e. $a_n = 0$ except for $n = n_k$ ($k = 1, 2, \dots$) where

$$(7.5) \quad n_{k+1}/n_k \geq q > 1, \quad k = 1, 2, \dots,$$

then the Bohr anomaly is impossible.

G. Piranian asked the following question: for which sequences $\{n_k\}$ does there exist a power series

$$(7.6) \quad \sum c_k z^{n_k}$$

which is uniformly but not absolutely convergent on the unit circle. Sequences $\{n_k\}$ for which such a series does not exist are called *Sidon sequences* (see [44]).

P. Erdős [28] has given, by a probabilistic method, sufficient conditions that such a series (7.5) should exist. He proved e.g. that it is sufficient that the condition

$$(7.7) \quad \liminf_{k \rightarrow +\infty} (n_k)^{1/k} = 1$$

should hold; he gave also the following, less restrictive condition (a simplified version of his proof is given in [17]): There exists a sequence k_j such that

$$(7.8) \quad \liminf_{j \rightarrow +\infty} (n_{k_{j+1}} - n_{k_j})^{1/j} = 1.$$

Let us now consider power series (7.6) which are regular and unbounded in the unit circle. If such a function is for every $\varepsilon > 0$ unbounded in the sector

$$|z| = re^{i\varphi}, \quad 0 \leq r < 1, \quad \vartheta - \varepsilon < \varphi < \vartheta + \varepsilon$$

we call the ray $\arg z = \vartheta$, a *singular radius* of $f(z)$ (see D. Gaier and W. Meyer-König [29]). Let us call a sequence $\{n_k\}$ an *S-sequence* if for every power series (7.6) which is regular and unbounded in the unit circle, every ray $\arg z = \vartheta$ ($0 \leq \vartheta < 2\pi$) is a singular radius. D. Gaier and W. Meyer-König [29] have proved that if the sequence $\{n_k\}$ satisfies the Hadamard gap condition (7.5) then it is an S-sequence. Let us call an S-sequence $\{n_k\}$ a *stable S-sequence* if there exists a sequence ω_k tending to $+\infty$ for $k \rightarrow +\infty$ such that every sequence n'_k such that $|n'_k - n_k| < \omega_k$ is also an S-sequence.

We have proved with P. Erdős [30] that if $\{n_k\}$ satisfies condition (7.8) then it is not a stable S-sequence. In proving this result we have used power series with fixed coefficients and *random exponents*. We have used the same method to the solution of a problem raised by A. Zygmund.

According to a famous theorem of N. Wiener, if the trigonometric series

$$(7.9) \quad \sum_{k=0}^{\infty} (a_k \cos n_k x + b_k \sin n_k x)$$

satisfies the gap condition

$$(7.10) \quad \lim_{k \rightarrow +\infty} (n_{k+1} - n_k) = +\infty$$

and it is Abel-summable on an arbitrary interval $[a, b]$ and its sum belongs to L^2 on this interval, then (7.9) is the Fourier series of an L^2 function, i.e.

$$(7.11) \quad \sum_{k=0}^{+\infty} a_k^2 + b_k^2 < +\infty.$$

Zygmund asked whether this theorem remains true for L^q with $q \neq 2$. We have shown that the answer is negative for every $q > 2$, by constructing a series of the form (7.9) satisfying the gap condition (7.10) such that (7.9) is the Fourier series of an L^2 function $f(x)$, which is bounded in every closed interval not containing any of the points $2k\pi$ ($k = 0, \pm 1, \dots$); however, the function $f(x)$ does not belong to the class L^q for any $q > 2$.

It should be emphasized that our proof is a proof of existence, which does not lead to an effective construction. P. Turán [31] and Y. Katznelson (oral communication) have constructed such functions for $q > 6$; however, a nonprobabilistic proof of our result for all $q > 2$ does not yet exist.

8. Orthogonal series. Let $\{W_n(x)\}$ denote the Walsh orthonormal system. Let $f(x)$ be a real function in the interval $[0, 1]$ belonging to the class L^2 , and let

$$(8.1) \quad f(x) \sim \sum_{n=1}^{\infty} b_n W_n(x)$$

be its Walsh-Fourier series, i.e. we put

$$(8.2) \quad b_n = \int_0^1 f(t) W_n(t) dt$$

which implies

$$(8.3) \quad \sum_{n=1}^{\infty} b_n^2 = \int_0^1 f^2(x) dx < +\infty.$$

Let us consider the partial sums

$$(8.4) \quad S_N(x) = \sum_{n=1}^N b_n W_n(x).$$

It is easy to see that if we consider x as a random variable with uniform distribution in $[0, 1]$ then the subsequence $S_{2^k-1}(x)$ ($k = 1, 2, \dots$) is a *Martingale*, and thus

$$(8.5) \quad \lim_{k \rightarrow +\infty} S_{2^k-1}(x) = f(x)$$

holds for almost all values of x .

As a special case it follows that if

$$R_n(x) = W_{2^n}(x) = \text{sign} \sin 2^{n-1} \pi x$$

denotes the n th Rademacher function and $\sum c_k^2 < +\infty$ then the series $\sum c_k R_k(x)$ is convergent almost everywhere. It has been recently noticed by L. Pál that this statement (which is, by the way, a special case of Kolmogoroff's celebrated "three series theorem") can be generalized as follows: if

$$(8.6) \quad \sum_{n=1}^{\infty} \sum_{k=0}^{n-1} c_{n,k}^2 < +\infty$$

then the series

$$(8.7) \quad \sum_{n=1}^{\infty} \sum_{k=0}^{n-1} c_{n,k} R_n(x) R_k(x)$$

is convergent almost everywhere. This theorem follows also easily from the Martingale convergence theorem and from Kolmogoroff's inequality.

It has been noticed by K. Krickeberg [32] that Haar's classical result [33] according to which the Haar-Fourier series of an L^2 -function converges almost everywhere, can also be deduced from Doob's Martingale convergence theorem.

It should be added that there is another, quite different connection between orthogonal expansions and probability theory: as pointed out by J. Lamperti [34], the Wiener process can be effectively constructed by integrating an orthogonal series. This is one of the several examples showing that often probability profits too from its connections with other areas of mathematics.

9. Absolutely monotonic sequences and functions. Let Δ denote the operator of differences applied to sequences, i.e. put $\Delta a_n = a_n - a_{n+1}$. A sequence $\{a_n\}$ ($n = 0, 1, \dots$) of positive numbers is called absolutely monotonic if $\Delta^k a_n \geq 0$ for every $n \geq 0$ and $k \geq 0$. According to Hausdorff's theorem every absolutely monotonic sequence $\{a_n\}$ with $a_0 = 1$ is the sequence of moments of the distribution function of a distribution in the closed interval $[0, 1]$, i.e. there exists a (uniquely determined) nondecreasing function $F(t)$ continuous from the left such that $F(0) = 0$ and $F(1 + 0) = 1$ such that

$$(9.1) \quad a_n = \int_0^1 t^n dF(t).$$

It has been shown in [35] that this theorem can easily be deduced from the theory of exchangeable events, because every absolutely monotonic sequence $\{a_n\}$ with $a_0 = 1$ is the sequence of de Finetti constants of some sequence of exchangeable events.

A closely related result is Bernstein's classical theorem, according to which if all derivatives of $f(x)$ exist in the interval $[0, +\infty)$, and $(-1)^n f^{(n)}(x) \geq 0$ for $n = 0, 1, \dots$ and $f(0) < +\infty$ then

$$(9.2) \quad f(x) = \int_0^{\infty} e^{-xt} dF(t)$$

where $F(t)$ is a nondecreasing function. Hausdorff has shown (see [37]) that this theorem can be deduced from his theorem. On the other hand, as pointed out in § 5, Bernstein's theorem can also be deduced from the inversion formula for the Laplace-Stieltjes transform, for which a probabilistic proof has been sketched there. Another probabilistic proof of the Hausdorff-Bernstein theorem has been given by Nawrotzki [38]. On the other hand, Bernstein's theorem is a very useful tool in the theory of point processes, for instance using this theorem it is easy to show the following theorem (see e.g. [38]): if a point process has the property that under the condition that n points of the process are lying in an interval I , these points are distributed as if they had been chosen independently and with uniform distribution in I , then the process is necessarily a mixed Poisson process.

10. Some further applications in analysis.

(A) *Summation of divergent series.* Let us consider a numerical series $\sum_{n=0}^{+\infty} a_n$, and let us put $s_n = \sum_{k=0}^n a_k$. A linear summation method is defined by taking a matrix $C = \{C_{n,k}\}$, satisfying the Toeplitz conditions:

$$\sum_{k=0}^{+\infty} |C_{n,k}| \leq A \quad (n \geq 1), \quad \lim_{n \rightarrow \infty} \sum_{k=0}^{\infty} C_{n,k} = 1$$

and $\lim_{n \rightarrow \infty} C_{n,k} = 0$ for $k = 0, 1, \dots$. Putting

$$(10.1) \quad S_n = \sum_{k=0}^{\infty} C_{n,k} s_k,$$

if the limit $\lim_{n \rightarrow \infty} S_n = S$ exists, we call the series $\sum a_k$ summable to S by the summation method corresponding to the matrix C . If $C_{n,k} \geq 0$ and $\sum_{k=0}^{\infty} C_{n,k} = 1$, S_n can be interpreted as the expectation of s_{v_n} where v_n is a random variable such that $P(v_n = k) = C_{n,k}$. It has been shown in [39] (see also [40] and [41]) that this interpretation is very useful in the theory of summation of divergent series, and leads to very simple proofs of several results on the connection of different methods of summation, e.g. the Hausdorff and Henriksson methods.

(B) *Polynomials.* Many classical polynomials admit a probabilistic interpretation, which can be used to study their properties. For instance let us consider a random walk on the line such that the point starts at the point 0 and at each step moves one unit to the right or one unit to the left with probability $\frac{1}{2}$. Let π_{2n} denote the number of times $\leq 2n$ when the point performing this random walk arrives from the right to the point 0. It can be shown (see [45]) that the characteristic function of $\pi_{2n} - n$ is

equal to $P_n(\cos t)$ where $P_n(x)$ is the n th Legendre polynomial

$$(10.2) \quad P_n(x) = \frac{1}{2^n \cdot n!} \frac{d^n}{dx^n} (x^2 - 1)^n.$$

Thus for instance from the arc sine law we get immediately the relation

$$(10.3) \quad \lim_{n \rightarrow +\infty} P_n \left(\cos \frac{t}{n} \right) = J_0(t)$$

where $J_0(t)$ is the Bessel function of order 0, i.e.

$$(10.4) \quad J_0(t) = \sum_{k=0}^{+\infty} \frac{(-1)^k}{(k!)^2} \left(\frac{t}{2} \right)^{2k}$$

As another example, let us consider a Poisson process with parameter λ and let the points of the process to the right of 0 be $\tau_1 < \tau_2 < \dots < \tau_n < \dots$. Let us consider the joint distribution function

$$(10.5) \quad G(x_1, x_2, \dots, x_n) = P(\tau_1 > x_1, \dots, \tau_n > x_n).$$

It can be shown that

$$(10.6) \quad \frac{\partial G}{\partial x_n} = \lambda^n e^{-\lambda x_n} P_n(x_1, \dots, x_n)$$

where $P_n(x_1, \dots, x_n)$ is a polynomial of degree $\leq n-1$ in each of its variables. Fixing the values of $x_1, \dots, x_{n-1}$, the polynomial of one variable $P_{n-1}(x) = P_n(y_{n-2}, \dots, y_0, x)$ of degree $n-1$ in x is the Abel-Gontcharoff polynomial defined by the conditions $p_{n-1}^{(k)}(y_k) = 0$ for $k = 0, 1, \dots, n-2$ and $p_{n-1}^{(n-1)}(x) \equiv 1$, which can be represented in the form

$$(10.7) \quad p_{n-1}(x) = \int_{y_0}^x \int_{y_1}^{z_1} \dots \int_{y_{n-2}}^{z_{n-2}} dz_1 dz_2 \dots dz_{n-1}.$$

(C) *Probabilistic proof of analytic identities.* Many analytic identities are obtained as by-products of the solution of probability problems. We mention only one example, Abel's following identity:

$$(10.8) \quad \sum_{k=0}^n \binom{n}{k} a(a+kb)^{k-1} (1-a-kb)^{n-k} = 1$$

which can be considered as a generalization of the binomial theorem, to which it reduces for $b = 0$. (10.8) can be proved (see [42]) by considering an ordered sample $\xi_1^* < \xi_2^* < \dots < \xi_n^*$ of size n from the uniform distribution in the interval $[0, 1]$ and put $\xi_0^* = 0$, $\xi_{n+1}^* = 1$. It can be shown

that if $0 < a < 1$ and $0 < b < (1 - a)/n$ and if v denotes the least integer for which $\xi_{v+1}^* > a + bv$, then

$$(10.9) \quad P(v = k) = \binom{n}{k} a(a + kb)^{k-1} (1 - a - kb)^{n-k}.$$

As v is a well-defined random variable, (10.8) follows immediately for the case $0 < b < (1 - a)/n$. As a polynomial which is constant in an interval is constant everywhere, it follows that (10.8) holds for every (complex) value of a and b .

It should be noticed that putting $a = b = x/(n + 1)$ and passing to the limit $n \rightarrow +\infty$, we obtain that the branch of the inverse function of $y = xe^{-x}$ which vanishes for $y = 0$ can be represented in the form

$$(10.10) \quad x = \sum_{n=1}^{\infty} \frac{n^{n-2} y^n}{(n-1)!},$$

the series (10.10) being convergent for $|y| \leq 1/e$ ((10.10) is usually proved by applying the Bürman-Lagrange formula, or the theory of trees).

(D) *Some further topics.* We mention here without going into details some further important areas of the application of probabilistic methods in analysis.

We have to mention in the first place potential theory, in which the theory of Markoff processes has been recently applied with great success (see e.g. [43]).

Another important area is that of the distribution of roots of polynomials. In this field Kac, Littlewood, Offord and Erdős obtained many remarkable results.

For instance Erdős and Offord (see [46]) proved that most of the 2^n polynomials $1 + \sum_{k=1}^n \varepsilon_k z^k$ where $\varepsilon_k = \pm 1$ (with the possible exception of $O(2^n/(\log \log n)^{1/2})$ such polynomials) have $\sim (2/\pi) \log n$ real roots.

In this field we mention the following conjecture of P. Erdős concerning polynomials with coefficients ± 1 : Among the 2^n polynomials $1 + \sum_{k=1}^n \varepsilon_k x^k$ where $\varepsilon_k = \pm 1$ ($k = 1, 2, \dots, n$) the majority has approximately $n/2$ roots in the interior of the unit circle. Erdős remarked that if the ε_k are independent random variables which take on the values ± 1 with probability $\frac{1}{2}$, and if v_n denotes the number of roots of the equation $1 + \sum_{k=1}^n \varepsilon_k x^k = 0$, which are lying in the unit circle, or on the half circle $x = e^{i\vartheta}$ with $0 \leq \vartheta < \pi$ then the expectation of v_n is equal to $n/2$; this follows from the fact that the number of roots of $x^n P(1/x)$ in the mentioned set is clearly $n - v_n$, and thus the expectation of v_n and of $n - v_n$ are equal. This remark certainly supports the conjecture.

There are still several other fields of applications which could be mentioned. I would like to finish by emphasizing again that the study of the applications of probability theory to other areas of mathematics is highly important for probability theory itself too, because it often leads to new interesting problems and gives stimulus to further research.

REFERENCES

1. C. Hooley, *On the difference between consecutive numbers prime to n* . III, Math. Z. **90** (1965), 355–364. MR **32** #1182.
2. A. Rényi, "On the distribution of numbers prime to n ," *Abhandlungen aus Zahlentheorie und Analysis, Zur Erinnerung an E. Landau*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1968, pp. 271–278.
3. ———, *Probabilistic methods in number theory*, Proc. Internat. Congress Math. (Edinburgh, 1958), Cambridge Univ. Press, New York, 1960, pp. 528–539. MR **22** #9478.
4. ———, *Additive and multiplicative number-theoretic functions*, Lithographic Notes, Ann Arbor, Mich., 1964.
5. J. Kubilius, *Probabilistic methods in the theory of numbers*, Uspehi Mat. Nauk **11** (1956), no. 2 (68), 31–66; English transl., Amer. Math. Soc. Transl. (2) **19** (1962), 47–85. MR **18**, 17; MR **24** #A1266.
6. H. Halberstam and K. F. Roth, *Sequences*. Vol. I, Clarendon Press, Oxford, 1966. MR **35** #1565.
7. A. Rényi, *Probabilistic methods in combinatorial mathematics*, Sympos. on Comb. Math., Chapel Hill, N.C., 1967.
8. P. Erdős and A. Rényi, *Probabilistic methods in group theory*, J. Analyse Math. **14** (1965), 127–138. MR **34** #2690.
9. R. J. Mieh, *On a conjecture of Erdős and Rényi*, Illinois J. Math. **11** (1967), 114–127. MR **34** #5918.
10. K. Bognár, *On a problem of statistical group theory*, Studia Sci. Math. Hungar. (to appear).
11. P. Erdős and P. Turán, a) *On some problems of a statistical group-theory*. I, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **4** (1965), 175–186. MR **32** #2465. b) II, Acta Math. Acad. Sci. Hungar. **18** (1967), 151–163. MR **34** #7624. c) III, Acta Math. Acad. Sci. Hungar. **18** (1967), 309–320. MR **35** #6743. d) IV, Acta Math. Acad. Sci. Hungar. **19** (1968), 413–435. MR **38** #1156.
12. W. Blaschke, *Vorlesungen über Integralgeometrie*, 3rd ed., VEB Deutscher Verlag der Wissenschaften, Berlin, 1955.
13. A. Rényi and R. Sulanke, *Über die konvexe Hülle von n zufällig gewählten Punkten*. I, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **2** (1963), 75–84. MR **27** #6190.
14. ———, *Über die konvexe Hülle von n zufällig gewählten Punkten*. II, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **3** (1964), 138–147. MR **29** #6392.
15. ———, *Zufällige konvexe Polygone in einem Ringgebiet*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **9** (1968), 146–157. MR **37** #4846.
16. W. Schmidt, *Some results in probabilistic geometry*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **9** (1968), 158–162. MR **37** #4847.
17. A. Rényi, a) *Probabilistic methods in analysis*. I, Mat. Lapok **18** (1967), 5–35. MR **37** #3606. b) II, Mat. Lapok, **18** (1967), 175–194.

18. P. C. Rosenbloom, *Probability and entire functions*, Studies in Mathematical Analysis and Related Topics, Stanford Univ. Press, Stanford, Calif., 1962, pp. 325–332. MR 26 #2609.
19. P. Erdős and A. Rényi, *On random entire functions*, Dedicated to H. Steinhaus, Zastos. Mat. (to appear).
20. P. Lévy, *Sur la croissance des fonctions entières*, Bull. Soc. Math. France 58 (1930), 29–59, 127–149.
21. E. Borel, *Sur les séries de Taylor*, C. R. Acad. Sci. Paris 123 (1896), 1051–1052.
22. H. Steinhaus, *Über die Wahrscheinlichkeit dafür, dass der Konvergenzkreis einer Potenzreihe ihre natürliche Grenze ist*, Math. Z. 31 (1930), 408–416.
23. R. E. A. C. Paley and A. Zygmund, *On some series of functions*, Proc. Cambridge Philos. Soc. 26 (1930), 337–357; *ibid.*, 28 (1932), 190–205.
24. A. Hurwitz and G. Pólya, *Zwei Beweise eines von Herrn Fatou vermuteten Satzes*, Acta Math. 40 (1915), 179–181.
25. C. Ryll-Nardzewski, *D. Blackwell's conjecture on power series with random coefficients*, Studia Math. 13 (1953), 30–36. MR 14. 994.
26. J.-P. Kahane, *Séries de Fourier aléatoires*, Université de Montréal, 1963, pp. 1–174.
27. L. Arnold, *Wachstumseigenschaften zufälliger ganzer Funktionen*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete 5 (1966), 336–347. MR 34 #6848.
28. P. Erdős, *On the uniform but not absolute convergence of power series with gaps*, Ann. Soc. Polon. Math. 25 (1952), 162–168. MR 15, 417.
29. D. Gaier and W. Meyer-König, *Singuläre Radian bei Potenzreihen*, Jber. Deutsch. Math. Verein. 60 (1957), 89–92.
30. P. Erdős and A. Rényi, *On a problem of A. Zygmund*, Studies in Math. Analysis and Related Topics, Stanford Univ. Press, Stanford, Calif., 1962, pp. 110–116. MR 26 #2586.
31. P. Turán, *On a certain problem in the theory of power series with gaps*, Studies in Math. Analysis and Related Topics, Stanford Univ. Press, Stanford, Calif., 1962, pp. 404–409, MR 26 #2587.
32. K. Krickeberg, *Wahrscheinlichkeitstheorie*, Teubner Verlagsgesellschaft, Stuttgart, 1963. MR 27 #3004.
33. A. Haar, *Gesammelte Arbeiten*, Verlag Akad. der Wissenschaften, Budapest, 1959. MR 21 #4884.
34. J. Lamperti, *Probability*, Benjamin, New York, 1966.
35. A. Rényi and P. Révész, *A study of sequences of equivalent events as special stable sequences*, Publ. Math. Debrecen 10 (1963), 319–325. MR 30 #1543.
36. W. Feller, *An introduction to probability theory and its applications*. Vol. II, Wiley, New York, 1966. MR 35 #1048.
37. D. V. Widder, *The Laplace transform*, Princeton Math. Series, vol. 6, Princeton Univ. Press, Princeton, N. J., 1941. MR 3, 232.
38. K. Nawrotzki, *Ein Grenzwertsatz für homogene zufällige Punktfolgen (Verallgemeinerung eines Satzes von A. Rényi)*, Math. Nachr. 24 (1962), 201–217. MR 27 #4272.
39. A. Rényi, *Summation methods and probability theory*, Magyar Tud. Akad. Mat. Kutató Int. Közl. 4 (1959), 389–399. MR 24 #A561.
40. L. Schmetterer, *Wahrscheinlichkeitstheoretische Bemerkungen zur Theorie der Reihen*, Arch. Math. 14 (1963), 311–316. MR 27 #3971.
41. P. Szűsz, *On a theorem of Buck and Pollard*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete 11 (1968), 39–40.

42. A. Rényi, *On some problems in the theory of order statistics. I*, Bull. Inst. Internat. Statist. **42** (1967), 165–176.

43. Paul A. Meyer, *Probability and potentials*, Blaisdell, Waltham, Mass., 1966. MR **34** # 5119.

44. P. Erdős, *On some applications of probability methods to function theory and on some extremal properties of polynomials*, Proc. Internat. Conf. Contemporary Problems in Theory Anal. Functions. (Erevan, 1965) "Nauka," Moscow, 1966, pp. 359–362. MR **34** #6034.

45. A. Rényi, *Legendre polynomials and probability theory*, Ann. Univ. Sci. Budapest Eötvös Sect. Math. **3/4** (1960/61), 247–251. MR **24** #A2978.

46. P. Erdős and C. Offord, *On the number of real roots of a random algebraic equation*, Proc. London Math. Soc. (3) **6** (1956), 139–160. MR **17**, 500.

THE STOCHASTIC GEYSER (SUMMARY OF A LECTURE)

A. RÉNYI

Let $\xi_1, \xi_2, \dots$ be independent, identically distributed bounded and positive random variables and let $\xi_n = \xi_1 + \xi_2 + \dots + \xi_n$, $\xi_n^* = [\xi_n]$, where $[x]$ denotes the integer part of the positive number x . The problem is to determine (with probability 1) the distribution function $F(x)$ or some characteristics of ξ_n through the statistical properties of ξ_n^* ($n = 1, 2, \dots$). If M denotes the expectation of ξ_n , then the relation

$$\lim_{n \rightarrow \infty} \frac{\xi_n^*}{n} = M$$

follows directly from the strong law of large numbers, i.e. M is determined by the sequence ξ_n^* ($n = 1, 2, \dots$) with probability 1. Write D^2 for the variance of ξ_n , then D can be determined with probability 1 by the law of iterated logarithm:

$$\lim_{n \rightarrow \infty} \frac{\xi_n^* - nM}{\sqrt{2n \log \log n}} = D.$$

The determination of higher moments is an open problem.

NOTE

The story of the geyser problem goes back far into the history of Hungarian mathematics. A lemma of Gy. König [5], which had been published almost a hundred years ago, was reformulated by J. Kürschák [6] in 1913. This inspired A. Rényi to create the stochastic version of the geyser problem in which the process ξ_n is represented by the eruptions of a geyser and for lack of any watch a shipwrecked man is able to observe only the days of the eruptions.

The problem was solved by P. Bártfai [1] in 1966. He gave a generalization of the problem: let $\zeta_n^* = \xi_1 + \xi_2 + \dots + \xi_n + r_n$ where r_n ($n = 1, 2, \dots$) is an arbitrary sequence of bounded random variables such that $|r_n| \leq R_n$ and $R_n = o(\log n)$ (nothing is supposed on the dependence between the processes ζ_n and r_n). In [1] he proved that $F(x)$ is uniquely determined with prob-

ability 1 by the observations ζ_n^* ($n = 1, 2, \dots$) provided $\mathbf{M}(e^{t\zeta_1}) < \infty$ for some $t > 0$, further he estimated the moments. In No. 342 Rényi gave another proof of Bártfai's theorem, but here the boundedness is replaced by $r_n = o(\log n)$ with probability 1.

Bárfai [2] proved that under the condition $r_n = o(n^{1/4+\delta})$ no other characteristics of ξ_1 than the first two moments are determined. This also follows from Strassen's earlier result [7]. In spite of the large distance between the $O(\log n)$ and $o(n^{1/4+\delta})$, Bárfai conjectured that the order of magnitude $O(\log n)$ in Bárfai's theorem cannot be increased. The first step in this direction was done by Csörgő and Révész [3], who proved on applying Bárfai's construction that no characteristics of ξ_1 are determined except for the first k moments if $r_n = o\left(\frac{1}{2k} + \delta\right)$. Finally, J. Komlós, P. Major and G. Tusnády [4] succeeded in proving completely Bárfai's conjecture. [P. B.]

REFERENCES

- [1] Bárfai, P.: Die Bestimmung der zu einem wiederkehrenden Prozess gehörenden Verteilungsfunktion aus den mit Fehlern behafteten Daten einer einzigen Realisation. *Studia Sci. Math. Hung.*, **1** (1966), 161–168.
- [2] Bárfai, P.: Über die Entfernung der Irrfahrtswege, *Studia Sci. Math. Hung.*, **5** (1970), 41–49.
- [3] Csörgő, M. and Révész, P.: A new method to prove laws of iterated logarithm of Strassen's type I – II. *Z. für Wahrscheinlichkeitstheorie* **31** (1975), 255–260, 261–270.
- [4] Komlós, J., Major, P. and Tusnády, G.: An approximation of partial sums of independent RV's, and the sample DF. I–II. *Zeitschrift für Wahrscheinlichkeitstheorie*. **32** (1975), 111–132, **34** (1976), 33–59.
- [5] König, Gy.: On a general solution of the algebraic equations. (In Hungarian.) *Műegyetemi Lapok*, **1** (1876), 20–28, 112–116.
- [6] Kürschák, J.: König Gyula. Memorial speech (in Hungarian). *A Magyar Mérnök-és Építész-Egylet Közlönye*, **15** (1914).
- [7] Strassen, W.: Almost sure behavior of sums of independent random variables and martingales. *Proc. 5th Berkeley Sympos. Math. Statist. Probab.*, (1965), **II**, (1), 315–343; Berkeley: University of California Press 1967.