Кибернетический сборник

НОВАЯ СЕРИЯ

ВЫПУСК

24

Сборник статей

Перевод с английского

ПОД РЕДАКЦИЕЙ
О. Б. ЛУПАНОВА

МОСКВА «МИР» 1987

ББК 32.81
К 38
УДК 519.95

К 38 **Кибернетический** сборник. Новая серия Вып. 24 Сб. статей: Пер. с англ. — М.: Мир, 1987. — 232 с., ил.

Продолжение серии, начатой издательством «Мир» в 1965 г. В данном выпуске большой интерес представляет обзор Д. Ли и Ф. Препараты (США) основных результатов по вычислительной геометрии. Специалистов по комбинаторике, теории кодирования, дискретного анализа, алгебры и др. заинтересует цикл статей по сильно регулярным графам и частичным геометриям, написанных К. Юбо (Бельгия), А. Браувером и Й. ван Линтом (США). Включены также небольшие статьи Л. Вэльянта, Х. Коэна и Х. Леистры (США) по теории сложности и теории графов.

Для научных работников, инженеров-исследователей, аспирантов и студентов, занимающихся и интересующихся теоретической кибернетикой и ее приложениями.

К $\frac{1702070000-463}{041(01)-87}$ 4-87, ч. 1 ББК 32.81

Редакция литературы по математическим наукам

Вычислительная геометрия. Обзор [1]

Д. Ли [2], *Ф. Препарата* [3]

Дается обзор исследований в области вычислительной геометрии — дисциплины, предметом исследований которой является сложность решения геометрических задач в рамках теории анализа алгоритмов. Эта недавно возникшая область исследований уже нашла многочисленные приложения в различных других областях, таких, как машинное проектирование, машинная графика, исследование операций, распознавание образов, робототехника и статистика. Обсуждаются пять главных направлений исследований: выпуклые оболочки, пересечения, поиск, близость и комбинаторная оптимизация. На примерах демонстрируются семь методов разработки алгоритмов: итерационное конструирование, заметание плоскости, геометрическое место точек, «разделяй и властвуй», геометрическое преобразование, поиск с отсечением и динамизация. Также включен набор преобразований задач, позволяющих получать нижние оценки сложности решения геометрических задач в рамках модели построения/проверки.

Ключевые слова и фразы. Алгебраическое дерево вычислений, анализ алгоритмов, комбинаторная оптимизация, вычислительная сложность, вычислительная геометрия, выпуклая оболочка, метод «разделяй и властвуй», метод динамизации, метод геометрического преобразования, метод заметания плоскости, близость.

1. ВВЕДЕНИЕ

Вычислительная геометрия, как она представляется сегодня занимается исследованием вычислительной сложности решения геометрических задач в рамках теории анализа алгоритмов. Однако словосочетание «вычислительная геометрия» использовалось, по крайней мере дважды, в смысле, отличном от указанного выше. В работах [47, 146, 299] изучались вопросы мо-

---

[1]) Lee D. T., Preparata Franco P. Computational geometry — A survey. — IEEE Transactions on Computers, 1984, v. C-33, No. 12, p. 1072—1101.

[2]) Senior member, IEEE, Department of Electrical Engineering and Computer Science, Northwestern University, Evanston.

[3]) Fellow, IEEE, Coordinated Science Laboratory, University of Illinois, Urbana.

делирования геометрических объектов (кривых и поверхностей) с помощью сплайнов. По своему содержанию эта область исследований, названная Форрестом «Вычислительная геометрия», ближе к численным методам, чем к геометрии. Минский и Пейперт [264] в своей книге, озаглавленной «Персептроны», рассматривают сложность предикатов, распознающих некоторые геометрические свойства, такие, как выпуклость[1]). Цель их работы состоит в определении возможности больших ячеистых структур, составленных из простых цепей, для решения задач распознавания образов.

Мы сосредоточим внимание на вычислительной геометрии в современном понимании этого термина, которая в наши дни стала самостоятельной дисциплиной в области анализа и разработки алгоритмов. Большой ряд прикладных областей, таких, как распознавание образов [328], машинная графика [268], обработка изображений [286], исследование операций, статистика [41, 314], машинное проектирование, робототехника и т. д., явились благодатной средой, в которой сформировалась эта дисциплина, по мере того как в них появлялись геометрические по сути задачи, требовавшие для решения разработки эффективных алгоритмов. К числу таких задач относятся евклидова задача о коммивояжере, задача о минимальном остовном дереве, задача линейного программирования и множество других. Алгоритмические исследования этих и других задач появлялись в научной литературе на протяжении двух последних десятилетий с нарастающей интенсивностью. К этой области исследований, названной в статье Шамоса [313], появившейся в 1975 г., «Вычислительная геометрия», было привлечено внимание постоянно возрастающего числа специалистов. Учитывая, что результаты, полученные в этой области исследований, разбросаны по литературе, представляется своевременным и необходимым дать их достаточно подробный обзор. Библиография, представленная в работе Эделсбруннера и ван Леувена [139], довольно хорошо отражает работы, относящиеся к данной области исследований и появившиеся до лета 1982 г. Более полное и подробное изложение вычислительной геометрии должно появиться в ближайшем будущем в виде книги [295].

В соответствии с природой рассматриваемых геометрических объектов можно выделить пять основных категорий, на основании которых может быть удобным образом классифицирована вся совокупность геометрических задач. А именно: выпуклость, пересечение, геометрический поиск, близость и оптимизация. В то же время для методов решения задач на сегодняшний

---

[1]) В издании на английском языке книга имеет подзаголовок «Введение в вычислительную геометрию». — *Прим. перев.*

день можно определить семь главных парадигм: итерационное конструирование, заметание плоскости, геометрическое место точек, разделяй и властвуй, геометрические преобразования, поиск с отсечением и динамизация. Мы в общих чертах продемонстрируем на примерах каждую из этих парадигм. Но, прежде чем перейти к обсуждению, следует подробно рассмотреть используемую модель вычислений и меры сложности алгоритмов.

Модели вычислений. В качестве модели вычислений обычно используется машина с произвольным доступом к памяти (РАМ), аналогичная описанной в (1) с добавлением возможности выполнения арифметических операций над действительными числами. Это значит, что в такой машине каждая ячейка памяти может содержать действительное число, а каждая арифметическая операция, такая, как сложение, умножение и деление, может быть выполнена за единицу времени. В зависимости от решаемой задачи машина имеет некоторые другие примитивные операции, подобные вычислению пересечения двух отрезков прямых или вычислению расстояния между двумя точками. При этом предполагается, что все эти примитивные операции выполняются за постоянное время.

В общем случае геометрические задачи можно отнести к одному из двух типов, условно называемых задачами «на построение» (конструирование) и «на проверку» (распознавание). В *задаче на построение* требуется построить некоторый геометрический объект, удовлетворяющий заданному свойству, в то время как в *задаче на проверку* необходимо проверить, удовлетворяет или нет геометрический объект заданному свойству. Почти в каждом конкретном случае задача на построение может быть преобразована в соответствующую конкретную задачу на проверку, а нижняя оценка сложности для задачи на проверку может быть использована для установления нижней оценки сложности для задачи на построение. (См. разд. III-F, где более подробно обсуждаются преобразования задач и нижние оценки сложности.) Таким образом, мы можем ограничить наше обсуждение соответствующей вычислительной моделью для задач на проверку, другими словами, так называемым алгебраическим деревом решений (проверки) [26, 108, 296, 298]. В этой статье, если не оговорено иное, мы будем использовать эту модель для установления нижней оценки времени вычислений задач на проверку и соответствующих им задач на построение.

Алгебраическое дерево вычислений [26] на множестве переменных $V = \{x_1, x_2, \ldots, x_n\}$, где $x_i \in \mathbf{R}$, — бинарное дерево T, размеченное следующим образом.

1. Каждой вершине v, имеющей в точности одного сына (простая вершина), приписывается операция вида $f_v := f_{v_1} \# f_{v_2}$, или $f_v := c \# f_{v_1}$, или $f_v := \sqrt{f_{v_1}}$, где v_i $(i = 1, 2)$ — предок вершины v в дереве T, или $f_{v_i} \in V$, $\# \in \{+, -, \times, /\}$, а $c \in \mathbf{R}$ является константой.

2. Каждой вершине v, имеющей двух сыновей (вершина ветвления), приписывается операция сравнения вида $f_{v_1} > 0$, или $f_{v_1} < 0$, или $f_{v_1} = 0$, где v_1 — предок вершины v в дереве T, или $f_{v_1} \in V$.

3. Каждому листу дерева приписывается одно из значений ДА или НЕТ.

Пусть $W \subseteq \mathbf{R}^n$ — произвольное множество. *Задача о принадлежности* (являющаяся задачей на проверку) для множества W заключается в определении того, принадлежит или нет множеству W точка $x = (x_1, x_2, \ldots, x_n) \in \mathbf{R}^n$. Для каждой заданной точки x программа прокладывает в дереве T путь $P(x)$, начинающийся в корне дерева. При прохождении каждой простой вершины выполняется арифметическая операция, приписанная этой вершине, а в каждой вершине ветвления происходит ветвление в соответствии с результатом сравнения, приписанного вершине. При достижении листа дерева возвращается ответ ДА или НЕТ. Предполагается, что всякий раз, когда встречается вершина v, а приписанная ей операция является делением, то делитель отличен от нуля, и что в случае операции извлечения квадратного корня операнд неотрицателен. Считается, что дерево вычислений T *решает* задачу о принадлежности, если возвращаемый ответ является верным для каждой исходной точки $x \in \mathbf{R}^n$. Сложность дерева T, обозначаемая через $C(T)$, определяется как максимум величины $\mathrm{cost}(x, T)$ по всем значениям x, где $\mathrm{cost}(x, T)$ — число вершин, проходимых путем $P(x)$ в дереве T. Сложность задачи на проверку принадлежности точки множеству W, обозначаемая через $C(W)$, есть минимум $C(T)$ по всем алгебраическим деревьям вычислений T, решающих задачу о принадлежности.

Разновидностью алгебраического дерева вычислений является так называемое (алгебраическое) дерево решений порядка d [324] для определения справедливости отношения принадлежности $x \in W \subseteq \mathbf{R}^n$. Дерево решений порядка d — это дерево, каждой вершине которого соответствует сравнение вида $f(x) ? 0$, где f имеет полиномиальную сложность относительно входных данных с показателем степени не более d и $? \in \{<, >, =\}$. В случае когда d равно 1, получается *линейное дерево решений*, с использованием которого получены доказа-

тельства ряда нижних оценок сложности [99, 107, 108, 298, 349, 352].

Временна́я и емкостная сложности. Время и объем памяти, используемые алгоритмом, являются двумя главными мерами эффективности конкретного алгоритма. Обычно мы подсчитываем лишь число ключевых операций, например сравнений, выполняемых алгоритмом, и представляем его в виде функции от размера входных данных. Поступая таким образом, мы должны гарантировать, чтобы число неучитываемых при подсчете операций было пропорционально числу ключевых операций, так что время выполнения алгоритма отличалось бы от полученной при таком подсчете оценки лишь постоянным множителем. Что касается объема памяти, требуемого при выполнении алгоритма, то мы подсчитываем максимальный объем памяти, который может потребоваться в какой-либо момент выполнения алгоритма. Эта величина также представляется в виде функции от размера входных данных. Ниже приводится стандартная форма обозначений, предложенная Кнутом [204].

$O(f(n))$ — множество всех функций $g(n)$, таких, что существуют положительные константы C и n_0 и при этом $|g(n)| \leqslant Cf(n)$ для всех $n \geqslant n_0$.

$\Omega(f(n))$ — множество всех функций $g(n)$, таких, что существуют положительные константы C и n_0 и при этом $g(n) \geqslant Cf(n)$ для всех $n \geqslant n_0$.

$\theta(f(n))$ — множество всех функций $g(n)$, таких, что существуют положительные константы C, C' и n_0 и при этом $Cf(n) \leqslant g(n) \leqslant C'f(n)$ для всех $n \geqslant n_0$.

$o(f(n))$ — множество всех функций $g(n)$, таких, что *для всех положительных констант* C существует такое n_0 и для всех $n \geqslant n_0$ имеет место $g(n) \leqslant Cf(n)$.

Анализ сложности алгоритма может быть двух типов: анализ в худшем случае и анализ в среднем случае. При анализе худшего случая мы ищем максимальное количество времени (памяти), необходимого алгоритму по всем возможным входным данным. При анализе среднего случая мы обычно предполагаем, что входные данные распределены в соответствии с некоторой функцией распределения вероятностей, и изучаем поведение алгоритма для каждого набора входных данных, взятого из распределения. Обычно мы интересуемся асимптотическим поведением алгоритма (асимптотический анализ), т. е. поведением алгоритма, когда размер входных данных приближается к бесконечности. Так как анализ сложности алгоритма в среднем случае обычно очень труден и, кроме того, предположение о распределении вероятностей входных данных иногда трудно проверить, то в данной работе основное внимание будет

сосредоточено на анализе сложности алгоритмов в худшем случае. Мы будем рассматривать анализ сложности алгоритмов только в худшем случае, если не оговорено что-либо иное.

11. МЕТОДЫ РЕШЕНИЯ ЗАДАЧ

Теперь мы дадим примеры для каждого из семи основных методов решения задач, упоминавшихся выше.

А. Построение последовательным добавлением элементов

Это простейший и наиболее интуитивный метод решения задач, известный также как *итеративный жадный метод*. Основная идея состоит в том, что мы конструируем или вычисляем

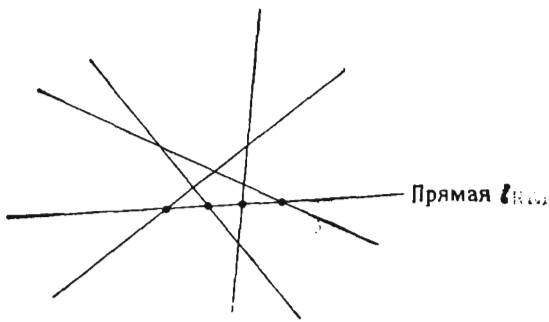


Рис. 1. Определение расположения прямой.

решение методом итераций. Аналогом этого метода является хорошо известный метод сортировки вставками [203], в котором упорядоченный список получается путем вставки элементов один за одним в частично упорядоченный список. Далее приведены конкретные примеры.

Рассмотрим задачу вычисления расположения прямых на плоскости. Пусть задано множество H из n прямых на плоскости. Необходимо вычислить (построить) разбиение плоскости, порождаемое множеством H. Очевидный метод решения состоит в конструировании разбиения путем последовательной обработки один за одним элементов множества и построения искомого разбиения итерационным способом [86, 133]. Так в случае, показанном на рис. 1, когда добавляется прямая i, необходимо просмотреть все области, которые рассекает эта прямая, при этом строится новое разбиение. Как оказывается, такой подход требует времени $O(n^2)$ и является асимптотически оптимальным в том смысле, что полное время построения решения пропор-

ционально объему памяти, необходимой для представления разбиения. Более того, этот подход обобщается на случай пространств более высокой размерности [133]. Так как этот метод является довольно самоочевидным, то мы опускаем описание алгоритма и формулируем результат в виде теоремы.

Теорема 1. *Задача вычисления расположения n прямых на плоскости может быть решена за время $O(n^2)$ методом последовательного добавления элементов.*

В качестве другого примера задачи, для которой с успехом может быть применен метод последовательного конструирования, который, как может быть показано, является оптимальным, рассмотрим задачу построения выпуклой оболочки множества точек на плоскости (см. разд. II-D). Мы просто последовательно просматриваем точки и сразу же строим выпуклую оболочку для просмотренных точек. Если очередная точка лежит внутри уже построенной выпуклой оболочки, то ничего делать не надо, и эта точка просто игнорируется. В противном случае она является граничной точкой выпуклой оболочки и текущая выпуклая оболочка должна быть изменена, для чего необходимо определить две опорные прямые, проходящие через эту новую точку. Оптимальная реализация этого подхода содержится в работах [21, 221, 291]. Хотя два приведенных примера показывают, что метод построения решения последовательным добавлением элементов позволяет получать оптимальные решения, как правило, это не имеет места для большинства задач, рассмотренных в литературе.

B. Заметание плоскости

Как следует из названия, предлагаемая схема прежде всего применима к задачам в случае двумерного пространства. Тем не менее ее обобщение на случай пространств большей размерности довольно очевидно и может быть найдено, например, в [50]. Этот метод известен в машинной графике также под названием *метода линейного сканирования* [268] и используется в различных приложениях, таких, как, в частности, затенение, заполнение многоугольных областей [58, 215, 286]. Для наглядности мы опишем схему этого метода в связи с ее применением к конкретному примеру и укажем основные её особенности.

Рассмотрим задачу обнаружения всех пересекающихся пар среди множества горизонтальных и вертикальных отрезков прямых. Пусть S — множество отрезков, $S=\{s_1, s_2, \ldots, s_n\}$, так что s_i — либо горизонтальный, либо вертикальный отрезок. Если s_i — горизонтальный отрезок, то он задается как $(x_{i1}, x_{i2}; y_i)$,

а если s_i — вертикальный отрезок, то он задается как $(x_i; y_{i1}, y_{i2})$, где x и y — координаты концов каждого отрезка. (Для простоты считается, что никакая пара отрезков не коллинеарна.) Предположим, что мы «заметаем» плоскость вертикальной прямой, двигая ее слева направо (или горизонтальной прямой сверху вниз) и сообщаем о наличии пары пересекающихся отрезков, как только точка их пересечения оказывается на заметающей прямой. Очевидно, что в интервале x-координат между конечными точками отрезков никаких новых пересекающихся пар отрезков не будет обнаружено. Другими словами, x-координаты отрезков определяют совокупность положений, в которых возможно пересечение отрезков, и они называются «критическими точками» [269, 295].

Заметим также, что заметающая прямая с абсциссой x разбивает множество отрезков на три подмножества S_1, S_2 и S_3, где S_1 — множество отрезков, лежащих целиком слева от заметающей прямой, S_2 — множество отрезков, пересекающих заметающую прямую, и S_3 — множество отрезков, лежащих целиком справа от заметающей линии. Множество отрезков S_1 не будет играть никакой роли в «будущем» при движении заметающей прямой слева направо, т. е. для заметающих прямых с абсциссой $x' > x$; множество S_2 содержит «активные» отрезки, которые могут войти в ответ, т. е. могут в дальнейшем пересечь отрезки из множества S_3; S_3 — множество отрезков, не играющих никакой роли в текущий момент времени. Суть этого метода состоит в поддержании «адекватной» информации о множестве активных отрезков в каждой критической точке. Как только некоторый отрезок становится активным, он добавляется как составной элемент к этой адекватной информации, а когда заметающая прямая проходит отрезок, он удаляется.

В нашем примере адекватная информация — это последовательность ординат всех активных отрезков, представленная в виде сбалансированного по высоте дерева [1]. Если следующая критическая точка соответствует вертикальному отрезку, то этот отрезок используется для просмотра текущего состояния структуры данных, и все горизонтальные отрезки, y-координаты которых лежат в интервале, определяемом вертикальным отрезком, регистрируются как пересекающиеся с этим отрезком. Если следующая критическая точка соответствует левому концу горизонтального отрезка, то этот отрезок становится активным и вставляется в дерево; в противном случае эта критическая точка является правым концом горизонтального отрезка, который ввиду этого должен быть удален из дерева. Корректность этого алгоритма может быть легко установлена. С точки зрения выполнения алгоритма полное время его работы равно $O(n \log n + k)$, где k — число обнаруженных пересечений, так

как в каждой критической точке необходимо выполнить либо операцию вставки элемента в дерево, либо операцию исключения элемента из дерева, каждая из которых требует времени $O(\log n)$, либо сообщить об обнаруженном пересечении. Имеет место следующая теорема.

Теорема 2. *Задача обнаружения всех k пар пересекающихся отрезков в множестве из n горизонтальных и вертикальных отрезков может быть решена за время $O(n \log n + k)$ методом заметания плоскости.*

В заключение отметим, что имеются две основные структуры данных, связанные с методом заметания плоскости, а именно: (i) *список критических точек*, представляющий последовательность абсцисс, упорядоченных в порядке прохождения слева направо, и (ii) *статус заметающей прямой*, представляющий соответствующее описание необходимой информации относительно геометрических объектов, находящихся на заметающей прямой. Заметим, что эти структуры данных в различных ситуациях могут быть разными, а список критических точек может динамически изменяться в процессе выполнения алгоритма. Так, в рассмотренном выше примере список критических точек является фиксированным упорядоченным списком, а статус заметающей прямой реализован как сбалансированное по высоте дерево. Случаи использования метода заметания плоскости, в которых список критических точек динамически изменяется, обсуждаются в работах [38, 63, 229, 269]; в этом случае обычно используется одна из форм очереди с приоритетами [1].

C. Геометрическое место точек

Этот метод связан, главным образом, с задачами геометрического поиска в так называемом режиме с повторением (произвольно длинная последовательность запросов к фиксированному файлу), когда необходимо эффективно обрабатывать однотипные запросы [278]. Например, мы хотим сделать предобработку некоторого множества точек на плоскости с тем, чтобы ответ на запрос, известный как *запрос на интервальный поиск*, используемый для обнаружения точек множества S, лежащих внутри некоторого прямоугольного окна, мог быть получен как можно быстрее. Используя этот метод, нам хотелось бы разбить пространство запросов на «клетки» таким образом, чтобы все точки из данной клетки порождали бы один и тот же ответ на запрос. Более формально, мы разбиваем пространство на ряд классов «эквивалентности» на основе отношения, зависящего непосредственно от задачи. Рассмотрим, например, *двумерную задачу о доминировании*, которая приводится ниже.

Двумерная задача о доминировании. На плоскости задано множество S из n точек $p_1, p_2, \ldots, p_n$. Допускается предобработка. Необходимо найти число точек множества S, над которыми доминирует заданная точка q. (Считается, что точка q *доминирует* над точкой p, если как x-координата, так и y-координата точки p не превосходят соответствующих координат точки q.)

Мы покажем, как метод геометрического места точек позволяет отвечать на запросы за время $\theta(\log n)$, что является оптимальным. Сначала определим отношение T в $\mathbf{R}^2$ таким образом, что для пары точек (p, q) в $\mathbf{R}^2$ имеет место отношение T, если подмножества множества S, над которыми доминируют точки p и q соответственно, совпадают. Отношение T, являясь отношением эквивалентности, порождает разбиение плоскости в общем случае на $(n+1)^2$ классов эквивалентности. Геометрически это можно представить так. Если мы проведем вертикальные и горизонтальные прямые через каждую точку множества S, то n этих вертикальных и горизонтальных линий разделят плоскость на $(n+1)^2$ клеток. Каждая такая клетка представляет класс эквивалентности, так как для любых двух точек в клетке подмножества множества S, над которыми доминируют эти две точки, идентичны. Таким образом, наша задача становится по сути *задачей определения положения точки*, т. е. определения того, какой из клеток принадлежит точка из запроса, и та клетка, в которую попадает точка из запроса, и будет содержать решение исходной задачи (некоторое целое число). Так как двукратное применение процедуры двоичного поиска позволяет определить, какой из $O(n^2)$ клеток, определенных ранее, принадлежит точка из запроса, то мы имеем следующую теорему.

Теорема 3. *Двумерная задача о доминировании может быть решена за время $O(\log n)$ методом геометрического места точек с использованием предобработки, требующей $\theta(n^2)$ затрат по времени и по памяти.*

К числу других задач, к которым применим метод геометрического места точек, относятся задачи поиска ближайшего соседа [147, 157, 354], задача нахождения наикратчайшего пути при наличии препятствий [229, 327] и т. д.

D. «Разделяй и властвуй»

Это классический метод решения задач, оказавшийся также ценным и для геометрических задач [30, 40, 42, 83, 172, 174, 198, 205, 220, 228, 293, 315]. Применение этого метода обычно заключается в разбиении исходной задачи на несколько подзадач, рекурсивном решении каждой подзадачи и последующем

объединении полученных решений подзадач с целью получения решения исходной задачи. Хорошо известным примером применения этого метода является задача построения *выпуклой оболочки*. А именно, пусть задано множество S из n точек на плоскости. Необходимо построить выпуклую оболочку множества точек S (наименьшее выпуклое множество, содержащее S). Ниже приведен алгоритм вычисления выпуклой оболочки множества S методом «разделяй и властвуй». Здесь предполагается, что исходные данные представлены совокупностью точек, заданных своими координатами, а результатом работы алгоритма является последовательность точек, принадлежащих выпуклой оболочке. Заметим, что выпуклая оболочка множества точек на плоскости является выпуклым многоугольником. Поэтому результатом работы алгоритма является последовательность вершин этого выпуклого многоугольника, перечисляемых, например, в порядке обхода по часовой стрелке.

Алгоритм Выпуклая оболочка (S)
If $|S| \leqslant 2$ **then return** (S)
else begin
разбить S на S_1 и S_2 таким образом, что
$|S_1| = \lfloor 1/2 \rfloor |S|$ и $S_1 \cup S_2 = S$;
$S' :=$ ВЫПУКЛАЯ ОБОЛОЧКА (S_1);
$S'' :=$ ВЫПУКЛАЯ ОБОЛОЧКА (S_2);
$T :=$ ОБЪЕДИНИТЬ (S', S'');
return (T)
end

Здесь ОБЪЕДИНИТЬ (S', S'') реализует шаг «властвуй». Это процедура, которая соединяет две выпуклые оболочки в одну, т. е. вычисляет выпуклую оболочку их объединения. В работах [293, 313, 316] было показано, что это объединение может быть найдено за время $O(|S'|+|S''|)$ (см. задачу 3.1.2 в разд. III). Анализ алгоритма «разделяй и властвуй» относительно прост. Обозначим через $L(T)$ время, требуемое для выполнения алгоритма *Выпуклая оболочка*, где $n = |S|$. Предположим далее, что n — степень числа 2. Тогда имеем следующее рекуррентное соотношение:

$$T(1) = \text{const},$$
$$T(n) = 2T(n/2) + M(n/2,\ n/2),$$

где $M(s, t)$ — время, необходимое для вычисления выпуклой оболочки объединения двух выпуклых многоугольников с s и t вершинами соответственно. Так как $M(n/2, n/2) = O(n)$, то $T(n) = O(n \log n)$. Таким образом, имеет место следующая теорема.

Теорема 4. *Задача нахождения выпуклой оболочки множества из n точек на плоскости может быть решена методом «разделяй и властвуй» за время $O(n \log n)$.*

Е. Геометрические преобразования

Применение подходящих преобразований к геометрическим объектам часто может быть вызвано стремленнем преобразовать исходную задачу к некоторой эквивалентной ей задаче. В одних случаях точки d-мерного пространства отображаются в точки этого же пространства, в других случаях преобразование отображает k-мерные многообразия в $(d-1-k)$-мерные многообразия. Имеется важный класс преобразованнй последнего типа, известных под названием *полярное* или *двойственное* преобразования, которые в последнее время с большим успехом были использованы в ряде приложений. Главная причина этого успеха состоит в том, что преобразованная задача более непосредственно воздействует на интуицию и, следовательно, в большей степени способствует созданию эффективного алгоритма.

Приведем конкретный пример, иллюстрирующий это положение. Рассмотрим задачу о пересечении n полуплоскостей (на плоскости). А именно, пусть даны n полуплоскостей, каждая из которых определяется линейным неравенством вида $y \leqslant a_i x + b_i$ или $y \geqslant a_i x + b_i$. Необходимо найти их пересечение. Так как пересечение является выпуклым многоугольником, который может быть, а может и не быть ограниченным, эта задача может быть решена методом «разделяй и властвуй», при этом шаг объединения решений подзадач заключается в нахождении пересечения двух выпуклых многоугольников. Так как пересечение двух выпуклых многоугольников может быть выполнено за линейное время, то время выполнения алгоритма «разделяй и властвуй» равно $O(n \log n)$ [313, 317]. Однако для решения этой задачи мы воспользуемся методом геометрического преобразования, имеющим ту же оценку сложности, которая является оптимальной [315] с точностью до постоянного множителя в рамках модели вычислений, допускающей аналитические функции от входных параметров [155] или в рамках модели алгебраических деревьев вычислений Бен-Ора [26].

Прежде всего будем считать, что ни одна из заданных прямых, определяющих полуплоскости, не является вертикальной. (Это всегда может быть достигнуто в результате поворота системы координат.) Будем называть полуплоскость *нижней полуплоскостью*, если ограничивающая ее прямая расположена над открытой полуплоскостью. В противном случае полуплоскость называется *верхней полуплоскостью*. Таким образом, нижняя полуплоскость определяется неравенством вида $y \leqslant$

$\leqslant a_i x + b_i$, а верхняя полуплоскость — неравенством вида $y \geqslant a_i x + b_i$.

Используемое нами геометрическое преобразование отображает точки в прямые линии и известно под названием *полярность*. Полярность в случае плоскости (и с очевидным обобщением в случае пространств произвольной размерности) связана с коническими кривыми второго порядка. Эти кривые могут быть выбраны множеством различных удобных способов. Если, например, мы выбираем в качестве конической кривой параболу $y = x^2/2$, то точка (a, b) отображается в прямую $y = ax - b$ и *наоборот* (полярность всегда является *инволютивным* преобразованием). Если (a, b) является внешней по отношению к параболе точкой, то ее образ, называемый *полярой*, есть прямая, проходящая через точки касания опорных прямых к параболе, проведенных из точки (a, b). Это преобразование сохраняет инцидентность, т. е. если точка (c, d) лежит на прямой $y = ex - f$, то же самое справедливо и для двойственных к ним элементов: точка (e, f) лежит на прямой $y = cx - d$.

Рассмотрим теперь задачу нахождения пересечения нижних полуплоскостей. Заметим, что нижняя полуплоскость k является *несущественной* тогда и только тогда, когда существуют две нижние полуплоскости i и j, такие, что

(i) ограничивающая прямая L_k расположена выше точки p пересечения прямых L_i и L_j, ограничивающих полуплоскости i и j соответственно, и

(ii) угол наклона прямой L_k находится между углами наклона прямых L_i и L_j.

Соответствующие утверждения имеют место и в двойственной плоскости. Заметим, что мы отображаем прямые, определяющие полуплоскости, в точки в двойственной плоскости. Точка p_k в двойственной плоскости, представляющая образ прямой L_k, является несущественной тогда и только тогда, когда существуют две точки p_i и p_j, такие, что

(i) p_k находится ниже прямой L_p, представляющей образ точки пересечения прямых L_i и L_j, и

(ii) x-координата точки p_k находится между x-координатами точек p_i и p_j.

Другими словами, точка в двойственной плоскости является несущественной тогда и только тогда, когда она находится непосредственно под отрезком, определяемым двумя другими точками. С учетом сказанного можно показать [61], что существенные верхние полуплоскости соответствуют вершинам ломаной, ограничивающей снизу выпуклую оболочку точек в двойственной плоскости. Так как выпуклая оболочка может быть построена за время $O(n \log n)$, то пересечение n верхних полуплоскостей может быть найдено за время $O(n \log n)$. Аналогич-

но пересечение n нижних полуплоскостей также может быть найдено за время $O(n \log n)$. Если уже найдены пересечения верхних полуплоскостей и нижних полуплоскостей, то пересечение двух неограниченных многоугольников может быть найдено за линейное время, например, методом заметания плоскости, так как ребра, определяющие пересечения, упорядочены. Таким образом, имеет место следующая теорема.

Теорема 5. *Пересечение n полуплоскостей может быть найдено за время $O(n \log n)$ методом геометрического преобразования.*

Заметим, что данный метод преобразования легко может быть расширен на случай пространств большей размерности. В частности, пересечение n полупространств может быть найдено за время $O(n \log n)$ путем построения нижней части выпуклой оболочки точек в двойственном пространстве с помощью алгоритма, разработанного Препаратой и Хонгом [293]. Описание общих схем нахождения пересечения n произвольных полупространств за время $O(n \log n)$ можно найти в [294] (см. также [117]). Более подробное обсуждение геометрических преобразований и их применения можно найти, например, в [61, 62, 71, 86, 132, 133, 265, 295].

F. Поиск с отсечением

Этот подход, использованный Меджиддо [257—259] и Дайером [118], первоначально применялся для решения оптимизационных задач и, как было показано, является мощным средством, позволяющим создавать эффективные алгоритмы для решения ряда геометрических оптимизационных задач, одной из которых является хорошо известная задача линейного программирования. Блестящий полиномиальный алгоритм, разработанный несколько лет назад Хачияном (см. [195, 28*, 38*]), представляет главным образом теоретический интерес, так как он не может конкурировать с более практическим симплекс-методом [96]. Совсем недавно Меджиддо и Дайер независимо предложили новый метод многомерного поиска, который мы классифицируем как *метод поиска с отсечением*, с целью получить линейный по времени алгоритм для задачи линейного программирования в случае, когда размерность пространства фиксирована [257, 259].

Заметим, однако, что временна́я сложность является дважды экспоненциальной относительно размерности пространства. Использование этого метода позволяет эффективно решать некоторые геометрические оптимизационные задачи. В частности, укажем следующие: задача линейной отделимости, т. е. заданы

n точек в $\mathbf{R}^d$, сгруппированные в два непересекающихся множества, и требуется найти гиперплоскость, если она существует, которая разделяет эти два множества; задача Чебышёва о регрессии, а именно: заданы n точек $p_i = (x_{i1}, x_{i2}, \ldots, x_{id}) \in \mathbf{R}^d$, $i = 1, 2, \ldots, n$, требуется найти линейную функцию

$$f(x_1, x_2, \ldots, x_d) = \sum_{j=1}^{d-1} a_j x_j + a_d,$$

минимизирующую

$$\max\left\{\left|\sum_{j=1}^{d-1} a_j x_{ij} + a_d - x_{id}\right|, \quad i = 1, 2, \ldots, n\right\};$$

задача об охватывающей гиперсфере, а именно: заданы n точек в $\mathbf{R}^d$, требуется найти наименьшую гиперсферу, содержащую все эти точки. Все эти задачи могут быть решены за время $O(n)$ при условии, что d фиксировано. Метод может быть обобщен для решения оптимизационных задач квадратичного программирования. Обсуждение подробностей такого расширения и других связанных с этим задач, решаемых указанным или аналогичным ему методом, может быть найдено в [257].

Теперь мы дадим небольшой набросок этого замечательного метода для случая двумерного пространства. Задача линейного программирования формулируется следующим образом:

минимизировать $ax + by$

при условии $a_i x + b_i y + c_i \leqslant 0$, $i = 1, 2, \ldots, n$.

Рассматриваемый метод отбрасывает не только несущественные ограничения, но также и те ограничения, которые гарантированно не содержат вершину области возможных решений, минимизирующей функционал. Сначала мы реализуем линейное преобразование точек плоскости так, что функционал станет равным одной из двух координат, например ординате. Тогда исходная задача сводится к нахождению экстремума кусочно-линейной выпуклой функции, зависящей от абсциссы. Ключевой момент состоит в том, что так как все, что нам требуется, — это определить абсциссу точки экстремума, то нет необходимости явно строить эту выпуклую функцию, которая остается неявно определенной множеством линейных ограничений.

Прежде всего положим $Y = ax + by$, $X = x$. Предполагая без потери общности, что $b \neq 0$, получаем

минимизировать Y

при условии $\alpha_i X + \beta_i Y + c_i \leqslant 0$, $i = 1, 2, \ldots, n$,

где

$$\alpha_i = (a_i - (a/b)\, b_i), \quad \beta_i = b_i/b.$$

В такой новой форме мы должны вычислить наименьшее значение Y для вершин выпуклого многоугольника P (область возможных решений), определяемого этими ограничениями (рис. 2). В зависимости от того, является ли β_i равным нулю, отрицательным или положительным числом, n ограничений распадаются на три класса I_0, I_-, I_+. Множество I_0 определяет интервал $[u_1, u_2]$ значений X, в котором необходимо искать решение, в то время как множества I_- и I_+ определяют в неявном

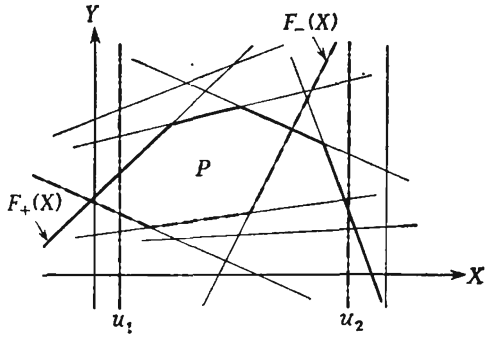


Рис. 2. Пример области возможных решений, определяемой множеством линейных ограничений.

виде соответственно выпуклую вниз и выпуклую вверх кусочно-линейные функции $F_-(X)$ и $F_+(X)$, определяющие границу области возможных решений. Таким образом, исходная задача преобразуется в следующую:

минимизировать $F_-(X)$

при условии $F_-(X) \leqslant F_+(X)$, $u_1 \leqslant X \leqslant u_2$.

Значения $F_-(X)$ и $F_+(X)$ для произвольного X могут быть вычислены за время $O(n)$. Это относится и к величине наклона функций. Таким образом, в рамках указанного ограничения по времени для каждой точки $X' \in [u_1, u_2]$ может быть получен один из следующих результатов: (i) значение X' недопустимо и задача не имеет решения; (ii) значение X' недопустимо и нам известно, с какой стороны от X' (слева или справа) может находиться некоторое допустимое значение X; (iii) значение X' допустимо и нам известно, с какой стороны от X' находится точка минимума $F_-(X)$ и (iv) значение X' соответствует мини-

муму функции $F_-(X)$. Случаи (i) и (iv) дают окончательные решения.

Чтобы выбрать X', мы разбиваем как l_+, так и l_- на пары ограничений (прямых линий) и определяем абсциссу X_{ij} их пересечения. Если $X_{ij} \overline{\in} [u_1, u_2]$, то одно из ограничений может быть немедленно отброшено как несущественное. Для множества значений $X_{ij} \in [u_1, u_2]$ за время $O(n)$ [1, 111, 306] мы находим их медиану X'' и оцениваем $F_+(X'')$ и $F_-(X'')$. Затем, согласно приведенным выше соображениям, половина значений X_{ij} лежит в области, не содержащей значения, на котором достигается минимальное значение, так что одно ограничение пары может быть исключено. Таким способом при каждом вычислении $F_+(X)$ и $F_-(X)$ некоторая фиксированная часть α оставшихся на текущий момент ограничений может быть удалена. Это приводит к заключению, что за $\log_{1/(1-\alpha)} n$ шагов размер множества оставшихся ограничений станет достаточно малым для поиска решения прямым способом. Так как требуемое время равно

$$Cn + C\alpha n + C\alpha^2 n + \ldots = O(n),$$

где C — некоторая константа, то имеем следующий результат.

Теорема 6. *Двумерная задача линейного программирования с n ограничениями может быть решена за время $O(n)$.*

G. Метод динамизации

Эти методы разработаны для задач, база данных которых изменяется со временем (время изменяется дискретно). Идея состоит в том, чтобы использовать хорошие структуры данных для статической (фиксированной) базы данных и дополнить их механизмами динамизации таким образом, чтобы операции с базой данных (вставки и исключения элементов) можно было выполнять эффективно.

Как и ранее, опишем общий подход на примере. Пример относится к классу *задач геометрического поиска*. Типичной задачей поиска является задача *о принадлежности*, а именно задано множество объектов F и необходимо определить, принадлежит ли x множеству F? Если F — множество вещественных чисел, то может представлять интерес вопрос о ближайшем соседе x, т. е. таком элементе F, который наиболее близок к x. В литературе эта задача известна под названием задачи о наиболее подходящем элементе [64, 156] или задачи поиска ближайшего соседа [147, 157, 171, 354]. Более формально, в общем случае запрос к базе данных представляет некоторый вопрос, содержащий переменную типа $T1$ и относящийся к множеству,

состоящему из элементов типа $T2$, а ответ на вопрос — значение типа $T3$. В запросе о принадлежности $T1$ и $T2$ совпадают, а $T3$ — логический тип; в запросе о ближайшем соседе типы $T1$, $T2$ и $T3$ одинаковы — вещественные числа. Запрос Q можно рассматривать как отображение из $T1$ и множества подмножеств $T2$ в $T3$, т. е. Q: $T1 \times 2^{T2} \rightarrow T3$ [39, 304].

Далее определен класс задач, называемых *задачами поиска, допускающими декомпозицию*, к которым применимы методы динамизации.

Определение [29]. Задача поиска с операцией запроса Q допускает декомпозицию, если существует эффективно вычислимый бинарный оператор @ (ассоциативный и коммутативный), удовлетворяющий условию

$$Q(x, A \cup B) = @(Q(x, A), Q(x, B)).$$

Легко видеть, что оба приведенных выше примера допускают декомпозицию.

В задаче поиска мы имеем некоторую структуру данных для множества элементов, среди которых производится поиск. Существуют три меры затрат ресурсов, связанные с некоторой структурой данных A, а именно:

1) $P_A(N)$ — время предобработки, необходимое для построения структуры A,

2) $Q_A(N)$ — время, необходимое для поиска в структуре A по запросу,

3) $S_A(N)$ — объем памяти, необходимый для хранения структуры A.

Здесь N — число элементов множества, для представления которого используется структура A.

Процедура динамизации включает в себя преобразование некоторого вида, которое преобразует статическую структуру данных в динамическую, допускающую вставку и исключение элементов. Рассмотрим задачу поиска ближайшего соседа на плоскости. Пусть на плоскости задано множество из n точек и требуется найти ближайшего соседа некоторой запрашиваемой точки x. Для статического варианта этой задачи имеем следующие *меры затрат ресурсов*:

$$P_A(n) = O(n \log n), \quad Q_A(n) = O(\log n) \text{ и } S_A(n) = O(n),$$

где A, например, одна из структур данных, рассматриваемых в работах Липтона и Тарьяна [242], Киркпатрика [197] или Эделсбруннера и др. [128]. Теперь рассмотрим, как можно преобразовать структуру данных A в динамическую структуру данных D, чтобы иметь возможность выполнять операции вставки, исключения и поиска по запросам. Существует целый ряд ме-

тодов динамизации [121, 164, 166, 248, 262, 263, 276, 279, 280, 282, 304, 339, 340, 341], известных в литературе, но здесь мы опишем метод, разработанный ван Леувеном и Вудом [341], который воплощает все существенные черты этого подхода.

Общий принцип состоит в том, чтобы организовать файл в виде совокупности отдельных структур данных таким образом, чтобы каждая корректировка данных затрагивала одну из них (или, возможно, небольшое фиксированное число). Однако, чтобы избежать переноса центра тяжести задачи на обработку запросов, следует воздерживаться от чрезмерной фрагментации, так как обычно запросы охватывают всю совокупность данных. Вооружившись этой общей идеей, рассмотрим следующий пример. Пусть $\{x_k\}_{k\geq 1}$ — возрастающая последовательность целых чисел, называемых *точками переключения*, где x_k делится на k и $x_{k+1}/(k+1) > x_k/k$. Положим $x_0 = 0$, $y_k = x_k/k$ и пусть n — текущий размер множества точек. Множество точек разбивается на совокупность подмножеств, каждое из которых представляется отдельной статической структурой данных. Для заданного целого числа k, называемого *уровнем*, динамическая структура данных D состоит из $(k+1)$ структур одного и того же типа A: k из них, называемые *блоками*, имеют размер в диапазоне от y_k до y_{k+1}, в то время как одна, называемая *кучей*, имеет размер от 0 до $(y_{k+1}-1)$ Каждая такая структура B снабжена счетчиком $s(B)$, определяющим ее *статус* — «мало», «частично» или «полностью» в зависимости от того, имеет место $s(B) = y_k$, $y_k < s(B) < y_{k+1}$ или $s(B) = y_{k+1}$ соответственно.

Как отмечалось ранее, запрос охватывает все $(k+1)$ структур с полным временем ответа на запрос $O(kQ_A(y_{k+1}))$, так как y_{k+1} является границей для их размеров. Более тонкой является обработка корректировок, где, для того чтобы контролировать расход ресурсов, необходимо контролировать максимальный размер структур данных. Вставки являются более простыми операциями, так как все они могут быть отнесены к куче. Исключения же элементов могут возникнуть, где угодно, и может оказаться необходимым сочетать исключение элемента в блоке с перемещением из другого блока (особенно из блока со статусом «частично», если исключение имеет место в блоке со статусом «мало»).

Разумеется, статическая структура данных должна быть снабжена словарем [1] размера n для того, чтобы за время $C(n)$ можно было определить блок, из которого удаляется элемент. Во всех случаях затраты на коррекцию данных составляют $O(U_A(y_{k+1}) + C(n))$, так как y_{k+1} — максимальный размер статических структур. Отметим, что значительные изменения n сопровождаются более умеренными изменениями параметра k. Действительно, когда все блоки на уровне k заполнены, мы

переключаемся на уровень $k+1$ в тот момент, когда размер кучи также достигает y_{k+1}. Это делается путем включения кучи в совокупность блоков (число блоков доводится до $k+1$), изменения их статуса с «полностью» на «мало» и инициализации новой кучи с числом элементов, равным 0. Заметим, что когда мы переключаемся с уровня k на уровень $k+1$, то имеем в точности $(k+1)y_{k+1} = x_{k+1}$ точек в множестве. С другой стороны, когда размер множества изменяется с x_k до $x_k - 1$, мы аналогичным образом переключаемся с уровня k на уровень $k-1$, при этом блок превращается в кучу. Можно показать [341], что переключение между уровнями может быть корректно выполнено за время $O(1)$. Следующая теорема подводит итог предыдущему обсуждению.

Теорема 7. *Любая статическая структура данных A, используемая при решении задачи поиска, допускающей декомпозицию, может быть преобразована в динамическую структуру данных D для той же самой задачи со следующими характеристиками. Если $x_k \leqslant n < x_{k+1}$, то время $Q_D(n)$ ответа на запрос для D есть $Q_D(n) = O(kQ_A(y_{k+1}))$. Время корректировки данных $U_D(n)$ (вставка или удаление элемента) для D есть $U_D(n) = O(C(n) + U_A(y_{k+1}))$. Необходимый объем памяти равен $S_D(n) = O(kS_A(y_{k+1}))$.*

Если, например, выбирать в качестве точек переключения такие целые числа, что x_k — первое число, кратное k, большее или равное 2^k, то k примерно равно $\log_2 n$ и y_k примерно равно $n/\log_2 n$. Так как для задачи поиска ближайшего соседа имеется структура данных A, такая, что

$$Q_A(n) = O(\log n) \text{ и } U_A(n) = P_A(n) = O(n \log n)$$

[197, 242], то имеет место приводимое ниже следствие.

Следствие 1. *Задача поиска ближайшего соседа на плоскости может быть решена таким образом, что время ответа на запрос будет $O(\log^2 n)$, а время корректировки структуры будет $O(n)$. (Отметим, что в нашем случае $C(n) = O(\log n)$.)*

Существует несколько других схем динамизации с разными соотношениями (время ответа на запрос)/(требуемая память) и (время ответа на запрос)/(время на перестройку). Например, если в рассмотренной схеме выбрать иную последовательность точек переключения, то получатся и другие время ответа на запрос и время корректировки. Читателя, интересующегося деталями, мы отсылаем к упоминавшимся выше работам.

III. КЛАССЫ ЗАДАЧ

В этом разделе мы дадим обзор каждого из классов задач, о которых было сказано в введении.

А. Выпуклые оболочки

Задача построения выпуклой оболочки не только оказывается центральной для практических приложений, но является также основой для решения ряда других важных вопросов вычислительной геометрии.

Задача 3.1.1. Выпуклая оболочка. Задано множество S из n точек в d-мерном пространстве. Требуется найти выпуклую оболочку этого множества. (Выпуклая оболочка множества — это наименьшее выпуклое множество, содержащее заданное множество; граница выпуклой оболочки S обозначается $\mathrm{CH}(S)$.)

Задача построения выпуклой оболочки, в частности для множества точек на плоскости, интенсивно изучалась и имеет разнообразные приложения в распознавании образов [5, 115], обработке изображений [301] и других областях [152]. В разд. II-D мы уже видели, что эта задача может быть решена методом «разделяй и властвуй» за время $O(n \log n)$. Имеется длинный список статей, содержащих результаты о выпуклой оболочке множества точек на плоскости [3, 4, 6, 7, 31, 32, 42, 66, 68, 120, 167, 184, 293, 310, 313]. Время работы предлагаемых алгоритмов равно либо $O(n \log n)$, либо $O(nH)$, где H — число точек на границе выпуклой оболочки. Исключение составляют работы [68, 310], в которых рассматривается построение выпуклой оболочки в пространствах более высокой размерности.

Отметим здесь, что результатом решения задачи построения выпуклой оболочки на плоскости является упорядоченный список вершин, лежащих на границе выпуклой оболочки. Следовательно, время $O(n \log n)$ является необходимым и достаточным для построения выпуклой оболочки (см. лемму 3.6.2).

Мы начнем с краткого обзора двух ранних подходов к решению этой задачи, известных под названиями: метод сканирования Грэхэма [167] и метод обхода Джарвиса [184]. Обе эти схемы содержат много плодотворных для данной темы идей. В связи с этим следует обратить внимание на работу [333], в которой приоритет на разработку первого алгоритма построения выпуклой оболочки приписывается Бэссу и Шуберту [25].

Метод сканирования Грэхэма. Грэхэм в одной из первых работ, посвященных задачам вычислительной геометрии [167], предложил алгоритм со сложностью $O(n \log n)$ для вычисления выпуклой оболочки n точек на плоскости. Этот алгоритм работает следующим образом. Во-первых, произвольным образом

выбирается некоторая внутренняя точка O, например геометрический центр масс трех из заданных точек. Во-вторых, точки множества упорядочиваются в соответствии с их углом поворота относительно точки O. Затем выбирается точка, про которую заведомо известно, что она лежит на выпуклой оболочке, например точка v_0 с минимальной y-координатой (и максимальной x-координатой, если таких точек несколько). Предположим, что множество точек представлено упорядоченным списком $v_0, v_1, \ldots, v_{n-1}$, в котором точки перечислены в порядке обхода против часовой стрелки относительно выбранной ранее точки O, и при этом $v_i =$ СЛЕДУЮЩИЙ (v_{i-1}), $i = 1, 2, \ldots, n$, и $v_n = v_0$. Указатель ПРЕДЫДУЩИЙ соответствует обходу в обратном порядке по часовой стрелке. Теперь просмотрим все точки, обрабатывая на каждом шаге по три точки. Будем говорить, что три точки t, u, v образуют *левый поворот*, если точка v расположена строго слева от направленной прямой, идущей от t к u. Просмотр точек выполняется следующим образом.

```
begin v := v0;
      while СЛЕДУЮЩИЙ(v) ≠ v0 do
         if v, СЛЕДУЮЩИЙ(v), СЛЕДУЮЩИЙ
            (СЛЕДУЮЩИЙ(v)) образуют левый поворот
         then v := СЛЕДУЮЩИЙ(v)
         else begin
                 УДАЛИТЬ СЛЕДУЮЩИЙ(v);
                 if v ≠ v0, then v := ПРЕДЫДУЩИЙ(v)
              end
end
```

Всякий раз, когда последовательная тройка вершин образует левый поворот, мы продвигаемся дальше. В противном случае средняя точка СЛЕДУЮЩИЙ(v) не принадлежит выпуклой оболочке и должна быть удалена (и больше никогда не просматриваться вновь). При удалении вершины мы *возвращаемся назад* для того, чтобы проверить, что точка v по-прежнему принадлежит выпуклой оболочке. Таким образом, мы либо продвигаемся вперед по списку вершин, либо возвращаемся назад по списку вершин, отнесенных предварительно к выпуклой оболочке. Так как на выполнение каждого шага требуется постоянный квант времени, то весь просмотр списка осуществляется за линейное время. Поэтому полное время выполнения алгоритма равно $O(n \log n)$, так как определяющим является шаг сортировки.

Метод обхода Джарвиса. Указав на то, что независимо от окончательной выпуклой оболочки алгоритм Грэхэма всегда

выполняется за время $O(n \log n)$, Джарвис предложил альтернативное решение задачи построения выпуклой оболочки, требующее времени $O(nH)$, где H — число вершин выпуклой оболочки [184]. Следовательно, если $H = o(\log n)$, то алгоритм Джарвиса лучше, чем алгоритм Грэхэма. Подход, выбранный Джарвисом, соблазнителен идеей «заворачивания подарка в бумагу», также применимой к методу [68]. Начиная с точки u, про которую известно, что она принадлежит выпуклой оболочке (как и в методе Грэхэма), за линейное время мы находим следующую точку v, такую, что ребро $\overline{u, v}$ входит в выпуклую оболочку, т. е. все остальные точки лежат по одну сторону от ориентированной прямой, содержащей ребро $\overline{u, v}$. После того как вершина v найдена, тот же самый метод применяется для выявления следующей точки w, такой, что $\overline{v, w}$ является ребром выпуклой оболочки, и так далее до тех пор, пока мы не «обернем» снова начальную точку u. Легко видеть, что число необходимых итераций в точности равно числу вершин выпуклой оболочки, так что полное время равно $O(nH)$, так как каждая итерация требует времени $O(n)$.

Другой интересный подход, допускающий обобщение на случай трехмерного пространства, основан на методе «разделяй и властвуй» [293, 315]. После разбиения исходного множества точек на два примерно равных подмножества и рекурсивного построения их выпуклой оболочки шаг соединения получившихся решений выполняется на основе решения следующей задачи.

Задача 3.1.2. Объединение двух непересекающихся выпуклых многоугольников. Заданы два непересекающихся выпуклых многоугольника P и Q с p и q вершинами соответственно. Требуется найти их выпуклую оболочку.

Эта задача решена в работе [293] путем нахождения общих опорных прямых к P и Q, где *опорная прямая* к многоугольнику P — это прямая линия, имеющая по крайней мере одну общую точку с P, и все вершины P расположены по одну сторону от этой линии. Так как по предположению P и Q не пересекаются, то P и Q имеют две опорные прямые, такие, что P и Q находятся по одну сторону. Такие прямые могут быть найдены за время $O(p + q)$.

Стягивая Q до одной точки, получаем непосредственно решение следующей дополнительной задачи.

Задача 3.1.3. Опорные прямые к выпуклому многоугольнику. Задан выпуклый многоуольник P с n вершинами и внешняя по отношению к P точка u. Требуется найти две опорные прямые к P, проходящие через точку u.

Эта задача, тривиальная без использования предобработки, становится более интересной в режиме многократного использования и может быть решена за время $O(\log n)$ путем очевидной адаптации процедуры бинарного поиска [316].

Некоторые из представленных выше идей были элегантно соединены в новом интересном методе построения выпуклой оболочки, разработанном недавно Киркпатриком и Сейделом [198]. Их метод представляет комбинацию подходов разделяй и властвуй и поиска с отсечением и для его выполнения требуется время $O(n \log H)$, что является асимптотически оптимальным [199]. Алгоритм раздельно строит верхнюю и нижнюю части оболочки, а именно две цепочки вершин оболочки, разделенные самой левой и самой правой вершинами. С учетом симметричности построения рассматривается построение только верхней части оболочки. Сначала множество точек S разбивается на два подмножества примерно равного размера. Далее вместо рекурсивного построения верхней части оболочки двух половин и вычисления их общей опорной прямой (называемой *верхним соединением*) сначала строится это соединение, а затем раздельно верхние оболочки множеств, соответственно слева и справа от самой левой и самой правой конечных точек соединения (*точек соединения*).

Ключевым моментом метода является эффективный способ построения соединения, который будет обсужден ниже. Сначала мы дадим не совсем формальное описание схемы алгоритма. Если M_1 и M_2 — индексы точек множества S, имеющих самую маленькую и самую большую абсциссы (для простоты считается, что абсциссы всех точек различны), то верхняя часть оболочки строится в результате обращения СОЕДИНИТЬ(M_1, M_2; S) к следующей процедуре:

Procedure СОЕДИНИТЬ (min, max; A)
begin
1. Найти вертикальную прямую $x = m$, **разделяющую** A на две половины.
2. $(i, j) :=$ СОЕДИНЕНИЕ(A, m)
   (**Comment**: i и j — индексы точек **соединения** p_i и p_j, расположенных соответственно **слева и справа от** вертикальной прямой.)
3. Пусть $A_1 = \{p \in A,\ x(p) \leqslant x(p_i)\}$
   Пусть $A_2 = \{p \in A,\ x(p) \geqslant x(p_j)\}$
4. **If** $i = \min$ **then** печатать(i)
   else СОЕДИНИТЬ(min, i; A_1);
   if $j = \max$ **then** печатать(j)
   else СОЕДИНИТЬ(j, max; A_2)

end

Время выполнения процедуры СОЕДИНИТЬ зависит от времени выполнения функции СОЕДИНЕНИЕ. Последняя, однако, как легко видеть, представляет задачу линейного программирования для двух переменных и n ограничений. Действительно, соединение принадлежит прямой L^*, такой, что каждая точка S находится ниже L^*, и ордината пересечения которой с прямой $x = m$ минимальна. Таким образом, положив L: $y = ax + b$, имеем

минимизировать $(ma + b)$
при условии $x_j a + b \geqslant y_j$, $j = 1, 2, \ldots, n$.

Используя метод поиска с отсечением из работ [118, 257], коротко рассмотренный в разд. II-F, эту задачу можно решить за время $\theta(n)$. Отмечая, что нахождение медианы на шаге 1 выполнения процедуры СОЕДИНИТЬ также требует времени $\theta(n)$, и обозначая через h число ребер верхней части оболочки, находим, что время выполнения $T(n, h)$ СОЕДИНИТЬ удовлетворяет следующему рекуррентному соотношению:

$$T(n, h) = cn, \quad \text{если } h = 1,$$
$$T(n, h) = cn + \max_{h_1+h_2=h}(T(n/2, h_1) + T(n/2, h_2)),$$
$$\text{если } h > 1, \ c \text{ — некоторая константа.}$$

Нетрудно заметить, что $T(n, h)$ равно $O(n \log h)$. Таким образом, за время $O(n \log h)$ мы можем получить верхнюю часть выпуклой оболочки. Аналогичным образом вычисляется нижняя часть выпуклой оболочки, так что легко устанавливается верхняя оценка $O(n \log H)$ времени построения полной оболочки. Обращаем внимание также на работу [254], в которой дана модификация алгоритма из работы [198], обладающая лучшим поведением в среднем.

При размерности пространства $d \geqslant 3$ имеем следующие результаты. В работе [8] приведен алгоритм построения выпуклой оболочки в трехмерном пространстве без анализа временной сложности алгоритма. В [185] дан алгоритм со сложностью $O(nF)$, где F — число граней трехмерной выпуклой оболочки, разработанный на основе подхода, аналогичного рассмотренному в [184]. В работе [293] дан оптимальный ($O(n \log n)$) алгоритм на основе метода «разделяй и властвуй» для построения выпуклой оболочки в пространствах размерности 2 и 3. В работах [68] и [310] дан алгоритм решения задачи построения выпуклой оболочки в случае пространств размерности $d \geqslant 3$. Алгоритм в работе [185] является частным случаем для $d = 3$ метода, рассмотренного в [68], а алгоритм в работе [310] является оптимальным для пространств четной размерности.

В работе [42] дан алгоритм с линейной сложностью в среднем для задачи построения выпуклой оболочки на плоскости. (См. также работу [97], содержащую обзор алгоритмов построения выпуклой оболочки с линейной сложностью в среднем.)

Мы завершаем этот раздел обзором нескольких дополнительных задач, имеющих отношение к понятию выпуклой оболочки.

Задача 3.1.4. Выпуклая оболочка простого многоугольника. На плоскости задан простой многоугольник с n вершинами. Требуется найти его выпуклую оболочку.

Тот факт, что точки заданы в виде некоторой последовательности вершин простого многоугольника, позволяет решить эту задачу за линейное время [48, 168, 214, 249, 334].

Задача 3.1.5. Принадлежность выпуклому многоугольнику. Задан выпуклый многоугольник P с n вершинами. При условии что допускается предобработка, определить, находится ли некоторая пробная точка u внутри P.

Эта задача может быть решена очень легко. Возьмем произвольную внутреннюю точку O многоугольника P в качестве начала. Представим вершины многоугольника P в виде бинарного дерева поиска (это можно сделать, так как вершины P упорядочены в порядке обхода при движении вокруг точки O). Выполняя бинарный поиск, определим сектор, в котором находится пробная точка. (Сектор — это область плоскости, определяемая точкой O и двумя последовательными вершинами многоугольника P.) Если сектор уже определен, достаточно выполнить единственное сравнение, чтобы определить, с какой стороны от ребра многоугольника P находится точка, т. е. определить, находится ли она внутри P.

Задача 3.1.6. Последовательное построение выпуклой оболочки. Задано множество из n точек $p_1, p_2, \ldots, p_n$, поступающих последовательно по одной точке за раз. Требуется найти выпуклую оболочку множества $\{p_1, p_2, \ldots, p_i\}$ после поступления точки p_i.

Прямой подход непосредственного построения выпуклой оболочки каждый раз, когда поступает новая точка, является вполне корректным, но при этом время вычислений равно

$$\sum_{i=2}^{n} O(i \log i) = O(n^2 \log n).$$

Вопрос состоит в том, можно ли сделать это лучшим образом. Оказывается, что, используя свойство выпуклости, можно раз-

работать алгоритм со сложностью $O(n \log n)$, при этом время, достаточное для конструирования новой выпуклой оболочки для каждой вновь поступившей точки, составляет $O(\log n)$ [291]. Основная идея состоит в том, чтобы организовать вершины текущей выпуклой оболочки в виде бинарного дерева определенного вида и для каждой новой точки p_i прежде всего определить, находится ли она внутри текущей выпуклой оболочки. Если это так, то точка игнорируется. В противоположном случае ищутся две опорные прямые из точки p_i к текущей выпуклой оболочке. Затем выпуклая оболочка изменяется путем удаления соответствующего множества вершин, заключенных между опорными прямыми, и включения точки p_i в качестве новой вершины. Проверка принадлежности точки к внутренности выпуклой оболочки, определение опорных прямых и удаление вершин, не принадлежащих выпуклой оболочке, могут быть выполнены за время $O(\log i)$. Детальное обсуждение см. в работе [291]. Более простой альтернативный метод может быть найден в работах [21, 221].

Естественный вопрос, который может быть задан в этом месте, состоит в том, а что же произойдет, если разрешить удалять точки. В этом случае мы больше не можем уничтожать те точки, о которых стало известно, что они не находятся на выпуклой оболочке, так как они могут вновь стать вершинами выпуклой оболочки после удаления некоторой точки выпуклой оболочки. Таким образом, мы имеем следующую задачу.

Задача 3.1.7. Поддержание выпуклой оболочки. Задана последовательность точек $p_1, p_2, \ldots, p_n$, часть из которых соответствует исключаемым точкам, а часть — добавляемым. Необходимо поддерживать выпуклую оболочку этого множества точек.

Эта задача была элегантно решена Овермарсом и ван Леувеном [281]. Они показали, что выпуклую оболочку можно поддерживать, затрачивая на операции добавления и исключения точек время, равное $O(\log^2 n)$.

Задача 3.1.8. Глубина и выпуклые слои множества. Задано множество S из n точек на плоскости. Требуется найти последовательность $(\mathrm{CH}(S_i) \mid i = 1, 2, \ldots, d)$, где $S_0 = S$ и $S_i = S_{i-1} - V(\mathrm{CH}(S_{i-1}))$, $i = 1, 2, \ldots, d$. Здесь $V(\mathrm{CH}(T))$ обозначает множество вершин $\mathrm{CH}(T)$, а $S_d = V(\mathrm{CH}(S_d))$. Глубина множества точек равна d, т. е. числу выпуклых слоев, полученных в результате указанной процедуры.

Эта задача возникает при статистическом оценивании, где «наблюдения» (точки) на внешних слоях выпуклых оболочек представляют «шум» и должны быть исключены из числа ис-

пользуемых для оценивания. Модифицируя алгоритм Джарвиса, легко получить алгоритм со сложностью $O(n^2)$. При использовании алгоритма Овермарса и ван Леувена [281] граница для худшего случая может быть улучшена до $O(n \log^2 n)$. Недавно Чазелле получил для этой задачи оптимальный алгоритм со сложностью $O(n \log n)$. Этот результат имеет применение в задаче полупланарного интервального поиска и при вычислении *глубины* произвольной заданной точки. (*Глубина* некоторой пробной точки в множестве точек S определяется как число выпуклых слоев множества S, охватывающих эту точку.) С помощью предобработки выпуклых слоев глубина пробной точки может быть определена в результате вычисления, в какую из областей между последовательными слоями она попадает (ср. с задачей 3.3.10).

Эффективный алгоритм, отличный от тривиального, для вычисления выпуклых слоев множества точек в пространствах размерности $d \geqslant 3$, неизвестен.

В. Пересечения

Задачи пересечения и их вариации возникают во многих областях науки и практики, таких, как проектирование в архитектуре, машинная графика, распознавание образов и т. д. При архитектурном проектировании нельзя поместить два непроницаемых объекта в одно и то же место в пространстве. При отображении объектов на двумерном поле скрытые части (или пересекающиеся части) должны быть удалены, чтобы усилить ощущение реальности. Это — давняя задача, известная как задача удаления скрытых (невидимых) линий или поверхностей [268].

При проектировании интегральных схем два различных элемента должны быть удалены друг от друга на определенное расстояние, и обнаружение того, выполняется или нет это условие, по сути дела является задачей пересечения. Так как конкретная задача может содержать тысячи объектов, то необходимы быстрые алгоритмы для обнаружения пересечения или сигнализации о наличии пересечения перекрывающихся объектов. Другой повод для изучения сложности алгоритмов для задач пересечения состоит в том, что это может пролить свет на присущую геометрическим задачам сложность. Например, насколько сложной является процедура определения, является ли заданный многоугольник с n вершинами простым (проверка простоты), или как много времени необходимо для определения, имеются ли среди n объектов на плоскости, таких, как многоугольники, отрезки и т. д., два пересекающихся (*обнаружение пересечения*)? Обе задачи решаются за время $O(n \log n)$

[317]. Этот результат является оптимальным в рамках модели алгебраических деревьев вычислений (с некоторым набором примитивных операций) [26] для последней задачи, в то время как для первой задачи остается открытым вопрос о том, является ли $\Omega(n \log n)$ нижней оценкой.

Среди множества задач о пересечении объектов можно выделить два основных типа: задачи на построение и задачи на обнаружение пересечения. В задачах первого типа требуется явно вычислить пересечение, в то время как задачи второго типа относятся к категории задач на проверку (в которой требуется определить, какие два объекта пересекаются, если пересечение вообще имеет место). Очевидно, что задача обнаружения пересечения легче задачи построения пересечения объектов, и убедительное доказательство этого приведено в работе [82]. Теперь мы обсудим класс важных задач о пересечении объектов. В дальнейшем мы предполагаем, что если задан простой многоугольник P, то *стандартной* формой определения многоугольника является последовательность вершин, т. е. $P=(v_0, v_1, \ldots, v_{n-1})$, и (v_i, v_{i+1}) является ребром для $i=0, 1, \ldots, n-1$, а $v_n = v_0$. При этом внутренняя область многоугольника оказывается расположенной слева при прохождении ребер в указанном порядке.

Задача 3.2.1. Пересечение выпуклых многоугольников. Заданы два выпуклых многоугольника P и Q, имеющие m и n вершин соответственно. Требуется построить их пересечение. Эта задача может быть решена оптимальным образом за время $O(m+n)$ [317] методом заметания плоскости. Очевидно, что пересечение каждого многоугольника с вертикальной полосой, расположенной между двумя последовательными критическими точками, является в общем случае трапецоидом (возможно, пустым или выродившимся в треугольник). Учитывая, что пересечение двух трапецоидов может быть найдено за время $O(1)$, получаем указанный результат (рис. 3). Альтернативный метод был предложен в работе [273].

Задача 3.2.2. Пересечение звездных многоугольников. Заданы два звездных многоугольника с m и n вершинами соответственно. Требуется найти их пересечение. (Многоугольник P называется звездным, если существует по крайней мере одна точка q внутри P, такая, что каждая точка многоугольника P *видна* из q, т. е. отрезок, соединяющий q и произвольную точку многоугольника P, целиком лежит внутри P.)

Для решения этой задачи, однако, требуется время $\Omega(mn)$, так как пересечение может состоять из $O(mn)$ отдельных компонент. Таким образом, общая задача пересечения многоугольников имеет квадратичную сложность решения в худшем случае.

Задача 3.2.3. Обнаружение пересечения отрезков. На плоскости заданы n отрезков. Определить, имеется ли хотя бы одна пара пересекающихся отрезков.

Эта задача может быть решена за время $O(n \log n)$ методом заметания плоскости [317]. Алгоритм основан на следующей идее. Рассмотрим вертикальную заметающую прямую L, которая пересекает некоторое подмножество из заданных отрезков, и эти пересечения образуют полностью упорядоченное множество. Этот порядок сохраняется в каждой вертикальной полосе, не содержащей пересечений или конечных точек отрезков. Если два отрезка пересекаются, то они должны быть смежными друг

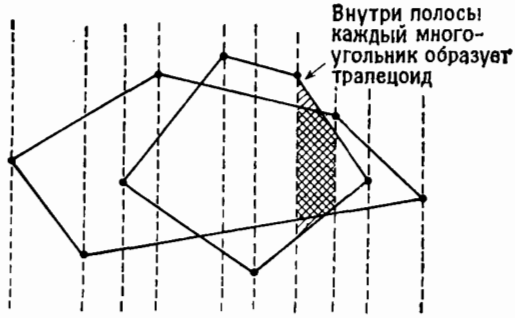


Рис. 3. Вертикальные полосы, определяемые вершинами двух выпуклых многоугольников.

с другом в ходе процесса заметания плоскости. Таким образом, как только отрезок становится активным, он проверяется на пересечение с двумя его соседями, а как только отрезок заканчивается, производится проверка на пересечение двух его соседей (они теперь стали смежными друг с другом). Так как мы выполняем не более n вставок и n исключений, а каждая из этих операций может быть проделана за время $O(\log n)$ (проверка пересечения выполняется за время $O(1)$), то полное время равно $O(n \log n)$, что является оптимальным (ср. с леммой 3.6.4). Отсюда следует, что *задача проверки простоты*, т. е. определение того, что заданный многоугольник является простым, может быть решена за время $O(n \log n)$, и задача определения того, пересекаются ли какие-либо две из n заданных окружностей, также может быть решена за время $O(n \log n)$.

Задача 3.2.4. Обнаружение пересечения многоугольников Заданы два простых многоугольника P и Q, имеющие m и n вершин соответственно. Определить, пересекаются ли они.

Два многоугольника пересекаются, если либо некоторое ребро одного многоугольника пересекает ребро другого многоугольника, либо один многоугольник целиком содержится внутри

другого многоугольника. Первый случай может быть обнаружен за время $O(N \log N)$, где $N = m + n$, а второй требует для своего решения времени $O(m + n)$. Последнюю проверку можно выполнить, выбирая произвольную вершину многоугольника P и Q и проверяя ее принадлежность другому многоугольнику, так как если многоугольник P содержит многоугольник Q, то он должен содержать и любую вершину многоугольника Q. Таким образом, полное время равно $O(N \log N)$.

(*Задача об охвате точки*, т. е. определение того, принадлежит ли точка p многоугольнику Q, может рассматриваться как задача о пересечении, т. е. проверка справедливости равенства $\{p\} \cap Q = \varnothing$, и может быть решена за линейное время [313].) Отметим, что если как P, так и Q являются выпуклыми, то задача может быть решена за время $O(\log N)$ [82].

Задача 3.2.5. Перечисление пересечений отрезков. Заданы n отрезков прямых. Найти все пересекающиеся пары отрезков.

Это типичная задача на перечисление пересечений. Метод заметания плоскости работает здесь так же хорошо, как и ранее. В работе [38] можно найти алгоритм, имеющий временну́ю и емкостную сложности $O((n + k)\log n)$ и $O(n + k)$ соответственно, где k — число пересекающихся пар, о которых сообщит алгоритм. Браун [63] показал, что с помощью более тщательной реализации списка критических точек, который изменяется со временем, необходимый объем памяти может быть уменьшен до $O(n)$. Недавно Чазелле [76] получил алгоритм с временно́й сложностью $O(n \log^2 n/\log\log n + k)$ и емкостной сложностью $O(n + k)$. Это первое из известных решений общей задачи, имеющее сложность, пропорциональную размеру выходных данных k.

Задача 3.2.6. Подсчет числа пересечений. Заданы n отрезков. Найти число пересекающихся пар отрезков.

Эта задача отличается от задачи 3.2.5 тем, что необходимо лишь подсчитать число пересекающихся пар, а не перечислять каждое пересечение. Очевидно, что любой алгоритм, строящий точки пересечения, может быть использован для решения соответствующей задачи на подсчет пересечений. Но, так как параметр k, который определяет размер выходных данных алгоритма, может быть довольно большим ($O(n^2)$ в нашем случае), то это может оказаться неэффективным. Чазелле в той же работе [76] ссылается на ранее полученный алгоритм с временно́й сложностью $O(n^{1,695})$ и емкостной сложностью $O(n)$.

Задача 3.2.7. Построение пересечения n полуплоскостей. На плоскости заданы n полуплоскостей. Построить пересечение всех заданных полуплоскостей.

Можно показать, что *пересечение n полуплоскостей* может быть найдено за время $O(n \log n)$ методом «разделяй и властвуй», так как шаг соединения решений по своей сути есть не что иное, как задача 3.2.1, которая может быть решена за линейное время. Эта оценка является оптимальной (см. разд. III-F).

Задача 3.2.8. Ядро многоугольника. Задан простой многоугольник с n вершинами. Найти его ядро. (*Ядро* многоугольника — это пересечение n полуплоскостей, каждая из которых расположена слева от прямой линии, содержащей ребро многоугольника и ориентированной в соответствии с прохождением ребра в стандартном представлении многоугольника.)

Очевидно, что ядро может быть найдено за время $O(n \log n)$ простым применением алгоритма для вычисления пересечения полуплоскостей. Однако учет того факта, что эти n полуплоскостей не являются произвольными, а определяются ребрами простого многоугольника, позволяет получить алгоритм со сложностью $\theta(n)$ [227].

Задача 3.2.9. Построение пересечения выпуклых многогранников. Заданы два выпуклых многогранника P и Q, имеющие m и n вершин соответственно. Найти их пересечение.

Эта задача является еще одним примером, для которого может быть с успехом применен метод геометрического преобразования, известного как двойственность. Маллер и Препарата [265] получили для этой задачи алгоритм со сложностью $O(N \log N)$, где $N = m + n$. Дайер также разработал алгоритм решения этой задачи, имеющий сложность $O(N \log N)$ [117]. Недавно для решения этой задачи был предложен совершенно другой элегантный алгоритм, использующий метод заметания пространства [176].

Задача 3.2.10. Обнаружение пересечения выпуклых многогранников. Заданы два выпуклых многогранника P и Q, имеющие m и n вершин соответственно. Определить, пересекаются ли они.

Очевидно, алгоритм решения соответствующей задачи построения пересечения работает и в этом случае. Однако так как нам необходимо лишь засвидетельствовать наличие пересечения (точка в пересечении), если многогранники действительно пересекаются, то мы вправе ожидать более быстрого решения. Добкин и Киркпатрик в работе [104] дают для этой задачи алгоритм со сложностью $O(n)$. В этой же работе они указывают на алгоритм, разработанный независимо Дайером и имеющий также линейную временну́ю сложность. Если выполнить предобработку многогранников, то может быть получено решение, сложность которого есть некоторый полином от логарифма раз-

мера задачи [82, 103, 105]. Аналогичные утверждения могут быть сделаны и относительно задачи обнаружения пересечения выпуклых многоугольников. В работах [2, 57] приведены другие методы обнаружения пересечения между твердыми телами.

Задача 3.2.11. Построение пересечения полупространств. В трехмерном пространстве заданы n полупространств. Найти их пересечение.

Эта задача со всей очевидностью может быть решена методом «разделяй и властвуй» за время $O(n \log^2 n)$, так как шаг соединения решений по сути есть задача 3.2.9, которая может быть решена за время $O(n \log n)$. Препарата и Маллер [294] использовали метод геометрического преобразования и алгоритм отделяющей полуплоскости (см. задачу 3.5.2) для получения оптимального алгоритма решения этой задачи, имеющего сложность $O(n \log n)$.

Задача 3.2.12. Перечисление пересечений прямоугольников. Заданы n изотетичных прямоугольников, т. е. прямоугольников, стороны которых параллельны осям координат. Найти все k пар пересекающихся прямоугольников.

Эта задача возникает при проектировании СБИС. Каждый прямоугольник используется для моделирования компоненты цепи и при этом необходимо придерживаться определенных правил конструирования [24, 35, 46, 126, 207, 250, 251, 320]. Оптимальный по времени алгоритм, имеющий временну́ю сложность $O(n \log n + k)$ и емкостную сложность $O(n)$, был независимо получен Мак-Крейтом [250] и Эделсбруннером [123]. Оба они использовали метод заметания плоскости в сочетании с новой структурой данных, называемой *деревом интервалов*, для поддержания статуса заметающей прямой. Те же самые оценки по времени и памяти могут быть достигнуты при использовании метода «разделяй и властвуй» [174, 220]. Используя *дерево отрезков* [28, 292], Чазелле и Инчерпи [87] также разработали алгоритм, имеющий те же оценки сложности. Более того, метод, называемый методом *распутывания* деревьев отрезков, рассмотренный в работе [87], может быть обобщен на случай пространств более высокой размерности, как об этом говорится ниже. Методом преобразования этой задачи в пакет запросов, вставок и удалений Эделсбруннер и Овермарс [136] также получили аналогичные результаты.

Задача 3.2.13. Перечисление пересечений d-мерных параллелепипедов. Заданы n изотетичных d-мерных параллелепипедов в d-мерном пространстве, $d > 2$. Найти все k пар пересекающихся d-мерных параллелепипедов.

Сикс и Вуд получили алгоритм, имеющий временну́ю и емкостную сложности $O(n \log^{d-1} n + k)$ и $O(n \log^{d-1} n)$ соответственно [321]. Позднее Эделсбруннер улучшил временну́ю оценку этого алгоритма до $O(n \log^{d-2} n)$ [126]. В пределах той же оценки времени выполнения алгоритма Чазелле и Инчерпи [187] и Эделсбруннер и Овермарс [136] снизили емкостную сложность алгоритма до $O(n)$, что является оптимальным.

Задача 3.2.14. Подсчет числа пересечений d-мерных параллелепипедов. Заданы n изотетичных d-мерных параллелепипедов в d-мерном пространстве, $d \geqslant 1$. Найти число пересекающихся пар.

В отличие от задачи подсчета числа пересечений отрезков эта задача может быть решена за время $O(n \log^{d-1} n)$ при объеме памяти $O(n \log^{d-2} n)$ путем незначительного изменения алгоритма решения задачи перечисления пересечений [321]. Отметим, что алгоритм, приведенный в работе [87], не может быть приспособлен для эффективного решения задачи подсчета числа пересечений.

Задача 3.2.15. Перечисление включений прямоугольников. Заданы n изотетичных прямоугольников. Найти все k пар прямоугольников, таких, что один включает другой.

Впервые эта задача была изучена в работе [336], в которой сообщалось об алгоритме, имеющем временну́ю и емкостную сложности $O(n \log^2 n + k)$ и $O(n \log^2 n)$ соответственно. Ли и Вонг [234] и независимо от них Эделсбруннер [122] получили тот же самый результат, используя геометрическое преобразование, которое отображает задачу для d-мерного случая в задачу для $2d$-мерного случая при $d \geqslant 1$. Позднее Ли и Препарата [228] использовали метод «разделяй и властвуй», что позволило улучшить оценку требуемой памяти до $O(n)$. Было показано, что эта задача эквивалентна четырехмерной задаче о доминировании [135, 228] (ср. разд. II-C).

Задача 3.2.16. Обнаружение включения многоугольника. Заданы два многоугольника P и Q, имеющие m и n вершин соответственно. При условии что допускается перенос и вращение многоугольников, определить, включает ли многоугольник Q многоугольник P.

Чазелле [71] разработал несколько алгоритмов решения этой задачи для случая многоугольников общего вида, выпуклых многоугольников и т. д. Если как P, так и Q являются многоугольниками общего вида, то задача может быть решена за время $O(m^3 n^3 (m+n) \log(m+n))$, а в случае, когда Q — выпуклый многоугольник, задача может быть решена за время $O(mn^2)$.

Задача 3.2.17. Видимость многоугольника из точки. На плоскости заданы множество непересекающихся многоугольников и некоторая точка q. Найти участки границы многоугольников, видимые из точки q.

Это по сути дела задача удаления невидимых линий, возникающая в машинной графике. Задача удаления невидимых линий или невидимых поверхностей интенсивно изучалась в целом ряде работ [65, 152, 153, 159, 326]. Если множество состоит из единственного простого многоугольника, то для этого случая известны по крайней мере два алгоритма, имеющие линейную временну́ю сложность [143, 218]. Используемый при этом метод аналогичен методу сканирования Грэхэма в том плане, что сначала определяется некоторая точка, видимая из q, а затем при помощи свойства простоты многоугольника организуется просмотр вершин многоугольника P и при этом те участки границы P, которые не видны из q, удаляются. В случае когда множество состоит из m непересекающихся выпуклых многоугольников с общим числом ребер, равным n, эта задача может быть решена за время $O(m \log n + F)$, где F — размер выходных данных [221]. В работе Эделсбруннера и др. [138] также изучается эта задача. В этой же работе обсуждается задача видимости многоугольников и в случае, когда допускается добавление или исключение многоугольников, а также вопрос изменения видимой части границы многоугольников при изменении направления взгляда или когда допускается перемещение точки зрения (наблюдения).

Задача 3.2.18. Видимость многоугольника с ребра. Заданы простой многоугольник P с n вершинами и некоторое ребро многоугольника P. Найти часть границы многоугольника P, видимую с ребра e. (Точка q, принадлежащая P, считается *видимой с ребра* e, если существует точка r, лежащая на ребре e, такая, что отрезок q, r не пересекает границу многоугольника P.)

Задача видимости с ребра впервые была изучена Ави и Туссеном [22]. Они предложили алгоритм со сложностью $O(n)$ для определения видимости многоугольника P с ребра e (в [22] для этого используется термин *слабая видимость*). В работе [22] показано, что граница многоугольника P видима с ребра e тогда и только тогда, когда внутреняя часть P видима с ребра e, и вместе с тем задача определения видимости многоугольника за время $O(n)$ отмечена как открытая. Алгоритм со сложностью $O(n \log n)$ был независимо предложен Эль Гинди [142] и Ли и Лином [223]. Чазелле и Гуибас [85], используя теорему о разрезании многоугольника [70], также получили алгоритм, имеющий временну́ю сложность $O(n \log n)$.

Имеется ряд других задач, связанных с вычислением пло-

щади, периметра, нахождением контура или числа связных компонент объединения изотетичных прямоугольников или других объектов, таких, как квадраты или круги [87, 134, 172, 178, 179, 182, 183, 239—241, 323, 342]. Однако исследования пересечений между множествами объектов не получили должного внимания. Например, пусть заданы два множества отрезков и требуется найти все пары пересекающихся отрезков, таких, что оба отрезка не принадлежат одному и тому же множеству. Недавняя статья Мэрсона и Столфи [246] содержит оптимальный алгоритм решения этой задачи, имеющий временну́ю и емкостную сложности $O(n \log n + k)$ и $O(n)$ соответственно, в предположении, что никакая пара отрезков, принадлежащих одному и тому же множеству, не пересекается. Таким образом, отсюда следует [246], что пересечение двух простых многоугольников может быть найдено за время $O(n \log n + k)$.

C. Геометрические задачи поиска

В этом разделе мы представим ряд геометрических задач поиска. Задача *поиска* определяется *запросом* к некоторой базе данных и *процедурой выбора ответа в базе данных*. База данных представляет набор геометрических объектов определенного вида и обычно организована в виде некоторой структуры, чтобы облегчить процесс поиска. В соответствии с классификацией, предложенной в [295], имеются два типа запросов: *однократные* и *многократные*. В зависимости от того, является ли база данных фиксированной или изменяется на протяжении времени работы с ней, мы имеем два типа организации базы данных: *статическую* и *динамическую* соответственно. Однократные запросы менее интересны, чем многократные. Мы имеем четыре меры стоимости, зависящие от размера базы данных n и размера ответа на запрос F.

1) Время ответа $Q(n, F)$ — время, необходимое для ответа на запрос.

2) Объем памяти $S(n)$ — объем памяти, необходимой для представления структурированной базы данных.

3) Время предобработки $P(n)$ — время, необходимое для организации базы данных в форме, наиболее удобной для поиска.

4) Время перестройки — время, необходимое для вставки $I(n)$ и удаления $D(n)$ элементов. Эти меры имеют смысл только для динамических баз данных. Если $I(n) = \theta(D(n))$, то мы полагаем, что время перестройки есть $U(n) = O(I(n)) = O(D(n))$.

Рассматриваемые далее задачи формулируются для случая двумерного пространства. При необходимости будут упоминать-

ся обобщения на случай d-мерных пространств. В этом случае указанные меры стоимости будут иметь индекс d.

Задача 3.3.1. Интервальный поиск с подсчетом. На плоскости заданы n точек. Найти число точек, расположенных в заданном (в запросе) прямоугольнике, определяемом как декартово произведение интервалов $(a_1, a_2) \times (b_1, b_2)$. Это значит, что необходимо найти число v точек $p = (x, y)$, таких, что $a_1 \leqslant x \leqslant a_2$, $b_1 \leqslant y \leqslant b_2$. (Отметим, что размер ответа на запрос F определяется единственным целым числом.)

Эта задача может быть решена методом геометрического места точек, обсуждавшимся в разд. II-В. Положим, что вершины A, B, C и D заданного в запросе прямоугольника имеют координаты (a_1, b_2), (a_1, b_1), (a_2, b_1) и (a_2, b_2) соответственно, и обозначим через $\mathrm{Dom}(q)$ число точек, над которыми доминирует точка q. Так как число точек, попадающих в заданный прямоугольник, равно $\mathrm{Dom}(D) - \mathrm{Dom}(A) - \mathrm{Dom}(C) + \mathrm{Dom}(B)$, то для решения задачи достаточно четыре раза выполнить процедуру поиска с тем, чтобы определить положение каждой из вершин прямоугольника среди $O(n^2)$ *клеток*, на которые разбивается плоскость исходными точками. (Положение точки на плоскости определяется в результате *двукратного* выполнения процедуры бинарного поиска: один раз для определения вертикальной полосы, в которой находится точка, и второй раз для определения горизонтальной полосы.) Таким образом, мы имеем $Q(n) = O(\log n)$, $S(n) = P(n) = O(n^2)$. В d-мерном пространстве метод геометрического места точек, или метод разбиения на клетки, может быть естественным образом обобщен, что дает следующий результат:

$$Q_d(n) = O(\log n) \quad \text{и} \quad S_d(n) = P_d(n) = O(n^d).$$

Для решения задачи интервального поиска Бентли ввел структуру данных, названную *деревом интервалов*. Используя эту структуру, Люкер и Виллард [244, 344, 347], Ли и Вонг [233] и Бентли и Шамос [41] сумели получить следующий результат для задачи подсчета числа точек при интервальном поиске в случае d-мерного пространства: $d \geqslant 2$, $Q_d(n) = O(\log^d n)$, $P_d(n) = S_d(n) = O(n \log^{d-1} n)$. Структура дерева интервалов будет описана ниже.

Задача 3.3.2. Перечисление точек при интервальном поиске. На плоскости заданы n точек. Перечислить все точки, попадающие в заданный (в запросе) прямоугольник. (Запрос делается в такой же форме, что и в задаче 3.3.1.)

Эта задача имеет очевидное приложение к системам баз данных. В базе данных, содержащей записи о служащих неко-

торой компании, каждая запись может иметь несколько атрибутов, таких, как возраст, жалованье и т. д., и может рассматриваться как точка в d-мерном пространстве, в котором каждый атрибут соответствует измерению, а число измерений пространства d равно числу атрибутов. Типичная задача интервального поиска для двух измерений заключается в выявлении всех служащих, чьи возраст и жалованье находятся в заданных интервалах. В этой области выполнен большой ряд исследований. В работе Бентли и Фридмена [34], содержащей обзор алгоритмов и структур данных для интервального поиска, описывается состояние дел на 1979 г. Решение этой задачи, а также ее варианта, касающегося подсчета числа точек, полученное Виллардом [346], основано на использовании дерева интервалов; имеем следующие характеристики:

$$Q_d(n, F) = O(\log^{d-1} n + F), \quad P_d(n) = S_d(n) = O(n \log^{d-1} n).$$

Другие методы, имеющие те же самые оценки, приведены в работе [158]. Позднее оценка необходимого объема памяти была улучшена Чазелле на множитель $\log \log n$ [74]. Однако это улучшение имеет место только для задачи перечисления точек.

Дерево интервалов по своей форме напоминает «пирамиду», и обычно о нем говорят как о дереве деревьев. Мы начнем со структуры для одномерного случая, а затем рекурсивно определим деревья для случая d-мерных пространств, основываясь при этом на $(d-1)$-мерном случае. Одномерное дерево интервалов — это упорядоченный массив, т. е. массив или список записей, упорядоченный в порядке возрастания значений первой координаты. Дерево интервалов для двумерного случая — это обычное сбалансированное дерево бинарного поиска, организованное в соответствии со *второй координатой* каждой записи. Каждому листу дерева соответствует одна запись, а каждому узлу — записи в его поддереве. Кроме того, к каждому узлу присоединено одномерное дерево интервалов, организующее записи, соответствующие узлу, в зависимости от их *первой координаты*. Отсюда видно, что n записей на уровне i примерно равномерно распределены между 2^i узлами. Это распределение распространяется примерно на $\log_2 n$ уровней и подходящим образом заканчивается, когда множество записей становится настолько маленьким, что все они могут быть без затруднений просмотрены методом «грубой силы». Эта же идея обобщается на случай пространств более высокой размерности, так что в случае d-мерного пространства мы имеем сбалансированное дерево бинарного поиска по координате с номером d, а каждый узел связан с $(d-1)$-мерным деревом интервалов для $(d-1)$-мерных записей, соответствующих узлу.

Алгоритм поиска по дереву интервалов является рекурсив-

ным, и без потери общности мы опишем его для случая двух измерений. Каждый узел в дереве представляет некоторый интервал по y-координате. При прохождении узла мы прежде всего сравниваем y-интервал запроса с y-интервалом узла. Если y-интервал узла целиком попадает в y-интервал запроса, то мы осуществляем поиск в упорядоченном массиве, запоминаемом в узле, для обнаружения всех точек, попадающих в x-интервал запроса. Если y-интервал запроса целиком находится ниже величины, с которой производится сравнение в узле, то мы рекурсивно проходим левое поддерево. Если y-интервал запроса целиком находится выше величины, с которой производится сравнение в узле, то мы рекурсивно проходим правое поддерево. В противном случае (y-интервал запроса содержит величину, с которой производится сравнение) мы проходим оба поддерева.

Анализ планарного дерева интервалов довольно сложен. Так как имеются $\log_2 n$ уровней и каждый уровень содержит n точек, то суммарный объем требуемой памяти составляет $O(n \log n)$. (Предобработка также может быть выполнена за время $O(n \log n)$. Что касается времени ответа, то анализ показывает, что на каждом уровне дерева производится поиск не более чем в двух упорядоченных массивах, на что в каждом случае тратится время $O(\log n)$, поэтому суммарные затраты составляют $O(\log^2 n)$ плюс время на выборку ответа. Таким образом, мы имеем

$$P(n) = S(n) = O(n \log n) \text{ и } Q(n, F) = O(\log^2 n + F).$$

Обобщая приведенные выше аргументы, для d-мерной задачи перечисления точек при интервальном поиске получаем следующее:

$$P_d(n) = S_d(n) = O(n \log^{d-1} n) \text{ и } Q_d(n, F) = O(\log^d n + F).$$

Тщательное исследование позволяет улучшить время ответа на запрос на множитель $\log n$. Обращаясь вновь к двумерному случаю, легко сообразить, что имеется существенная избыточность при поиске в упорядоченных массивах для x-координат, так как множество каждого узла является подмножеством множеств его предков. Имея в виду это соображение, массивы всех узлов, кроме корня, заменяются списками. Интервальный поиск по x-координате выполняется исключительно в одномерной структуре, связанной с корнем дерева, а положение в каждом потомке задается указателями. При таком способе организации может быть получена следующая оценка времени ответа на запрос: $Q_d(n, F) = O(\log^{d-1} n + F)$ [344, 346, 347].

Описание других структур данных, используемых для решения задачи перечисления точек при интервальном поиске, может быть найдено в работах [27, 37, 43, 231].

Отметим, что структуры данных, обсуждавшиеся выше, не позволяют делать вставки и исключения записей. Однако, используя метод динамизации (ср. разд. II-G), дерево интервалов можно адаптировать для работы в динамических условиях, так как задачи интервального поиска допускают декомпозицию в смысле Бентли [29]. Если допускаются только вставки, начиная с пустой базы данных, то, как показано в работах [39, 304], могут быть достигнуты следующие характеристики:

$$P_d(n) = O(n \log^d n), \quad S_d(n) = O(n \log^{d-1} n) \text{ и}$$
$$Q_d(n, F) = O(\log^{d+1} n + F),$$

где n — текущее количество выполненных вставок. Люкер и Виллард [244] улучшили время ответа на запрос на множитель $\log n$, сохранив неизменными две другие меры даже в том случае, когда допускаются исключения записей. В работе [347] показано, как можно обеспечить быстрое выполнение каждой отдельной операции по перестройке структуры, а не только последовательности таких операций. В частности, могут быть получены следующие характеристики: $Q_d(n, F) = O(\log^d n + F)$, $S_d(n) = O(n \log^{d-1} n)$, а время вставки и исключения записей при этом равны $I_d(n) = O(\log^d n)$ и $D_d(n) = I_d(n)/\log n$ соответственно [283]. Увеличив время операции исключения на множитель $\log n$, Эделсбруннеру удалось уменьшить время ответа на запрос на множитель $\log n$ [125].

С использованием метода динамизации были получены и некоторые другие результаты с иными показателями (время ответа на запрос)/(требуемая память) или (время ответа на запрос)/(время на перестройку). (Соответствующие ссылки приведены в разд. II-G.) Фридмен на некоторой ограниченной модели показал, что $\Omega(n \log^d n)$ является нижней оценкой сложности выполнения последовательности из n операций перестройки структуры базы данных или выбора ответа на запрос [151]. Болоур описал метод хеширования [52], который он использовал вместо поиска по древовидным структурам в задаче интервального поиска. Применение этого метода позволило получить довольно быстрые в среднем решения задачи интервального поиска при условии, что область запросов находится в заранее определенных границах.

Задача 3.3.3. Перечисление точек в многоугольнике. На плоскости заданы n точек. Найти все точки, находящиеся в заданном в запросе многоугольнике с k сторонами. Допускается предобработка.

Это довольно общая задача поиска. Виллард [345] разработал структуру данных, названную ***деревом многоугольников***,

и показал, что данная задача может быть решена за время $Q(n, F) = O(kn^{0.77} + F)$ и $P(n) = O(n^2)$ в худшем случае (время предобработки можно уменьшить до $P(n) = O(n \log^2 n)$ в среднем случае). Необходимая при этом память $S(n) = O(n)$. В случае поиска с подсчетом числа точек время, достаточное для ответа на запрос, равно $O(kn^{0.77})$. При использовании новой структуры данных, названной деревом соединений [141], эти результаты были улучшены до $Q(n, F) = O(kn^{0.695} + F)$ и $O(n^{0.695})$ для задач перечисления и подсчета соответственно.

Интересное упрощение данной задачи представляет *задача перечисления точек в полуплоскости* [140], в которой многоугольник вырождается в полуплоскость. Среди результатов, полученных для этой задачи, следует отметить следующие: $S(n) = O(n^3)$, $Q(n, F) = O(\log n + F)$ [131], $S(n) = O(n)$, $Q(n) = O(n^{0.695} + F)$ [141] и, конечно, результат, полученный в работе [345]. Самый последний результат [86], основанный на сочетании идеи геометрических преобразований и выпуклых слоев (задача 3.1.8), показывает, что задача может быть решена за оптимальное время $Q(n) = O(\log n + F)$ с $S(n) = O(n)$ и $P(n) = O(n \log n)$. Однако метод, примененный в [86], не может быть использован для решения соответствующей задачи подсчета числа точек с сохранением тех же самых оценок. Этот вопрос остается открытым. Используя дерево октантов, Яо [353] получил для задачи перечисления точек в полуплоскости решение с $S(n) = O(n)$ и $Q(n, F) = O(n^{0.93} + F)$. Позднее время ответа на запрос улучшили до $O(n^{0.916})$ Добкин и Эделсбруннер [101]. При объеме памяти $O(n^4)$ задача может быть решена за время $O(\log n + F)$ [95]. В действительности Коул и Яп [95] показали, что при объеме пространства $O(dn^{2^{d-1}})$ время $O(2^d \log n)$ оказывается достаточным.

Задача 3.3.4. Перечисление точек в круге фиксированного радиуса. На плоскости заданы n точек. Найти все точки, попадающие в круг, радиус которого фиксирован, а положение центра может быть произвольным. Допускается предобработка.

Эта задача известна так же, как задача поиска соседей в пределах фиксированного радиуса. Используя метод геометрического места точек, Бентли и Маурер [36] разработали алгоритм со следующими характеристиками: $Q(n, F) = O(\log n + F)$, $P(n) = S(n) = O(n^3)$. Чазелле [73] улучшил как время предобработки, так и требуемый объем памяти, получив для них оценку $O(n^2 \log n)$. Оценка необходимого объема памяти была впоследствии улучшена до $O(n^2)$ [128]. Совсем недавно Чазелле и Эделсбруннер [84] сообщили о разработке оптимального (по памяти $O(n)$ и времени $O(\log n + F)$) алгоритма решения данной задачи, при этом время предобработки составляет $O(n^2)$.

Задача 3.3.5. Перечисление точек в круге переменного радиуса. На плоскости заданы n точек. Найти все точки, попадающие в круг произвольного радиуса и с произвольным расположением центра. Допускается предобработка.

Яо разработал алгоритм с временем ответа на запрос, равным $O(n^{0.98}+F)$, линейной оценкой требуемой памяти и временем предобработки $O(n^4)$ [353] — первый алгоритм, имеющий сложность $o(n)$ в худшем случае. Коул и Яп [95] получили алгоритм с оценками требуемого объема памяти и времени выполнения $O(n\log^3 n)$ и $O(\log n+F)$ соответственно. Оценка для объема памяти была улучшена до $O(n(\log n\log n)^2)$ [80].

В рассмотренной выше задаче интервального поиска объекты в базе данных представляли точки пространства. Интересные задачи интервального поиска возникают в случае, когда объекты имеют более сложную природу, как, например, прямые отрезки или многоугольники. Ниже мы рассмотрим эти важные обобщения.

Задача 3.3.6. Интервальный поиск с перечислением в множестве отрезков. На плоскости задано множество из n отрезков. Найти все отрезки, имеющие непустое пересечение с заданным прямоугольником.

В машинной графике эта задача известна под названием обрезания по окну [268]. Овермарс [277] и Эделсбруннер с соавторами [137] получили элегантное решение этой задачи, разрешив при этом даже перестройку базы данных. Решение имеет следующие характеристики:

$$Q(n,F)=O(\log^2 n+F),\quad U(n)=O(\log^2 n)\quad \text{и}\quad S(n)=O(n\log n).$$

Если окно двигается в некотором фиксированном направлении, параллельном одной из координатных осей, то отрезки, статус которых по отношению к окну изменился, могут быть определены за время $Q(n,k)=O(\log^2 n+k)$, где k — суммарное число таких отрезков.

Задача 3.3.7. Поиск пересечения ортогональных объектов. На плоскости задано множество из n ортогональных объектов. Найти все объекты, пересекающие заданный ортогональный объект. (*Ортогональный* объект размерности d представляет собой декартово произведение d интервалов, каждый из которых может вырождаться в точку. Например, точка, изотетичный прямоугольник и вертикальный или горизонтальный отрезок являются ортогональными объектами.)

Этот класс задач поиска включает задачи 3.3.1 и 3.3.2. *Обратный интервальный поиск*, или задача *об охвате точки*, также принадлежит этому классу. В этой задаче требуется в заданном

множестве из n изотетичных прямоугольников найти все прямоугольники, охватывающие заданную (в запросе) точку. Вайшнави [335] предлагает структуру данных, позволяющую осуществлять поиск с временем ответа на запрос $O(\log n + F)$ и с $P(n) = S(n) = O(n \log^2 n)$. Чазелле [74] дает оптимальный алгоритм решения этой задачи, требующий $O(n)$ памяти, время ответа на запрос которого равно $O(\log n + F)$. Овермарс и ван Леувен [279, 282], используя метод динамизации, показали, что динамическая задача об охвате точки может быть решена за время

$$Q(n, F) = O(\log^3 n + F)$$

с $I(n) = O(\log^3 n)$, $D(n) = O(\log^2 n)$ и $S(n) = O(n \log^2 n)$.

Задача *поиска пересечений ортогональных отрезков*, в которой требуется найти все отрезки из заданного множества, содержащего n горизонтальных и вертикальных отрезков, пересекающие заданный ортогональный отрезок, исследовалась Вайшнави и Вудом [337]. Они предложили алгоритм со временем ответа на запрос $O(\log n + F)$ и временем предобработки и памятью $O(n \log n)$. Оценка для памяти может быть уменьшена до $O(n)$ [74]. Для случая когда множество различных значений координат имеет мощность $O(n)$ и допускается добавление и исключение отрезков. Мак-Крейт [251] предложил динамическую структуру данных, использование которой для решения данной задачи требует $O(n)$ памяти и при этом

$$Q(n, F) = O(\log^2 n + F) \quad \text{и} \quad U(n) = O(\log^2 n).$$

Липский и Пападимитриу [239] разработали алгоритм, имеющий

$$Q(n, F) = O(\log n \log\log n + F),$$

$$U(n) = O(\log n \log\log n) \quad \text{и} \quad S(n) = O(n \log n).$$

Для общей динамической задачи Эделсбруннер [124] дал алгоритм с

$$Q(n, F) = O(\log^2 n + F), \quad U(n) = O(\log^2 n) \quad \text{и} \quad S(n) = O(n \log n).$$

Задача *поиска пересечений прямоугольников* касается изотетичных прямоугольников и рассматривается в работах Ли и Вонга [234] и Эделсбруннера [122, 123]. Преобразуя эту задачу для случая d-мерного пространства в задачу интервального поиска с перечислением в $2d$-мерном пространстве, Ли и Вонг [234] разработали алгоритм, имеющий

$$Q_d(n, F) = O(\log^{2d-1} n + F), \quad P_d(n) = S_d(n) = O(n \log^{2d-1} n).$$

Эделсбруннер [122, 123] обобщил свои результаты о перечислении всех пар пересекающихся прямоугольников (ср. с за-

дачей 3.2.12) на случай d-мерного пространства и улучшил оценки для времени предобработки и требуемой памяти, полученные в работе [234], получив

$$P_d(n) = O(n \log^d n) \quad \text{и} \quad S_d(n) = O(n \log^{d-1} n).$$

Совсем недавно Эделсбруннер и Маурер [129] объединили все предыдущие подходы к решению этого класса задач поиска пересечений и получили следующие результаты. Для статического варианта задачи имеется структура данных, использование которой позволяет достичь следующих характеристик:

$$Q_d(n, F) = O(\log^{d-1} n + F) \quad \text{и} \quad P_d(n) = S_d(n) = O(n \log^d n).$$

Оценка требуемой памяти улучшена до $O(n \log^{d-1} n/\log \log n)$ [85]. Для динамического варианта задачи имеется динамическая структура данных, позволяющая достичь следующих характеристик:

$$Q_d(n, F) = O(\log^d n + F),$$
$$S_d(n) = O(n \log^d n) \quad \text{и} \quad U_d(n) = O(\log^d n).$$

Более подробное обсуждение содержится также в работах [124, 158].

Задача 3.3.8. Нахождение множества объектов и нахождение числа объектов. В пространстве задано множество, состоящее из n объектов, и некоторый запрашиваемый объект — объект, входящий в запрос. Необходимо перечислить множество объектов, пересекающих запрашиваемый объект (нахождение множества), или просто найти мощность этого множества (нахождение числа объектов) [173].

Выбор такого экзотического названия[1]) связан с двумерным вариантом задачи, когда объекты (например, многоугольники) лежат в плоскости, а запрашиваемый объект является точкой, ассоциируемой с «иглой», перпендикулярной плоскости. Если объекты ортогональны, то мы вновь приходим к задачам перечисления пересечений и подсчета пересечений ортогональных объектов соответственно. В работе [131] даны общие решения задач нахождения множества объектов и нахождения числа объектов, для которых $Q(n, F) = O(\log n + F)$ и $Q(n) = O(\log n)$ соответственно. Но при этом стоимость и время предобработки оказались очень большими. В одномерном пространстве, когда объекты — интервалы, а запрашиваемый объект — точка, были получены оптимальные решения, время ответа на запрос для которых равно $O(\log n + F)$ в случае за-

[1]) В оригинале используется термин stabbing — накалывание, переведенный как «нахождение». — *Прим. перев.*

дачи нахождения множества объектов [74, 122, 250] и $O(\log n)$ в случае задачи нахождения числа объектов [129, 164].

Некоторые свойства этой задачи в настоящее время продолжают исследоваться. Например, задача нахождения числа объектов для множества из n многоугольников, стороны которых имеют конечное постоянное множество направлений ориентации, может быть решена с временем ответа на вопрос, равным $O(\log n)$, и оценкой $O(n \log n)$ для времени предобработки и необходимой памяти [173]. Эделсбруннер с соавторами [132] разработали алгоритм нахождения трансверсальной прямой, которая пересекает каждый из n заданных отрезков. Алгоритм имеет сложность $O(n \log n)$ и требует $O(n)$ памяти. В работе также приведен алгоритм определения, является ли некоторая заданная прямая трансверсальной, имеющий сложность $O(\log n)$. Задачи нахождения того, какие отрезки или сколько отрезков пересекают заданный отрезок, и задача нахождения того, какие или сколько многоугольников с ограниченным числом сторон содержат заданную точку, могут быть решены за время $O(n^{0.695})$ [102]. В работе [74] представлен алгоритм перечисления отрезков, пересекающих заданный отрезок, имеющий следующие характеристики:

$$P(n) = O(n^2 \log n), \quad S(n) = O(n^2) \quad \text{и} \quad Q(n, F) = O(\log n + F).$$

Задача 3.3.9. Поиск пересечений многоугольников. Задано множество простых многоугольников, каждый из которых имеет ограниченное число ребер. Найти многоугольники, имеющие непустое пересечение с некоторым запрашиваемым многоугольником того же типа.

Это наиболее общая задача поиска пересечений, для которой большинство из приведенных ранее задач на плоскости являются частными случаями. Эта задача путем применения подходящих преобразований [131] может быть сведена к трем подзадачам, каждая из которых является обобщением своего двойника в задаче поиска пересечений ортогональных объектов (задача 3.3.7), т. е. обратной задачи интервального поиска, задачи поиска пересечений ортогональных отрезков и задачи интервального поиска.

Эти три подзадачи следующие: (i) задана некоторая точка; требуется найти множество многоугольников, охватывающих эту точку; (ii) задан отрезок и требуется найти множество пересекающихся с ним отрезков и (iii) задан многоугольник и требуется найти все точки, попадающие в него. Задача (i) может быть решена методом определения положения точки (ср. с задачей 3.3.10, приведенной ниже), задача (ii) — методом геометрического преобразования, а задача (iii) — в результате ответа на ограниченное число запросов относительно принадлеж-

ности *точки некоторому треугольнику*. В целом на это требуется время $O(\log n + F)$. При этом стоимость предобработки и необходимой памяти может доходить до $O(n^7)$ (131). Недавно Добкин и Эделсбруннер [102], изучив эту задачу, получили почти линейный алгоритм.

Задача 3.3.10. Положение точки. Задано разбиение плоскости, содержащее n ребер. Найти область разбиения, содержащую заданную точку. (Разбиение плоскости можно рассматривать как совокупность многоугольников, и мы ищем многоугольник, имеющий непустое пересечение с заданной точкой.)

Эту задачу следует рассматривать как одну из фундаментальных задач поиска в области вычислительной геометрии. Она возникает во многих областях науки. Так, например, при классификации образов желательно соотнести заданный образ с одним из классов некоторой конечной совокупности классов. Образы отображаются в точки некоторого пространства, которое разбито на области, каждая из которых соответствует конкретному классу. Классификация осуществляется путем определения области, которой принадлежит классифицируемый образ, и название соответствующего класса и будет ответом.

Добкин и Липтон [106] были, по-видимому, первыми, кто предложил алгоритм со сложностью $O(\log n)$ для определения положения точки в разбиении многомерного пространства на области [297]. Их метод основан на идее разбиения пространства на слои (так называемый *метод слоев*), в двумерном случае это будут полосы; наиболее хорошо он описан для двумерного случая (см. также [295, 315]). Обобщение метода Добкина — Липтона [106] содержится в работе [78]. Предположим, что имеется разбиение плоскости, каждое ребро которого является отрезком прямой. Получившийся граф называется *плоским прямолинейным графом* или сокращенно ППГ [295]. Предположим для простоты, что никакие две вершины графа не имеют одинаковых значений y-координаты, и проведем через каждую вершину горизонтальную прямую. Две такие последовательные прямые образуют полосу (слой), внутри которой никакие два ребра ППГ не пересекаются (рис. 4). Заметим, что внутри каждой полосы множество ребер является полностью упорядоченным. Задача определения положения точки может быть решена в результате двукратного применения процедуры бинарного поиска — один раз для определения полосы, которой принадлежит заданная точка, и второй раз для определения положения точки внутри полосы. Полное время поиска равно $O(\log n)$. Каждая полоса представляется с помощью бинарного дерева поиска с общим объемом памяти $O(n^2)$. Предобработка также может быть выполнена за время $O(n^2)$ [295]. Обобщение

этого метода на случай пространств более высокой размерности очевидно.

Однако, учитывая довольно большую стоимость предобработки и используемой памяти, впоследствии предложили несколько улучшений метода. Метод цепей, разработанный Ли и Препаратой [225], имеет время выполнения $Q(n)=O(\log^2 n)$ и при этом $P(n)=O(n\log n)$ и $S(n)=O(n)$. Липтон и Тарьян [242] предложили чрезвычайно искусно разработанный алгоритм, основанный на теореме о планарной отделимости и достигающий оптимальных характеристик, т. е.

$$Q(n)=O(\log n),$$
$$P(n)=O(n\log n),$$
$$S(n)=O(n).$$

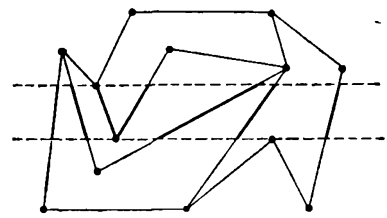


Рис. 4. Внутри полосы никакие два отрезка не пересекаются.

К сожалению, метод Липтона — Тарьяна представляет только теоретический интерес. Позднее Препарата [292] предложил новую схему, известную теперь как *метод трапецоидов, управляемый медианой*, который решает эту задачу, давая оптимальное время ответа на запрос, т. е. $O(\log n)$, но при этом требуется $P(n)=S(n)=O(n\log n)$.

Киркпатрик [197] использовал триангуляции для получения иерархического представления ППГ с $O(\log n)$-уровнями триангуляций, каждый из которых является уточнением другого уровня. Это позволило получить более практичный оптимальный алгоритм со временем ответа на запрос $O(\log n)$, временем предобработки $O(n\log n)$ и объемом необходимой памяти $O(n)$. Все приведенные выше методы, за исключением метода Киркпатрика, могут обрабатывать планарные разбиения с криволинейными ребрами определенного вида. Другой алгоритм с аналогичными возможностями был предложен Эделсбруннером и Маурером [130] и имеет следующие характеристики:

$$Q(n)=O(\log^3 n),\quad P(n)=O(n\log n)\quad \text{и}\quad S(n)=O(n).$$

Недавнее сообщение Эдахиро и др. [119] содержит всестороннее сравнение, включая действительные времена выполнения рассмотренных выше алгоритмов определения положения точки. Недавно был предложен новый оптимальный метод [128], возможно самый практичный из имеющихся на сегодня. Ключевая идея метода состоит в адаптации философии выделения слоев [346] с улучшенной оценкой используемой памяти $O(n)$ [74]

к методу цепей Ли — Препараты [225]. Чазелле получил алгоритм определения положения точки в трехмерном комплексе с $O(n)$ вершинами, имеющий временну́ю сложность $O(\log^2 n)$ и требующий $O(n)$ памяти.

D. Близость и связанные задачи

Геометрические объекты, такие, как точки и окружности, используются для моделирования физических объектов реального мира. В некоторых случаях нам хотелось бы иметь доступ к соответствующим соседям этих объектов. Например, при управлении движением самолетов мы хотим следить за двумя наиболее близкими друг к другу самолетами. При моделировании самолетов движущимися в пространстве точками мы хотим в каждый конкретный момент времени находить пару наиболее близких друг к другу точек. Сначала перечислим ряд задач, причем некоторые из них могут показаться не относящимися к делу, а затем опишем некоторую геометрическую конструкцию, называемую *диаграммой Вороного*, которая может быть использована для решения этих задач в пределах временны́х затрат, имеющих тот же самый порядок, что и затраты на построение диаграммы. Далее приведены некоторые задачи, связанные с близостью.

1. ОСНОВНЫЕ ЗАДАЧИ, СВЯЗАННЫЕ С БЛИЗОСТЬЮ

Задача 3.4.1. Ближайшая пара. На плоскости заданы n точек. Найти две наиболее близкие друг к другу точки.

Очевидно, что задача, являющаяся обобщением этой задачи на k-мерный случай, $k \geqslant 1$, может быть решена за время $O(kn^2)$ путем сравнения расстояний между каждой парой точек. В одномерном случае мы можем решить эту задачу проще за время $O(n \log n)$, упорядочив предварительно заданные точки. Оказывается, что сортировку нельзя обобщить на случай пространств более высокой размерности. Используя метод «разделяй и властвуй», Бентли и Шамос [40] показали, что для решения этой задачи в k-мерном случае ($k \geqslant 1$) время $O(n \log n)$ является достаточным, а указанная оценка оптимальна (см. разд. III-F). В работе [45] приведено исследование этой задачи в среднем случае, а также проиллюстрирован оптимальный в среднем случае алгоритм. Другие относящиеся к данной задаче результаты содержатся в работах [93, 158, 189].

Задача 3.4.2. Все ближайшие соседи. На плоскости заданы n точек. Требуется для каждой точки найти ближайшего соседа (отличного от самой этой точки).

Задача 3.4.3. Евклидово минимальное остовное дерево — ЕМОД. На плоскости заданы n точек. Требуется найти дерево, которое соединяет все заданные точки и имеет минимальную сумму длин ребер.

Эта задача имеет очевидное приложение к созданию сетей ЭВМ, когда мы хотим соединить между собой все ЭВМ, получив при этом сеть минимальной стоимости. Однако при такой формулировке задачи запрещается вводить дополнительные точки. Если же допускается вводить дополнительные точки, которые называются *точками Штейнера*, то данная задача превращается в задачу построения *дерева Штейнера минимальной длины*, которая, как показано, является NP-трудной [160]. Заметим также, что задачу построения ЕМОД можно рассматривать как задачу теории графов, в которой вес ребра определяется как расстояние между точками, соединяемыми этим ребром. В работе [90] проиллюстрировано несколько алгоритмов построения минимального остовного дерева. В общем случае при решении задачи о минимальном остовном дереве с n вершинами требуется время $\Omega(n^2)$ для определения ребра, имеющего минимальный вес и входящего в дерево, а входные данные представлены набором из $O(n^2)$ независимых весов ребер. Однако можно воспользоваться свойствами евклидовой метрики, что позволит решить задачу построения ЕМОД за время $\theta(n \log n)$.

Задача 3.4.4. Триангуляция. На плоскости заданы n точек. Требуется построить планарный граф с вершинами в заданных точках, такой, что каждая грань внутри выпуклой оболочки является треугольником.

Эта задача возникает при интерполяции функции от двух переменных, когда значения функции известны в некоторых нерегулярно расположенных в плоскости точках [208—210, 253, 289], и при применении метода конечных элементов [67]. Триангуляция этих n точек может быть использована для оценки значения функции в некоторой новой точке путем интерполяции по значениям функции в точках, являющихся вершинами треугольника, содержащего эту новую точку.

Задача 3.4.5. Поиск ближайшего соседа. На плоскости заданы n точек. Требуется найти ближайшего соседа для некоторой запрашиваемой точки.

Эта задача, известная также как «задача о почтовом отделении», возникает при классификации образов [115], когда используется правило классификации по ближайшему соседу, когда новый образец соотносится с классом, которому принадлежит его ближайший сосед, а также при выборке информации из

базы данных, когда в качестве ответа на запрос выдается запись, *наилучшим образом сопоставимая с запросом* [64, 156]. См. также работы [264] и [116], в которых рассматриваются другие меры «расстояния» при решении задач поиска ближайшего соседа.

Задача 3.4.6. Поиск k ближайших соседей. Эта задача аналогична задаче 3.4.5, за тем исключением, что ищутся k ближайших соседей точки.

2. ДИАГРАММА ВОРОНОГО

Предыдущие задачи могут быть решены с использованием *метода геометрического места точек*, упоминавшегося в разд. II-С. Пусть задано множество S из n точек $\{p_1, p_2, \ldots, p_n\}$. Построим *диаграмму Вороного* множества S [300], обозначаемую $\mathrm{Vor}(S)$, которая разбивает плоскость на n классов «эквивалентности», причем каждый из них соответствует некоторой заданной точке. В частности, класс эквивалентности, соответствующий точке p_i, — это многоугольник Вороного $V(p_i)$, определяемый как

$$V(p_i) = \{r \mid r \in R^2,\ d(r, p_i) \leqslant d(r, p_j),\quad i \neq j\}.$$

Другими словами, $V(p_i)$ — это геометрическое место точек, таких, что они расположены ближе к точке p_i, чем к любой другой точке множества S, и этот многоугольник может быть также определен как пересечение полуплоскостей $\bigcap_{i \neq j} H(p_i, p_j)$, где $H(p_i, p_j)$ — полуплоскость, определяемая прямой, перпендикулярной отрезку p_ip_j, делящей его пополам и содержащей точку p_i. Таким образом, диаграмма Вороного множества из n точек представляет совокупность n выпуклых многоугольников Вороного, каждый из которых соответствует точке множества. Диаграмма Вороного известна также под названием *многоугольников Тиссена* [59].

Далее приведен список свойств диаграммы Вороного (см. [211, 212, 316]), которые могут быть получены, если принять упрощающее предположение о том, что никакие четыре точки из заданного множества не лежат на одной окружности. (На рис. 5 приведен пример диаграммы Вороного множества из 16 точек.) (i) Каждая вершина диаграммы Вороного, называемая *точкой Вороного*, имеет степень три. (ii) Каждый ближайший сосед p_j каждой точки p_i определяет ребро многоугольника $V(p_i)$, которое является частью прямой, перпендикулярной отрезку p_ip_j и делящей его пополам. (iii) $V(p_i)$ является неограниченным многоугольником тогда и только тогда, когда точка p_i лежит на границе выпуклой оболочки множества S.

(iv) Граф, двойственный диаграмме Вороного, ребра которого являются прямолинейными отрезками, является триангуляцией множества точек S. Эта триангуляция известна также под названиями *триангуляции Делоне* и *ячейки Дирихле* [55]. (v) Для числа ребер и вершин в диаграмме Вороного $\mathrm{Vor}(S)$ имеет место оценка $O(n)$, где $n = |S|$.

Построение диаграммы Вороного. Диаграмма Вороного множества S из n точек на плоскости может быть построена методом «разделяй и властвуй» за время $O(n \log n)$. Сначала мы разделяем множество S на две половины S_1 и S_2, отделенные друг от друга вертикальной прямой L. При этом S_1 располагается слева от L, а S_2 — справа от нее. Затем мы рекурсивно строим диаграммы Вороного для этих двух подмножеств точек и завершаем вычисления, объединяя две эти диграммы в окончательную диаграмму Вороного. Используя свойство (iii), можно показать, что каждое неограниченное ребро диаграммы Вороного принадлежит прямой, перпендикулярной некоторому ребру выпуклой оболочки и делящей это ребро пополам. Так как выпуклые оболочки множеств S_1 и S_2 не пересекаются, то две их общие опорные прямые (см. задачу 3.1.3) соответствуют двум неограниченным ребрам диаграммы Вороного $\mathrm{Vor}(S)$. Эти два ребра принадлежат ломаной σ, называемой *разделяющей цепью*, которая играет решающую роль на шаге объединения решений. Действительно, σ разбивает плоскость на две (неограниченные) области R_1 и R_2, расположенные соответственно слева и справа от σ. Можно показать, что

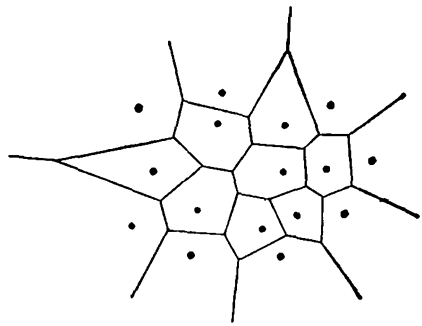


Рис. 5. Диаграмма Вороного для множества из 16 точек.

$$\mathrm{Vor}(S) = (\mathrm{Vor}(S_1) \cap R_1) \cup (\mathrm{Vor}(S_2) \cap R_2),$$

и тем самым обеспечить метод соединения решений. Построение ломаной осуществляется последовательным вычислением ее ребер, начиная с одного из неограниченных ребер. В этом процессе решающим образом используется свойство выпуклости многоугольников Вороного, чтобы показать, что каждое ребро $\mathrm{Vor}(S_1) \cup \mathrm{Vor}(S_2)$ просматривается не более чем фиксированное число раз. Это позволяет получить алгоритм соединения решений, время работы которого пропорционально суммарному чис-

лу ребер диаграмм, т. е. $O(|S_1|+|S_2|)=O(n)$ [196, 211, 212]. Поэтому полное время, необходимое для построения диаграммы Вороного множества S из n точек, равно $O(n \log n)$, что является оптимальным (см. разд. III-F).

Браун продемонстрировал интересную связь между диаграммами Вороного и выпуклыми оболочками. В работах [61, 62] он представил альтернативный алгоритм построения диаграммы Вороного, имеющий сложность $O(n \log n)$, методом преобразования задачи построения планарной диаграммы Вороного множества из n точек в задачу построения выпуклой оболочки n точек в трехмерном пространстве с помощью геометрического преобразования, известного как *инверсия*. Этот метод является общим для пространств произвольной размерности, т. е. диаграмма Вороного в k-мерном пространстве может быть получена из выпуклой оболочки в $(k+1)$-мерном пространстве (подробности см. в работе [61]).

Если имеется диаграмма Вороного, то задачи нахождения пары ближайших точек, нахождения всех ближайших соседей и триангуляции могут быть решены за время $O(n)$ следующим образом. Просматривая каждое ребро диаграммы Вороного, построить прямолинейный двойственный граф. Так как двойственный граф является триангуляцией, а полное число ребер в $\mathrm{Vor}(S)$ равно $O(n)$ (согласно свойствам (iv) и (v)), то этот процесс может быть выполнен за время $O(n)$. Согласно свойству (ii), мы также имеем, что пара ближайших точек определяется ребром триангуляции и аналогично ближайший сосед каждой точки задается ребром триангуляции. Поэтому обе задачи могут быть решены за время $O(n)$. В работе [316] было показано, что ЕМОД является подграфом триангуляции Делоне. Таким образом, задача построения ЕМОД может быть также решена с дополнительными затратами времени $O(n)$ алгоритмом Черитона и Тарьяна [90]. Как и для задачи поиска ближайшего соседа, все, что необходимо сделать, — это найти многоугольник Вороного, в котором располагается новая точка. Поэтому поиск является *задачей о положении точки*, как это обсуждалось в разд. III-C, и может быть выполнен за время $O(\log n)$ (см. задачу 3.3.10).

Расширения диаграммы Вороного. Был предложен ряд расширений и обобщений диаграммы Вороного. Диаграмма Вороного, обсуждавшаяся выше, связана с евклидовой метрикой (т. е. с так называемой L_2-метрикой в формулировке Минковского). Определение диаграммы Вороного может быть легко расширено на случай L_p-метрики, где $1 \leqslant p \leqslant \infty$ [212], а диаграмма по-прежнему может быть построена за время $O(n \log n)$, если мы допускаем, что корень p-й степени может быть вычис-

лен за постоянное время. Понятие остовного дерева также может быть расширено на случай L_p-метрики [177, 232]. Отметим, что при использовании L_1-метрики диаграмма Вороного не является однозначной, и как следствие ее двойственный граф не является триангуляцией Делоне. Триангуляция Делоне — это (единственная) триангуляция, такая, что окружность, описанная вокруг каждого треугольника, не содержит внутри ни одной другой точки. Таким образом, для построения триангуляции Делоне в случае L_1-метрики мы не можем воспользоваться диаграммой Вороного и требуется прямой метод. Алгоритм построения триангуляции Делоне прямым методом, имеющий сложность $O(n \log n)$, приведен в работе [230].

Второе расширение диаграммы Вороного состоит в том, что вместо множества точек рассматривается множество объектов. В работах [211, 222] рассмотрена диаграмма Вороного для множества прямоугольных отрезков или окружностей и даны алгоритмы ее построения, имеющие сложность $O(n \log^2 n)$. Позднее Киркпатрик улучшил оценку временнóй сложности до $O(n \log n)$ [196]. *Срединная ось* простого многоугольника, известная как *скелетон*, как оказывается, является частью диаграммы Вороного для простого многоугольника [217, 290]. Диаграмма Вороного множества прямолинейных отрезков или окружностей в случае L_2-метрики состоит из ребер, которые в общем случае не являются прямолинейными отрезками. (Они могут включать дуги как парабол, так и гипербол.) Однако недавний результат [183] (и независимо [16]) показывает, что диаграмма Вороного множества из n окружностей в геометрии Лагерра состоит из прямолинейных ребер и вычислима за время $O(n \log n)$. Эта частная диаграмма полезна для вычисления связных компонент множества кругов, вычисления контура объединения множества кругов и проверки принадлежности точки этому объединению.

Третье расширение фокусирует внимание на том факте, что в обсуждавшейся до сих пор диаграмме Вороного каждый многоугольник представляет геометрическое место точек, близких к одной точке. Чтобы быть более точными, такую диаграмму следовало бы называть *диаграммой Вороного ближайших соседей*. Шамос и Хой [316] рассмотрели диаграмму Вороного порядка k множества точек, в которой каждый многоугольник диаграммы связан с k точками, $k \geqslant 1$, тем свойством, что для каждой точки внутри этого многоугольника ее k ближайших соседей в точности совпадают с соответствующими k точками. С использованием диаграммы порядка k задача поиска k ближайших соседей может быть решена за время $O(\log n + k)$. В этом выражении первое слагаемое учитывает затраты на определение положения точки, а второе слагаемое — затраты на

перечисление точек в ответе. Свойства диаграммы Вороного порядка k и метод ее построения можно найти в работах [133, 216, 316]. На другом конце спектра (начиная с диаграммы Вороного ближайших соседей) находится диаграмма Вороного самого дальнего соседа, которая в действительности является диаграммой Вороного порядка $(n-1)$. Диаграмма Вороного самого дальнего соседа может быть построена за время $O(n \log n)$ [213, 315] и использована для решения задачи о диаметре (см. ниже) и задачи об 1-центре за время $O(n)$.

Четвертое расширение состоит в том, чтобы связать с каждой точкой некоторое положительное число — вес этой точки, что приводит к «взвешенной» диаграмме Вороного [53]. Взвешенная диаграмма Вороного состоит из n «областей», каждая из которых представляет геометрическое место точек, для которых взвешенное расстояние до некоторой заданной точки является минимальным. В работе [17] показано, что эти «области», связанные с каждой точкой, могут быть несвязными и диаграмма в действительности может содержать $\theta(n^2)$ ребер и вершин. Алгоритм построения такой взвешенной диаграммы за время $O(n^2)$ можно найти в работе [17].

Последнее расширение заключается в обобщении диаграммы или триангуляции на пространства более высокой размерности. Некоторые результаты, касающиеся этого вопроса, можно найти в работах [20, 51, 60, 200, 311, 343]. Используя связь между диаграммой Вороного в d-мерном пространстве и выпуклой оболочкой в $(d+1)$-мерном пространстве [61] и алгоритм построения выпуклой оболочки, данный Сейделом в работе [310], можно получить эффективное решение задачи построения диаграммы Вороного в пространствах высших размерностей. Задача построения минимального остовного дерева в пространствах высших размерностей также рассматривалась в ряде работ (см. [33, 98, 158, 192, 267, 351]), но остается отдельным предметом исследований.

3. ДРУГИЕ ЗАДАЧИ О БЛИЗОСТИ

Задача 3.4.7. Ближайшая пара вершин выпуклого многоугольника. На плоскости задан выпуклый многоугольник. Найти две ближайшие друг к другу вершины многоугольника.

Задача 3.4.8. Все ближайшие соседи для выпуклого многоугольника. На плоскости задан выпуклый многоугольник. Найти ближайшего соседа для каждой вершины многоугольника.

Используя выпуклость многоугольника, Ли и Препарата разработали алгоритм решения этой задачи, имеющий линейную сложность по времени [226, 348]. Однако вопрос о том, можно ли найти пару ближайших вершин простого многоугольника с

n вершинами за время $O(n \log n)$, остается открытым. Известное доказательство нижней оценки (см. лемму 3.6.5) неприменимо в данном случае, так как вершины заданы в известном порядке.

Задача 3.4.9. Самая удаленная пара или задача о диаметре. На плоскости заданы n точек. Найти две из них, самые удаленные друг от друга.

Эта задача возникает при кластеризации [175] и обработке изображений [322]. Так как пара наиболее удаленных точек должна принадлежать границе выпуклой оболочки, то эта задача может быть решена за время $O(n)$ в одномерном случае и $O(n \log n)$ в двумерном случае [295, 313]. Оба этих результата являются оптимальными (см. разд. III-F). В двумерном случае метод заключается в построении за время $O(n \log n)$ выпуклой оболочки n точек и последующего поиска за время $O(n)$ двух наиболее удаленных друг от друга точек путем вращения двух параллельных опорных прямых, как это описано в [316, 330]. Заметим, что для решения задачи о паре ближайших точек требуется время $\Omega(n \log n)$ для любой размерности пространства $d \geqslant 1$. Для задачи о паре наиболее удаленных точек в пространствах высоких размерностей, $d \geqslant 3$, Яо [351] получил алгоритм со сложностью $o(n^2)$. В частности, временна́я оценка равна

$$T(n, d) = O(n^{2-a(d)}(\log n)^{1-a(d)}), \quad \text{где} \quad a(d) = 2^{-(d+1)}.$$

Для $d = 3$ эта оценка может быть улучшена до $O((n \log n)^{1.8})$. Можно ли уменьшить разрыв между $T(n, d)$ и $\Omega(n \log n)$, является открытым вопросом.

Задача 3.4.10. Задача о диаметре для простого многоугольника. Задан простой многоугольник с n вершинами. Найти две наиболее удаленные из них.

Эта задача может быть решена за время $O(n)$, так как выпуклая оболочка простого многоугольника может быть построена за время $O(n)$, а пара наиболее удаленных вершин выпуклого многоугольника может быть найдена за линейное время. Таким образом, выпуклость и здесь играет важную роль. Но сможет ли это помочь также в случае трехмерного пространства, остается неясным. В частности, неизвестен алгоритм нахождения диаметра выпуклого многогранника за время, меньшее, чем $O((n \log n)^{1.8})$ [351]. Заметим, что задача нахождения пары наиболее удаленных вершин простого многоугольника является более простой (по крайней мере не сложнее), чем задача нахождения пары наиболее близких вершин простого многоугольника.

Следующие задачи несколько отличаются от рассмотренных выше в том плане, что в них речь идет о расстоянии между двумя множествами точек. Расстояние между двумя множествами точек A и B обычно определяется как минимум расстояния между точкой множества A и точкой множества B, а именно:

$$d(A, B) = \min_a \min_b d(a, b),$$

где $a \in A$ и $b \in B$, а d — евклидово расстояние. При таком определении $d(A, B) = d(B, A)$. Другая мера, представляющая интерес, — это расстояние *Хаусдорфа* [170], которое не является симметричным. Расстояние Хаусдорфа между множествами A и B определяется как

$$\max_a \min_b d(a, b)$$

и расстояние Хаусдорфа между множествами A и B равно

$$\max\{d(A, B), d(B, A)\}.$$

Задача 3.4.11. Ближайшая пара точек между множествами. Заданы два множества A и B (имеющие m и n точек соответственно, если A и B — конечные множества). Найти две точки, по одной из каждого множества, такие, что они являются наиболее близкими друг к другу.

Если A и B — оба конечные множества, то с помощью диаграммы Вороного эта задача может быть решена за время $O(N \log N)$, где $N = m + n$. А именно, определяется положение каждой точки $a \in A$ в диаграмме $\mathrm{Vor}(B)$ и каждой точки $b \in B$ в диаграмме $\mathrm{Vor}(A)$, что приводит к суммарным затратам времени $O(m \log n + n \log m)$ после того, как построены диаграммы Вороного обоих множеств точек. Отметим, что эта оценка времени является оптимальной (см. лемму 3.6.11).

Когда точки являются вершинами либо простого многоугольника, либо выпуклого многоугольника, можно ожидать получить более быстрое решение. В работе [41] обсуждается вычисление расстояния по Хаусдорфу между двумя выпуклыми многоугольниками и приводится алгоритм со сложностью $O(n)$. В работе [49] приведен алгоритм со сложностью $O(n \log n)$ вычисления пары *наиболее удаленных* точек двух множеств и алгоритм со сложностью $O(n)$ решения этой же задачи для случая, когда точки каждого из множеств образуют выпуклые многоугольники. В работе [308] рассматривается задача нахождения пары наиболее близких точек двух выпуклых многоугольников (два бесконечных множества) и приводится алгоритм со сложностью

$O(\log^2 n)$. Этот результат был впоследствии улучшен до $O(\log n)$ [91, 127]. Для нахождения пары наиболее близких вершин двух выпуклых многоугольников время $O(n)$ является необходимым и достаточным [92, 252, 331].

Задача 3.4.12. Ближайшие соседи в окрестности фиксированного радиуса. На плоскости заданы n точек и некоторая константа $d > 0$. Для каждой точки найти соседей, удаленных от нее на расстояние не более d.

Эта задача возникает в молекулярной графике, кластерном анализе и при передаче данных [44]. Используя метод геометрического места точек, Бентли с соавторами [44] показал, что в случае L_∞-метрики и при некотором предположении о плотности точек, а именно что гиперсфера диаметром d содержит не более некоторого постоянного числа c точек, эта задача может быть решена за время $O(3^k kn(\log n + c))$, где k — размерность пространства. Если предположение о плотности распределения точек не выполняется, то они показали, что полное число вычислений расстояния равно $3^k F$, где F — полное число пар соседей, т. е. размер выходных данных решения задачи.

Задача 3.4.13. Задача о кратчайшем пути с ограничениями. На плоскости заданы n геометрических объектов (называемых «препятствиями») и две точки s и t. Найти кратчайший путь между s и t, не пересекающий внутренность ни одного из препятствий.

В работе [229] были изучены два варианта этой задачи, каждый из которых может быть решен за время $O(n \log n)$. В первом случае препятствиями являются ребра, ограничивающие некоторый простой многоугольник, содержащий как s, так и t. Во втором случае s и t — это произвольные точки плоскости, а ограничения представляют совокупность параллельных отрезков. В работе [224] представлен алгоритм со сложностью $O(n^2 \log n)$ решения этой задачи для случая, когда ограничения представлены n кругами. Томпа [327] изучал эту задачу в связи с проблемой прокладки проводников. Другие результаты в этом направлении см. в [206, 243, 309, 318].

4. ЗАДАЧИ О РАЗБИЕНИИ МНОГОУГОЛЬНИКОВ

Задачи о разбиении многоугольников имеют приложения в распознавании образов. Чтобы облегчить процесс распознавания формы объектов, часто применяется стратегия разбиения объекта на простые части («примитивы») и их сравнение с некоторым набором образцов, имеющихся в библиотеке, с использованием некоторой меры сходства [274]. Часто набор примитивов ограничивается объектами определенных типов, таких,

как выпуклые многоугольники, звездные многоугольники и т. д. Туссен [328] называет этот класс задач декомпозиции *ориентированным на составляющие* (см. работы [328, 329], содержащие соответствующие ссылки). Заметим также, что задача о «триангуляции» принадлежит к этому классу задач. Бывают ситуации, когда некоторые вычисления трудно выполнить для многоугольников общего вида, но они могут быть легко выполнены для выпуклых многоугольников. В этом случае можно извлечь определенную выгоду, разбив многоугольник общего вида на выпуклые части и выполнив вычисления для каждой части в отдельности. Именно такой подход был выбран в работе [2] для обнаружения взаимодействий или столкновений между многоугольниками.

В основном имеются два типа декомпозиции: *разбиение*, при котором не допускается перекрытие компонент (составляющих частей), и *покрытие*, при котором допускается перекрытие частей. Иногда можно вводить дополнительные вершины, называемые *точками Штейнера*, для получения декомпозиций с минимальным числом частей. В недавнем обзоре Кейла и Сэка [194] с большими подробностями обсуждаются минимальные декомпозиции.

Задача 3.4.14. Триангуляция простого многоугольника. Задан простой многоугольник P с n ребрами. Выполнить декомпозицию внутренней области многоугольника на треугольники.

Пионерская работа в этой области была выполнена Гэри с соавторами [162], предложившими алгоритм со сложностью $O(n \log n)$. Выполнение этого алгоритма состоит из двух этапов. На первом этапе за время $O(n \log n)$ многоугольник P разбивается на ряд *монотонных* многоугольников. (Многоугольник Q является *монотонным*, если существует прямая L, такая, что граница многоугольника Q может быть разделена на две цепи ребер и каждая цепь пересекается не более одного раза с каждой прямой, ортогональной L.) На втором этапе с помощью *линейного* по времени алгоритма каждый монотонный многоугольник разбивается на треугольники. Другие алгоритмы триангуляции, имеющие сложность $O(n \log n)$, описаны в работах [70, 334]. Недавно Чазелле и Инчерпи ввели полезное понятие, названное *извилистостью* многоугольника P [88], т. е. число перемен направления движения относительно некоторой точки при круговом движении по границе многоугольника за один оборот. Используя метод разделяй и властвуй, они получили алгоритм триангуляции простого многоугольника P за время $O(n \log s)$, где s — извилистость многоугольника P. Можно ли выполнить триангуляцию простого многоугольника за время $O(n)$, остается открытой проблемой. Если допускаются

дыры, то, как было показано, время, необходимое для решения, равно $\Omega(n \log n)$ [12].

Задача 3.4.15. Триангуляция звездного многоугольника. Задан звездный многоугольник с n ребрами. Выполнить декомпозицию внутренней области многоугольника на треугольники.

Шоне и ван Леувен [307] предложили алгоритм решения этой задачи со сложностью $O(n)$. В действительности имеет место более общий факт, что любой L-выпуклый многоугольник может быть разбит на треугольники за линейное время [144].

Задача 3.4.16. Разбиение изотетичного многоугольника на четырехугольники. Задан изотетичный многоугольник с n ребрами. Выполнить декомпозицию внутренней области многоугольника на выпуклые четырехугольники.

Простой многоугольник не всегда допускает разбиение на четырехугольники, но изотетичный многоугольник всегда может быть разбит на четырехугольники [188]. Сэк [302] показал, что любой изотетичный многоугольник с n ребрами может быть разбит на четырехугольники за время $O(n \log n)$. Остается открытым вопрос, можно ли сделать это за время $o(n \log n)$. Если изотетичный многоугольник является *монотонным* или *звездным*, то его можно разбить на четырехугольники за линейное время [303].

Задача 3.4.17. Декомпозиция простого многоугольника на звездные многоугольники. Задан простой многоугольник P с n ребрами. Выполнить декомпозицию внутренней области многоугольника на звездные многоугольники.

Ави и Туссен предложили алгоритм решения этой задачи со сложностью $O(n \log n)$ [23]. Сначала они ищут триангуляцию многоугольника P, а затем выполняют 3-раскрашивание вершин многоугольника P таким образом, чтобы никакие две смежные в триангуляции вершины не были бы раскрашены в один цвет. Основываясь на этой раскраске, они удаляют все диагонали, инцидентные вершинам заданного цвета, получая, таким образом, разбиение на звездные многоугольники. Если ищется минимальное разбиение, как в работе Кейла [193], то использование метода динамического программирования дает алгоритм со сложностью $O(n^5N^2 \log n)$, где N — число *рефлексных* вершин, т. е. вершин, внутренний угол которых больше 180°.

Задача 3.4.18. Декомпозиция простого многоугольника на выпуклые части. Задан простой многоугольник P с n ребрами. Найти декомпозицию его внутренней области на выпуклые многоугольники.

Чазелле [69] предложил алгоритм со сложностью $O(n + N^2 \log(n/N))$, где N — число *рефлексных* вершин; алгоритм получен в предположении, что допускается введение точек Штейнера. Чазелле и Добкин [81] также представили алгоритм со сложностью $O(n^6)$ для нахождения минимального разбиения многоугольника P на выпуклые части. Этот результат был впоследствии улучшен до $O(n + N^3)$ [69]. Для трехмерного случая в работе [79] представлен алгоритм со сложностью $O(nN^3)$, порождающий $O(N^2)$ выпуклых частей и, как было показано, являющийся оптимальным при анализе худшего случая. Асано и Асано [9] получили алгоритм со сложностью $O(n^3)$ для разбиения P на *минимальное* число *трапецоидов* с двумя горизонтальными сторонами. Эта оценка была улучшена до $O(n^2)$ [10]. При условии что допускаются точки Штейнера, Фенг и Павлидис [145] описали алгоритм со сложностью $O(nN^3)$, а Грин [169] предложил алгоритм со сложностью $O(n \log n)$ для разбиения P на выпуклые части (при этом разбиение не обязательно является минимальным). Однако если ищется минимальное разбиение, то для этого имеются два алгоритма, сложность которых равна $O(n^2N^2)$ [169] и $O(N^2n \log n)$ [193].

Существуют варианты декомпозиции с иными целевыми функциями. Например, задача нахождения за полиномиальное время минимальной взвешенной триангуляции, т. е. триангуляции с минимальной полной длиной ребер множества из n точек на плоскости, по-прежнему остается открытой [161]. При этом довольно интересен тот факт, что минимальная взвешенная триангуляция простого многоугольника может быть выполнена за время $O(n^3)$ [163, 202] Другие результаты, связанные с этим направлением исследований, можно найти в работе [193] и обзоре [194].

Задача 3.4.19. Декомпозиция изотетичного многоугольника на прямоугольники Задан изотетичный многоугольник RP с n сторонами. Выполнить декомпозицию его внутренней области на прямоугольники.

Задача минимального разбиения элегантно решена Липским [237], что позволило создать алгоритм со сложностью $O(n^{3/2} \log n \log \log n)$ с использованием точек Штейнера. Имаи и Асано решили независимо эту же задачу, создав алгоритм со сложностью $O(n^{3/2} \log n)$ [180, 181]. В обоих алгоритмах используется максимальное соответствие двудольного графа пересечений множества вертикальных и горизонтальных отрезков, а требуемый объем памяти составляет $O(n \log n)$.

Задача 3.4.20. Декомпозиция многоугольников с дырами. Задан простой многоугольник, имеющий внутри дыры. Выполнить декомпозицию его внутренней области на более простые

части. (*Дыра* сама является простым многоугольником и не может содержать дыр.)

Оказывается, что многоугольники с дырами являются более трудными объектами для декомпозиции на более простые составляющие, такие, как выпуклые, звездные или монотонные многоугольники. Если допускается использование точек Штейнера, то задачи разбиения простого многоугольника с дырами на минимальное число треугольников или выпуклых частей [236] или на минимальное число трапецоидов с двумя горизонтальными сторонами [9] являются NP-трудными. Для разбиения простого многоугольника с n вершинами и h дырами на минимальное число трапецоидов с двумя горизонтальными сторонами был получен алгоритм со сложностью $O(n^{2+h})$ [10]. При использовании точек Штейнера задача построения минимального покрытия простого многоугольника выпуклыми составляющими, звездными или спиральными составляющими является NP-трудной [274]. Отметим, что, как известно, ни задача о минимальном покрытии, ни задача о минимальном разбиении не принадлежат классу NP. Однако, как было показано, обе эти задачи являются разрешимыми [72, 271]. Без использования точек Штейнера и задача о минимальном покрытии, и задача о минимальном разбиении простого многоугольника с дырами на выпуклые, звездные или спиральные составляющие являются NP-трудными [193, 236, 274].

Задача 3.4.21. Декомпозиция изотетичных многоугольников с дырами на прямоугольники. Задан изотетичный многоугольник с изотетичными дырами. Выполнить декомпозицию его внутренней области на прямоугольники.

Вариант этой задачи, касающийся минимального покрытия, является NR-трудной задачей [247]. Однако задача поиска минимального разбиения может быть решена за время $O(n^{5/2})$ [238, 270] методами максимального двудольного соответствия. В работе [181] Имаи и Асано дали для решения этой задачи алгоритм со сложностью $O(n^{3/2}\log n)$. Если дыры могут вырождаться в точки, то задача о минимальном разбиении становится NP-трудной [236].

Так как большинство задач о минимальной декомпозиции или минимальном разбиении на сегодняшний день являются трудно разрешимыми, то представляют интерес хорошие эвристические методы решения этих задач. Имеется лишь небольшое число результатов с известными оценками поведения [9—11].

Задача 3.4.22. Декомпозиция Делоне простых многоугольников. Задан простой многоугольник P с n вершинами. Найти де-

композицию этого многоугольника, основанную на триангуляции Делоне, а именно обладающую тем свойством, что окружность, описанная вокруг каждого треугольника, не содержит ни одной другой вершины многоугольника P, *видимой* хотя бы из одной вершины этого треугольника.

Эта задача является обобщением задачи о триангуляции Делоне множества точек на плоскости, обсуждавшейся в разд. III-D.2. В работе [211] дан алгоритм со сложностью $O(n^2)$, основанный на понятии *графа видимости* $\mathrm{VG}(P)$ множества вершин многоугольника P. Граф $\mathrm{VG}(P)$ имеет то же самое множество вершин, что и P, а вершины соединены ребром, если прямолинейный отрезок, определяемый этими двумя вершинами, не пересекает границу многоугольника P.

E. Задачи геометрической оптимизации

Этот раздел покрывает комбинаторные геометрические задачи, которые также часто рассматриваются в контексте теории графов или теории оптимизации. Так, например, задача об евклидовом минимальном остовном дереве (задача 3.4.2) является одной из таких задач, теоретико-графовый вариант которой лучше известен. По мере развития вычислительной геометрии изучались метрические свойства таких оптимальных задач в расчете получить более эффективные алгоритмы. Однако имеются задачи, геометрическая сущность которых, по-видимому, не дает каких-либо преимуществ. Евклидова задача о коммивояжере, задача о минимальном дереве Штейнера представляют два известных примера таких задач (обе они остаются NP-трудными [160, 284]). Далее приведен список оптимизации геометрических задач, которым в последнее десятилетие было уделено значительное внимание. Очевидно, при этом ряд оптимальных задач оказался неотраженным в этом списке.

Задача 3.5.1. Линейное программирование. Заданы n полупространств в d-мерном пространстве и некоторый вектор $\mathbf{x} = (x_1, x_2, \ldots, x_d)$. Найти точку $\mathbf{v} = (v_1, v_2, \ldots, v_d)$, принадлежащую пересечению этих полуплоскостей и максимизирующую целевую функцию $x_1v_1 + x_2v_2 + \ldots + x_dv_d$.

Это одна из самых известных задач в исследовании операций, имеющая длинную историю [96]. Двумерный вариант этой задачи может быть легко решен за время $O(n \log n)$ [313, 317] в результате нахождения пересечения n полуплоскостей (задача 3.2.7). Оптимальный алгоритм решения этой задачи за время $O(n)$ был получен с помощью элегантного метода Дайером [118] и Меджиддо [257], который мы в некоторых деталях описали в разд. II-F. Для пространств более высокой размерности эта задача также может быть решена за время $O(n)$ при усло-

вии, что размерность пространства фиксирована [259]. Добкин с соавторами показали [109], что задача линейного программирования является Log-space трудной для *P*. Добкин и Рейсс [112] недавно ввели понятие LP-полноты, а именно задача считается LP-полной тогда и только тогда, когда ее можно преобразовать за полиномиальное время в задачу линейного программирования и *наоборот*, и описали класс LP-полных задач.

Задача 3.5.2. Двумерная линейная отделимость. На плоскости заданы два множества точек P и Q, содержащие соответственно m и n точек. Определить, существует ли прямая, отделяющая друг от друга эти два множества.

Эта задача имеет приложения в статистике и распознавании образов [115]. Обратив внимание на тот факт, что P и Q линейно отделимы тогда и только тогда, когда пересечение выпуклых оболочек множеств P и Q пусто, Шамос [313] предложил алгоритм со сложностью $O(N \log N)$, где $N = m + n$, основанный на вычислении двух выпуклых оболочек в двумерном случае и проверке пустоты их пересечения. Тот же самый подход может быть использован и в трехмерном случае, при этом указанная оценка сложности сохраняется [293]. Для случая когда два множества точек образуют выпуклые многогранники, Маллер и Препарата [265], а позднее Добкин и Киркпатрик [104] получили линейные алгоритмы нахождения отделяющей плоскости для двух выпуклых многогранников, если она существует. Однако метод Дайера [118] и Меджиддо [257] может быть использован для нахождения отделяющей прямой и плоскости для любых двух множеств P и Q в двумерном и трехмерном случаях за время $O(N)$. В общем случае отделяющая гиперплоскость может быть найдена за время $O(N)$ для любого фиксированного числа измерений [259]. В работе [187] приведен рекурсивный метод нахождения отделяющей гиперплоскости.

Задача 3.5.3. Наименьшая охватывающая окружность. На плоскости заданы n точек. Найти наименьшую окружность, охватывающую все эти точки.

В теории расположения объектов [148] эта задача известна как задача об 1-центре. Эта задача может быть легко решена за время $O(n \log n)$ [316] с использованием диаграммы Вороного самого дальнего соседа для n точек (см. разд. III-D). Используя метод поиска с отсечением, Меджиддо [257] получил алгоритм нахождения наименьшей охватывающей гиперсферы, имеющий сложность $O(n)$.

Задача 3.5.4. Наименьший охватывающий прямоугольник. На плоскости задано множество из n точек. Найти наименьший

по площади прямоугольник, охватывающий точки множества.

Эта задача может быть решена за время $O(n \log n)$ методом, основанным на факте, отмеченном Фрименом и Шапира [154], заключающемся в том, что минимальный прямоугольник должен иметь сторону, параллельную ребру выпуклой оболочки множества S. После того как за время $O(n \log n)$ построена выпуклая оболочка, минимальный прямоугольник может быть найден за время $O(n)$ при помощи метода последовательного просмотра ребер выпуклой оболочки [313, 330]. Для этой задачи алгоритм со сложностью $o(n \log n)$ неизвестен. Заметим, что эта задача связана с *евклидовой задачей* о 1-линейном центре и заключается в следующем. На плоскости задано множество S из n точек и требуется найти прямую L, для которой максимальное евклидово расстояние от точек множества $S-L$ минимально. Сходство этих задач заключается в том, что прямая L должна быть параллельна некоторому ребру выпуклой оболочки множества S. В работе [235] показано, что время $O(n \log n)$ является необходимым и достаточным для решения задачи о 1-линейном центре.

Задача 3.5.5. Наименьший охватывающий треугольник. На плоскости задано множество S из n точек. Найти наименьший по площади треугольник, охватывающий точки множества.

Недавно Кли и Ласковский [201] изучали задачу нахождения всех локальных минимумов среди всех треугольников, охватывающих выпуклый многоугольник с n вершинами, и предложили алгоритм со сложностью $O(n \log^2 n)$. (Треугольник T является *локальным минимумом*, если существует $c > 0$, такое, что площадь треугольника T' не меньше площади T для каждого охватывающего треугольника T', хаусдорфово расстояние которого от T меньше c (см. разд. III-D).) Позднее О'Раурке с соавторами предложили оптимальный алгоритм нахождения наименьшего охватывающего треугольника для выпуклых многоугольников с n вершинами, имеющий сложность $\theta(n)$ [272].

Задача 3.5.6. Наибольшая пустая окружность. На плоскости задано множество S из n точек. Найти наибольшую окружность, центр которой находится внутри выпуклой оболочки множества S и которая не содержит внутри ни одной точки множества S.

Эта задача имеет приложение к размещению объектов, когда желательно разместить, например, мусоросборник в жилом районе таким образом, чтобы минимальное расстояние от него до жилых домов было максимально. Эта задача может быть решена оптимальным способом за время $\theta(n \log n)$ при помощи диаграммы Вороного для множества S [313, 332]. Задача о наибольшем пустом (изотетичном) квадрате также может быть ре-

шена за время $\theta(n \log n)$ при помощи диаграммы Вороного с метрикой L_∞ [212, 232].

Задача 3.5.7. Наибольший пустой прямоугольник. Задано множество S из n точек, расположенных в некотором прямоугольнике. Найти наибольший по площади прямоугольник, сходный с заданным прямоугольником и не содержащий ни одной точки множества S.

Эта задача впервые изучена в работе [266], в которой дан алгоритм, имеющий сложность $O(n^2)$ в худшем случае, и алгоритм, имеющий сложность $O(n \log^2 n)$ в среднем случае. В работе [83] с помощью метода разделяй и властвуй и модифицированного варианта диаграммы Вороного оценка для худшего случая была улучшена до $O(n \log^3 n)$. Задача нахождения наибольшего прямоугольника с произвольной ориентацией представляется значительно более сложной.

Имеются некоторые другие результаты для аналогичных оптимизационных геометрических задач. Добкин с соавторами [100] обсуждают, среди прочих, задачу о k-угольнике с наименьшим периметром, т. е. задачу нахождения многоугольника с k вершинами, выбранными из заданного множества точек, имеющего минимальный периметр, и показывают, что эта задача NP-трудна, если k есть $\Omega(n^c)$. Для фиксированного k задача может быть решена за время $O(n \log n)$. Заметим, что, когда k равно 2, задача превращается в задачу о ближайшей паре точек (задача 3.4.1). В работе [56] приведены алгоритм со сложностью $O(n \log n)$ для нахождения треугольника с максимальным периметром и алгоритм со сложностью $O(kn \log n + n \log^2 n)$ для нахождения k-угольника с максимальным периметром или площадью для произвольных значений k. Треугольник и четырехугольник с наименьшей площадью с вершинами, выбранными из числа вершин некоторого выпуклого многоугольника, могут быть найдены за линейное время [113, 315]. Треугольник наименьшей площади с вершинами, выбранными из заданного множества из n точек, может быть найден за время $O(n^2 \log^2 n)$ [110]. Позже эта оценка была улучшена до $O(n^2)$ [86, 133]. Задача нахождения наименьшего охватывающего эллипса составляет предмет исследований, проводимых в настоящее время Силверманом и Титтерингтоном [319] и Постом [287, 288].

Далее мы рассмотрим две общие задачи о расположении — задачу о p-центре и задачу о p-медиане — которые более известны в теоретико-графовой интерпретации и которые, как было показано, являются NP-трудными [190, 191]. Евклидова задача о p-центре формально определяется следующим образом. На плоскости задано множество S точек $\{p_1, p_2, \ldots, p_n\}$, ка-

ждой из которых приписан некоторый вес w_i. Найти множество F, содержащее p точек, называемых *центрами*, такое, что максимальное «расстояние» между множествами S и F минимально, т. е. минимизировать

$$\max_i \min_j w_i d(p_i, q_j),$$

где $p_i \in S$ и $q_j \in F$, а $d(f_i, q_j)$ — евклидово расстояние между точками p_i и q_j. Напротив, в задаче о p-медиане минимизируется сумма, а не максимум расстояний между множествами S и F. Евклидова задача о p-центре является стандартной минимаксной задачей, а задача о наименьшей охватывающей окружности есть не что иное, как задача о невзвешенном 1-центре. Как было замечено ранее, доказать, что геометрическая задача является NP-трудной, значительно труднее, чем сделать то же самое для ее теоретико-графового двойника [160, 284]. Тем не менее недавно было показано, что эти две задачи также являются NP-трудными [260]. В действительности даже поиск приближенного решения евклидовой задачи о p-центре остается NP-трудной задачей и аналогичное утверждение справедливо для задачи об изотетичном p-центре [260]. Следующая задача также является NP-полной [260].

Задача 3.5.8. Покрытие кругами. На плоскости заданы n точек и p кругов с одинаковым радиусом r. Определить, существует ли такое расположение этих p кругов, что они покрывают все точки, т. е. каждая заданная точка находится внутри по крайней мере одного круга.

Как следствие задача определения минимального числа кругов одинакового радиуса r, которыми можно покрыть n заданных точек, также является NP-трудной. Пападимитриу показал, что евклидова задача о p-медиане, в которой на множество F наложено ограничение — оно должно быть подмножеством множества S, является NP-трудной [285]. Отметим, что задача о p-центре в одномерном случае может быть решена за время $O(n \log n)$ [149], а задача о p-медиане — за время $O(n^2 p)$ [261].

Мы завершаем этот раздел обсуждением некоторых вариантов предыдущих задач о расположении. Задача о *наименьшей бомбе* [315, 325], т. е. задача о нахождении наименьшего круга, который покрывает по крайней мере k из n заданных точек, может быть решена за время $O(k^2 n \log n)$ [216]. Алгоритм, дающий приближенное решение этой задачи и допускающий обобщение на случай пространств более высокой размерности, приведен в работе [325]. Задача *о размещении бомбы фиксированного размера*, т. е. поиск такого расположения заданного круга на плоскости, при котором число (или суммарный вес)

точек, покрываемых этим кругом, был бы максимальным, может быть решена за время $O(n^2)$ [89], что является улучшением по сравнению с более ранним алгоритмом [114], время выполнения которого было $O(n^2 \log n)$.

Если круги заменить прямоугольниками, то получается *задача о расположении прямоугольника фиксированного размера*, которая может быть решена оптимальным способом за время $\theta(n \log n)$ в случае двумерного пространства [179] и за время $O(n^{d-1})$ в d-мерном пространстве, $d > 2$ [219]. Задача о взвешенном 1-центре на плоскости может быть решена за время $O(n \log^2 n)$ [255]. Более эффективные алгоритмы можно получить для L_1-метрики [256]. Недавно Коул [94] показал, что задача о взвешенном 1-центре может быть решена за время $O(n \log n)$. Представляет интерес вопрос о том, является ли эта оценка лучшей из возможных для этой задачи. (Напомним, что задача о невзвешенном 1-центре может быть решена за время $O(n)$ [257].) Изучались также и другие комбинаторные оптимизационные задачи, такие, как установление соответствия между $2n$ точками на плоскости. В обзоре, выполненном Ави [19], довольно подробно обсуждаются эвристики, используемые при решении задачи об установлении соответствия.

F. Преобразования задач и нижиие оценки сложности алгоритмов

В этом разделе мы подведем итог, дав небольшое число результатов относительно сложности алгоритмов, которые были установлены либо прямым доказательством по высоте дерева вычислений/решений, либо путем преобразований задач (будет определено ниже). Сначала мы без доказательства сформулируем несколько основных результатов.

Факт 1. Принадлежность. Дано множество S, содержащее n объектов. Для того чтобы определить, принадлежит ли конкретный объект множеству S, требуется по крайней мере $\lceil \log_2 n \rceil$ проверок в худшем случае. Это так называемая *теоретико-информационная* оценка для любой задачи о принадлежности [54].

Факт 2. Сортировка. Даны n элементов из полностью упорядоченного множества. Решение задачи сортировки этих n элементов в соответствии с порядком требует по крайней мере $\Omega(n \log n)$ сравнений в рамках любой основанной на сравнении или на дереве решений модели вычислений (коротко ДРМ) [1]. Это оценку можно рассматривать как теоретико-информационную, так как мы ищем конкретную перестановку в множестве

из $n!$ возможных перестановок этих n элементов, а $\lceil \log_2 n! \rceil = \Omega(n \log n)$.

Факт 3. Закрепление размерности. Если задача в d-мерном случае требует времени $f(n)$, то задача в k-мерном случае, где $k > d$, также требует времени $f(n)$ (см., например, [18]).

Определение. Даны две задачи A и B. Задача A называется *$f(n)$-сводимой* к B, если каждая индивидуальная задача A может быть сведена (преобразована) к некоторой индивидуальной задаче B, а решение индивидуальной задачи B может быть преобразовано обратно в решение индивидуальной задачи A за время $O(f(n))$, где n — размер задачи A.

Лемма 3.6.1 [315]. *Предположим, что задача A является $g(n)$-сводимой к задаче B. Если известно, что в рамках конкретной модели вычислений для решения задачи A требуется время $f(n)$, то для решения задачи B требуется время по крайней мере $f(n) - cg(n)$, где $c > 0$ — некоторая константа. Если B может быть решена за время $f(x)$, то A может быть решена за время $f(n) + c'g(n)$, где $c' > 0$ — некоторая константа.*

Как упоминалось ранее, мы будем использовать алгебраическое дерево вычислений (коротко АДВ), введенное Бен-Ором [26] в качестве нашей основной модели вычислений, возможно, дополнив ее рядом примитивных операций, таких, как проверка того, с какой стороны от направленной прямой лежит точка, в предположении, что все они выполняются за постоянное время. АДВ первого порядка называется линейным деревом вычислений (ЛДВ). Можно показать, что следующие задачи требуют для своего решения время $\Omega(n \log n)$ в рамках АДВ-модели вычислений [26].

Проверка единственности элементов [108]. Даны n чисел. Определить, все ли они различные.

Проверка равенства и включения множеств [298]. Даны два множества $A = \{x_1, x_2, \ldots, x_n\}$ и $B = \{y_1, y_2, \ldots, y_n\}$. Определить, имеет ли место $A = B$ или $A \subseteq B$.

Проверка пересечения множеств [298]. Даны два множества $A = \{x_1, x_2, \ldots, x_n\}$ и $B = \{y_1, y_2, \ldots, y_n\}$. Определить, имеет ли место $A \cap B = \varnothing$.

Проверка точек на значимость [324, 350]. Даны n точек на плоскости. Все ли n точек являются вершинами выпуклой оболочки?

Проверка ε-близости [150]. Даны n действительных чисел. Определить, находятся ли какие-либо два из них в ε-окрестности друг друга, где ε — некоторый фиксированный параметр задачи

Объединение интервалов [150]. На действительной прямой даны n интервалов. Вычислить объединение этих n интервалов. (Справедливость утверждения для этой задачи следует из того факта, что задача проверки ε-близости $O(n)$-сводима к ней.)

Проверка связности объединения интервалов [305]. На действительной прямой даны n интервалов. Определить, является ли объединение этих n интервалов само интервалом.

Следующая задача требует для решения времени $\Omega(n \log n)$ в рамках ЛДВ-модели вычислений.

Проверка равномерности распределения [245]. Даны n чисел и фиксированный параметр $c > 0$. Определить, является ли распределение этих точек равномерным с шагом c. (Множество вещественных чисел $\{x_1, x_2, \ldots, x_n\}$ называется *равномерно распределенным с шагом c*, если существует перестановка p чисел $\{1, 2, \ldots, n\}$, такая, что $x_{p(1)} \leqslant x_{p(2)} \leqslant \ldots \leqslant x_{p(n)}$ и $0 \leqslant x_{p(i+1)} - x_{p(i)} \leqslant c$ для $i = 1, 2, \ldots, n-1$.)

Теперь мы воспользуемся леммой 3.6.1, чтобы дать набросок доказательства некоторых дополнительных нижних оценок. Сейдел [312] приводит несколько результатов, касающихся нижних оценок, для задач, в которых некоторая дополнительная информация, предоставляемая входными данными, не приводит к более эффективным решениям.

Лемма 3.6.2 [315, 316]. *Для построения выпуклой оболочки n точек на плоскости требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

Доказательство. С помощью $O(n)$-сведения задачи сортировки. Преобразование выполняется следующим образом. Даны n положительных чисел $x_1, x_2, \ldots, x_n$. Мы отображаем каждое число в точку на параболе $y = x^2$, а именно x_i отображается в точку $p_i = (x_i, x_i^2)$. Так как вершины выпуклой оболочки точек $p_1, p_2, \ldots, p_n$ могут быть перечислены в порядке, начиная с вершины, имеющей наименьшую x-координату, то любой алгоритм построения выпуклой оболочки может быть использован для сортировки (рис. 6(a)).

Лемма 3.6.3 [317]. *Для построения пересечения n полуплоскостей требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

Доказательство. С помощью $O(n)$-сведения задачи сортировки. Заданы n вещественных чисел $x_1, x_2, \ldots, x_n$. Отображаем каждое число x_i в полуплоскость H_i, содержащую начало координат и определяемую касательной к параболе $y = x^2$ в точке x_i, тангенс угла наклона которой равен $2x_i$, т. е. число x_i отображается в полуплоскость $y \geqslant 2x_i x - x_i^2$ (рис. 6(b)). Так как пересечение полуплоскостей является выпуклым много-

угольником, последовательные ребра которого упорядочены в соответствии с углом наклона, то любой алгоритм построения пересечения полуплоскостей может быть использован для сортировки.

Лемма 3.6.4 [317]. *Для обнаружения пересечения n интервалов на действительной оси требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

Доказательство. С помощью $O(n)$-сведения задачи проверки единственности элементов. Действительно, каждое число в исходных данных для задачи проверки единственности элементов можно рассматривать как вырожденный интервал.

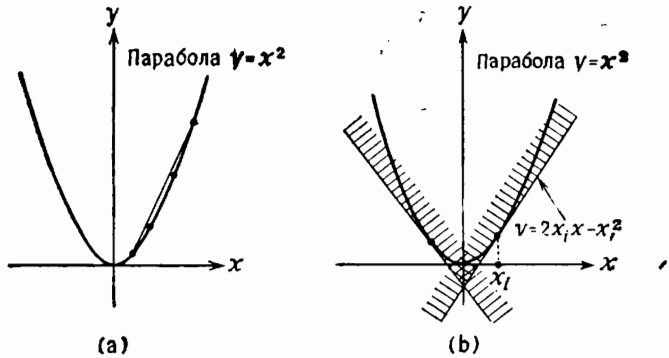


Рис. 6. Отображения чисел x_i в точки, лежащие на параболе $y = x^2$, или в полуплоскости, ограничивающие прямые которых являются касательными к параболе.

Лемма 3.6.5. [316]. *Для определения ближайшей пары точек среди n точек на действительной оси требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

Доказательство. С помощью $O(n)$-сведения задачи проверки единственности элементов. Даже если заранее известно, что точки, задаваемые в задаче различны, для решения задачи попрежнему требуется время $\Omega(n \log n)$, что может быть установлено с помощью $O(n)$-сведения задачи проверки ε-близости.

Лемма 3.6.6[1]) [61]. *Для определения диаметра множества из точек на плоскости требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

Доказательство. С помощью $O(n)$-сведения задачи проверки пересечения множеств. Даны два множества $A = \{x_1, x_2, \ldots, x_n\}$ и $B = \{y_1, y_2, \ldots, y_n\}$, где числа x_i и y_i находятся в интервале $(0, 1)$. Отображаем эти числа на единичную окружность

[1]) Добкин и Мунро независимо доказали эту лемму.

с центром в начале координат следующим образом. Сначала рассмотрим множества точек $S=\{p_i \mid p_i=(x_i, 1)\}$ и $T=\{q_i \mid q_i=(-y_i, -1)\}$ для $i=1, 2, \ldots, n$. Затем применим преобразование, отображающее каждую точку (x, y) множеств S и T в точку $\left(x/\sqrt{x^2+y^2},\ y/\sqrt{x^2+y^2}\right)$ на единичной окружности (рис. 7). Это преобразование эффективно отображает число из множества A в точку первого квадранта, лежащую на единичной окружности, и число из множества B в точку третьего квадранта. Отсюда немедленно следует, что диаметр множества точек на окружности равен 2 тогда и только тогда, когда множества A и B имеют непустое пересечение.

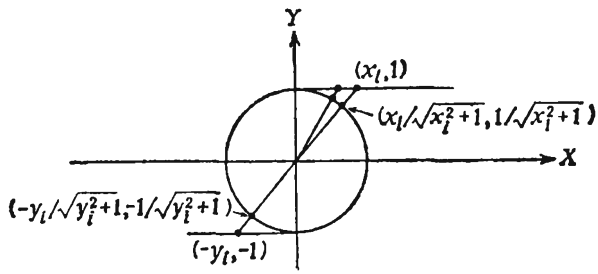


Рис. 7. Отображение чисел в точки единичной окружности $x^2+y^2=1$.

Лемма 3.6.7. [235]. *Для решения дискретной задачи о 1-центре для n точек, когда для заданных n точек требуется найти точку (центр), максимальное расстояние от которой до оставшихся $n-1$ точек минимально, требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

Доказательство. С помощью $O(n)$-сведения задачи проверки равенства множеств. Рассмотрим отображение двух множеств A и B, содержащих по n чисел из интервала $(0, 1)$, как описано в доказательстве предыдущей леммы. Так как расстояние между центром и его самым дальним соседом равно 2 в том и только том случае, если множества A и B равны, то отсюда следует доказываемое утверждение.

Лемма 3.6.8 [313]. *Для построения евклидова минимального остовного дерева (ЕМОД) для n точек на плоскости требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

Доказательство. С помощью $O(n)$-сведения задачи сортировки. Заданы n чисел $x_1, x_2, \ldots, x_n$, которые требуется отсортировать. Отобразим число x_i в точку $p_i=(x_i, 0)$ на оси x, $i=1, 2, \ldots, n$. Перечисление вершин ЕМОД этих n точек дает упорядоченную последовательность заданных точек, откуда сле-

дует, что каждый алгоритм построения ЕМОД может быть использован для сортировки.

Замечание. Задача о паре ближайших точек также $O(n)$-сводима к задаче построения ЕМОД, так как ребро между двумя ближайшими точками должно принадлежать дереву. Следовательно, это дает альтернативное доказательство того, что $\Omega(n \log n)$ является нижней оценкой для задачи построения ЕМОД.

Лемма 3.6.9 [313]. *Для построения триангуляции n точек на плоскости требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

Доказательство. С помощью $O(n)$-сведения задачи сортировки. Даны n чисел. Отобразим их в n точек оси x, как при доказательстве леммы 3.6.8. Добавив к множеству из n точек некоторую точку, не лежащую на оси x, мы получаем множество, триангуляция которого может быть перечислена таким образом, чтобы получить упорядоченную последовательность x-координат точек, лежащих на оси x. Следовательно, каждый алгоритм триангуляции может быть использован для сортировки.

Лемма 3.6.10 [205, 338]. *Для нахождения всех максимумов точек на плоскости требуется время $\Omega(n \log n)$ в рамках ДРМ. (Точка плоскости $p=(x, y)$ является максимумом, если не существует ни одной другой точки $q=(s, t)$, такой, что $x \leqslant s$ и $y \leqslant t$.)*

Доказательство. С помощью $O(n)$-сведения задачи сортировки. Даны n различных чисел $x_1, x_2, \ldots, x_n$. Отобразим их в точки прямой L с уравнением $x+y=c$, где c — некоторая константа, а именно число x_i отображается в точку p_i на прямой L с координатами (x_i, y_i). Заметим, что каждая точка p_i является максимумом. Для того чтобы определить, что p_i является максимумом, алгоритм должен иметь возможность проверить, что не существует точки p_j, $j \neq i$, такой, что $x_i < x_j$ и $y_i < y_j$. Это эквивалентно тому, что для всех $j \neq i$ либо $x_i < x_j$, либо $x_i > x_j$, т. е. для каждой пары x_i и x_j алгоритм должен определить их порядок.

Лемма 3.6.11. *Для определения минимального расстояния между двумя линейно отделимыми множествами точек, содержащими по n точек каждое, требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

Доказательство. С помощью $O(n)$-сведения задачи проверки пересечения множеств. Даны два множества действительных чисел $A=\{a_1, a_2, \ldots, a_n\}$ и $B=\{b_1, b_2, \ldots, b_n\}$. Отобразим эти числа на два линейно отделимых множества точек следующим

образом. Пусть числа из множества A отображаются в точки множества $P=\{(a_i, 0) \mid i=1, 2, \ldots, n\}$, и пусть числа из множества B отображаются в точки множества $Q=\{(b_i, 1) \mid i=1, 2, \ldots, n\}$. Легко видно, что множества A и B имеют общий элемент тогда и только тогда, когда расстояние между множествами P и Q равно 1.

Лемма 3.6.12 [305]. *Для определения того, имеются ли среди n горизонтальных отрезков хотя бы два взаимно видимых отрезка, требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений. (Два горизонтальных отрезка называются взаимно видимыми, если существует вертикальный отрезок, соединяющий две точки этих отрезков и не пересекающий ни одного другого отрезка.)*

Доказательство. С помощью $O(n)$-сведения задачи проверки связности объединения интервалов. Даны n интервалов I_1, $I_2, \ldots, I_n$. Отобразим каждый интервал I_j в горизонтальный отрезок H_j той же самой длины, имеющий ординату j. Затем добавим к этому множеству отрезков два новых горизонтальных отрезка, длина которых равна расстоянию между самым правым и самым левым концами интервалов и имеющих ординаты $y=0$ и $y=n+1$ соответственно. Тогда эти два новых горизонтальных отрезка являются *взаимно видимыми* тогда и только тогда, когда объединение интервалов не является интервалом.

Лемма 3.6.13. *Для определения того, имеется ли среди n заданных точек хотя бы одна, лежащая на какой-нибудь из n заданных прямых, требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений*[1]).

Доказательство. С помощью $O(n)$-сведения задачи проверки пересечения множеств. Даны два множества $A=\{x_1, x_2, \ldots, x_n\}$ и $B=\{y_1, y_2, \ldots, y_n\}$, где x_i и y_i — числа из интервала $(0, 1)$. Отобразим их на единичную окружность, как при доказательстве леммы 3.6.6. Затем превратим множество точек, соответствующих множеству B, в множество из n прямых, проходящих через начало координат и соответствующую этой прямой точку. Очевидно, что задача о принадлежности точки прямой имеет ответ ДА тогда и только тогда, когда множества A и B пересекаются.

Лемма 3.6.14. *Для определения того, имеется ли среди заданных точек на плоскости хотя бы одна тройка коллинеарных точек, требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

---

[1]) **Частное сообщение Хопкрофта.**

Доказательство. С помощью $O(n)$-сведения задачи проверки пересечения множеств. Даны два множества A и B, содержащие по n чисел из интервала $(0, 1)$. Выполним отображение так же, как и при доказательстве предыдущей леммы, и добавим к множеству точек начало координат. Результирующее множество, содержащее $2n+1$ точек, имеет три коллинеарные точки тогда и только тогда, когда множества A и B пересекаются.

Лемма 3.6.15. [245, 295]. *Для нахождения максимального окна, определяемого двумя последовательными точками из n заданных точек, требуется время $\Omega(n \log n)$ в рамках ЛДВ-модели вычислений.*

Доказательство. С помощью $O(n)$-сведения задачи проверки равномерности распределения. Действительно, можно сравнить длину окна с параметром c в задаче проверки равномерности распределения за постоянное время.

Замечание. Наша модель вычислений исключает использование функции, вычисляющей целую часть числа, в качестве одной из примитивных функций. Отметим, что Гонсалес получил с помощью функции вычисления целой части числа алгоритм решения данной задачи, имеющий сложность $O(n)$ ([165], см. также [295]).

Лемма 3.6.16. *Для нахождения закрытой полуокружности, содержащей максимальное число точек из n, заданых на окружности, требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

Доказательство. С помощью $O(n)$-сведения задачи проверки единственности элементов. Даны n чисел $x_1, x_2, \ldots, x_n$. Отобразим число x_i в две точки $(1/y_i, x_i/y_i)$ и $(-1/y_i, -x_i/y_i)$, где $y_i = \sqrt{1+x_i^2}$. Заданные числа являются различными тогда и только тогда, когда искомая закрытая полуокружность содержит в точности $n+1$ точку.

Лемма 3.6.17 [313, 315]. *Для построения диаграммы Вороного множества из n точек на плоскости требуется время $\Omega(n \log n)$ в рамках АДВ-модели вычислений.*

Доказательство. Мы можем свести к этой задаче целый ряд задач. Для примера возьмем задачу о ближайшей паре точек. Так как две ближайшие точки должны определять ребро в диаграмме Вороного, то мы можем использовать диаграмму Вороного для решения задачи о ближайшей паре точек.

Лемма 3.6.18. *Для решения задачи о максимальной пустой окружности, состоящей в построении наибольшей окружности, центр которой принадлежит выпуклой оболочке заданного мно-*

жества из n точек на плоскости и внутри которой не содержится ни одна из заданных точек, требуется время $\Omega(n \log n)$ в рамках ЛДВ-модели вычислений.

Доказательство. Данная задача является задачей о максимальном окне для двумерного случая (см. задачу 3.6.15).

IV. ЗАКЛЮЧЕНИЕ

Мы дали обзор современного состояния недавно возникшей области исследований, известной как вычислительная геометрия. Предполагалось сделать этот обзор по возможности более широким, хотя имеется целый ряд исследовательских находок, которые не включены в данную работу. Проблемные области и используемые методы не описаны с учетом всех мельчайших деталей, но вместе с тем описание выполнено по возможности более точно.

В вычислительной геометрии имеется ряд открытых проблем, большинство из которых были упомянуты в статье. Концепция динамической вычислительной геометрии [15, 275], когда рассматриваемые объекты перемещаются с течением (непрерывным изменением) времени, например, является одним из направлений исследований, заслуживающих дальнейшего изучения. В настоящее время главное внимание в вычислительной геометрии уделяется получению асимптотических оценок поведения алгоритмов. Чтобы ускорить начавшийся уже процесс переноса развитой в вычислительной геометрии технологии в другие области, следует больше уделять внимания неасимптотическому поведению алгоритмов, т. е. поведению алгоритмов на задачах «небольших» размеров. Более чем необходимо проводить сравнения временны́х характеристик различных алгоритмов, для которых имеется лишь асимптотическая оценка сложности, представленная с помощью O-большое нотации. Эти сравнения должны проводиться для таких значений размеров исходных данных, какие встречаются в практических задачах.

Авторы благодарны К. К. Вонгу, побуждавшему их написать этот обзор, и выражают глубокую признательность Т. Асано, Б. Чазелле, Х. Эделсбруннеру и Г. Туссену за их замечания и тщательное чтение начального варианта этого обзора.

ЛИТЕРАТУРА

[1] Aho A. V., Hopcroft J. E., Ullman J. D. The Design and Analysis of Computer Algorithms. — Reading, MA. — Addison-Wesley, 1974. [Имеется перевод: Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979.]

[2] Ahuja N., Chien R. T., Yen R., Birdwell N. Interference detection and collision avoidance among three-dimensional obejects. — In: Proc. 1st Annu. Nat. Conf. Artifical Intell. — Palo Alto, CA, 1980,p . 44—48.

[3] Akl S. G Two remarks on a convex hull algorithm. — Inform. Processing Lett., 1979, v. 8, p. 108—109.

[4] Akl S. G., Toussaint G. T. A fast convex hull algorithm. — Inform. Processing Lett., 1978, v. 7, p. 219—222.
[5] Akl S. G., Toussaint G. T. Efficient convex hull algorithms for pattern recognition applications. — In: Proc. 4th Int. Joint Conf. Pattern Recognition. — Kyoto, Japan, 1978, p. 483—487.
[6] Anderson K. R. A reevaluation of an efficient algorithm for determining the convex hull of a finite planar set. — Inform. Processing Lett., 1978. v. 7, p. 53—55.
[7] Andrew A. M. Another efficient algorithm for convex hulls in two dimensions. — Inform. Processing Lett., 1979, v. 9, p. 216—219.
[8] Appel A., Will P. M. Determining the three-dimensional convex hull of a polyhedron. — IBM J. Res. Develop., 1976, p. 590—601.
[9] Asano T., Asano T. Minimum partition of polygonal regions into trapezoids. — In: Proc. 24th IEEE Annu. Symp. Foundations Comput. Sci., Nov. 1983, p. 233—241.
[10] Asano T., Asano T., Imai H. Partitioning a polygonal region into trapezoids. — Dep. Math. Eng. Instrum. Phys., Univ. Tokyo, Tokyo, Japan, Res. Memo. RMI84-03, 1984.
[11] Asano T., Asano T., Ohsuga Y. Partitioning polygonal regions into triangles. — Papers of Tech. Groups of IECE, CAS 83-98, 1983. p. 31—36.
[12] Asano T., Asano T., Pinter R. Y. Polygon triangulation: Efficiency and minimality (представлено к публикации, 1984).
[13] Asano T., Edahiro M., Imai H., Iri M., Murota K. Practical use of bucketing techniques in computational geometry. — In: Computational Geometry, G. T. Toussaint, Ed. — New York: North-Holland, 1985.
[14] Atallah M. J. A linear time algorithm for the Hausdorff distance between convex polygons. — Inform. Processing Lett., Nov. 1983, v. 8, p. 207—209.
[15] Atallan M. J. Dynamic computational geometry. — In: Proc. 24th IEEE Annu. Symp. Foundations Comput. Sci., 1983, p. 92—99.
[16] Aurenhammer F. Power diagrams: Properties, algorithms and applications. — IIG, Tech. Univ. Graz, Graz, Austria, Rep. F120, 1983.
[17] Aurenhammer F., Edelsbrunner H. An optimal algorithm for constructing the weighted Voronoi diagrams in the plane. — Pattern Recognition, 1984, v. 17, No. 2, p. 251—257.
[18] Avis D. Lower bounds for geometric problems. — In: Proc. 18th Allerton Conf. Commun., Contr., Comput., 1980, p. 35—40.
[19] Avis D. A survey of heuristics for the weighted matching problem. — Networks, 1983, v. 13, p. 475—493.
[20] Avis D., Bhattacharya B. K. Algorithms for computing the *d*-dimensional Voronoi diagrams and their duals. — In: Advances in Computing Research, vol. 1, F. P. Preparata (ed.), JAI Press, 1983. p. 159—180.
[21] Avis D., El Gindy H., Seidel R. Simple on-line algorithms for convex polygons. — In: Computational Geometry. G. T. Toussaint (ed). — New York: North-Holland, 1985.
[22] Avis D., Toussaint G. T. An optimal algorithm for determining the visibility of a polygon from an edge. — IEEE Trans. Comput., Dec. 1981, v. C-30, p 910—914.
[23] Avis D., Toussaint G. T. An efficient algorithm for decomposing a polygon into star-shaped polygons. — Pattern Recognition, 1981, v. 13, p. 395—398.
[24] Baird H. S. Fast algorithms for LSI artwork analysis. — J. Design Automat. Fault-Tolerant Computing, 1978, v. 2, No. 2, p. 179—209.
[25] Bass L. J., Schubert S. R. On finding the disc of minimum radius containing a given set of points. — Math. Comput., 1967, v. 12, p. 712—724.
[26] Ben-Or M. Lower bounds for algebraic computation trees. — In: Proc. 15th ACM Annu. Symp. Theory Comput., Apr. 1983, p. 80—86.
[27] Bentley J. L. Multidimensional binary search trees used for associative searching. — Commun. Ass. Comput. Mach., Sept. 1975. v. 18, p. 509—517.

[28] Bentley J. L. Solutions to Klee's rectangle problems. — Carnegie-Mellon Univ. Pittsburgh, PA, 1977 (не опубликовано).
[29] Bentley J L. Decomposable searching problems. — Inform. Processing Lett., 1979, v. 8, p. 244—251.
[30] Bentley J. L. Multidimensional divide and conquer. — Commun. Ass. Comput. Mach., Apr. 1980, v. 23, p. 214—229.
[31] Bentley J. L. Notes on a taxonomy of planar convex hull algorithms. — Dep. Comput. Sci., Carnegie-Mellon Univ., Pittsburg, PA, manuscript, 1980.
[32] Bentley J. L., Faust G. M., Preparata F. P. Approximation algorithms for convex hulls. — Commun. Ass. Comput. Mach., 1982, v. 25, p. 64—68.
[33] Bentley J. L., Friedman J. H. Fast algorithms for constructing minimal spanning trees in coordinate spaces. — IEEE Trans. Comput., Feb. 1978, v. C-27, p. 97—105.
[34] Bentley J. L., Friedman J. H. Data structures for range searching. — Comput. Surveys, 1979, v. 11, p. 397—409.
[35] Bentley J. L., Haken D., Hon R. Fast geometric algorithms for VLSI tasks. — In: Proc. Comput. Conf., 1981, p. 88—92.
[36] Bentley J. L., Maurer H. A. A note on Euclidean near neighbor searching in the plane. — Inform. Processing Lett., 1979, v. 8, p. 133—136.
[37] Bentley J. L., Maurer H. A. Efficient worst-case data structures for range searching. — Acta Inform., 1980, v. 13, p. 155—168.
[38] Bentley J. L., Ottmann T. Algorithms for reporting and counting geometric intersections. — IEEE Trans. Comput., Sept. 1979, v. C-28, p. 643—647.
[39] Bentley J. L., Saxe J. B. Decomposable searching problems. I. Static-to-dynamic transformation. — J. Algorithms, 301—358, 1980, v. 1, p. 301—358.
[40] Bentley J. L., Shamos M. J. Divide-and-conquer in multidimensional space. — In: Proc. 8th ACM Annu. Symp. Theory Comput., 1976, p. 220—230.
[41] Bentley J. L., Shamos M. I. A problem in multivariate statistics: Algorithms, data structure and applications. — In: Proc. 15th Allerton Conf. Commun., Contr., Comput, 1977, p. 193—201.
[42] Bentley J. L., Shamos M. I. Divide and conquer for linear expected time. — Inform. Processing Lett., 1978, v. 7, p. 87—91.
[43] Bentley J. L., Stanat D. F. Analysis of range searches in quad trees. — Inform. Processing Lett., 1975, v. 3, p. 170—173.
[44] Bentley J. L., Stanat D. F., Williams E. H., Jr. The complexity of finding fixed-radius near neighbors. — Inform. Processing Lett., 1977, v. 6, p. 209—212.
[45] Bentley J. L., Weide B., Yao A. C. Optimal expected time algorithms for closest-point problems. — ACM Trans. Math. Software, 1980, v. 6, No. 4, p. 563—579.
[46] Bentley J. L., Wood D. An optimal worst-case algorithm for reporting intersections of rectangles. — IEEE Trans. Comput., July 1980, v. C-29, p. 571—577.
[47] Bezier P. Numerical Control — Mathematics and Applications, A. R. Forrest, Transl. — New York: Wiley, 1972.
[48] Bhattacharya B. K., El Gindy H. A new linear convex hull algorithm for simple polygons. — IEEE Trans. Inform. Theory, Jan. 1984, v. IT-30, p. 85—88.
[49] Bhattacharya B. K., Toussaint G. T. Efficient algorithms for computing maximum distance between two finite planar sets. — J. Algorithms, June 1983, v. 4, p. 121—126.
[50] Bieri H., Nef W. A recursive plane-sweep algorithm, determining all cells of a finite division of R^d. — Computing, 1982, v. 28, p. 189—198.

[51] Boissonnat J. D., Faugeras O. D., Triangulation of 3D objects. — In: Proc. 7th Int. Joint Conf. Artificial Intell. — Vancouver, B. C., Canada, 1981, p. 658—660.
[52] Bolour A. Optimal retrieval algorithms for small region queries. — SIAM J. Comput., 1981, v. 10, p. 721—741.
[53] Boots B. N. Weighting Thiessen polygons. — Econ. Geogr., 1979, p. 248—259.
[54] Borodin A. B. Computational complexity — Theory and practice. — In: Currents in the Theory of Computing. A. V. Aho (ed.). — Englewood Cliffs, NJ: Prentice-Hall, 1973, l. 35—89.
[55] Bowyer A. Computing Dirichlet tessellations. — Comput. J., 1981, v. 24, p. 162—166.
[56] Boyce J. E., Dobkin D. P., Drysdale R. L., III, Guibas L. J. Finding extermal polygons. — In: Proc. 14th ACM Annu. Symp. Theory Comput., 1982, p. 282—289.
[57] Boyse J. W. Interference detection among solids and surfaces. — Commun. Ass. Comput. Mach., vol. 21, pp. 3—9, 1979, v. 21, p. 3—9.
[58] Brassel K. E., Fegeas R. An algorithm for shading of regions on vector display devices. — Comput. Graphics, 1979, v. 13, p. 126—133.
[59] Brassel K. E., Reif D. A procedure to generate Thiessen polygons. — Geogr. Anal., 1979, v. 11.
[60] Brostow W., Dussault J.-P., Fox B. L. Construction of Voronoi polyhedra. — J. Comput. Phys., 1978, v. 29, p. 81—92.
[61] Brown K. Q. Geometric transformations for fast geometric algorithms. — Ph. D. dissertation, Dep. Comput. Sci., Carnegie-Mellon Univ., Pittsburgh, PA, Dec. 1979.
[62] Brown K. Q. Voronoi diagrams from convex hulls. — Inform. Processing Lett., 1979, v. 9, p. 223—228.
[63] Brown K. Q. Comments on 'Algorithms for reporting and counting geometric intersections'. — IEEE Trans. Comput., Feb. 1981, v. C-30, p. 147—148.
[64] Burkhard W. A., Keller R. M. Some approaches to best match file searching. — Commun. Ass. Comput. Mach., 1973, v. 16, p. 230—236.
[65] Burton R. P., Smith D. R. A hidden-line algorithm for hyperspace. — SIAM J. Comput., 1982, v. 11.
[66] Bykat A. Convex hull of a finite set of points in two dimensions. — Inform. Processing Lett., 1978, v. 7, p. 296—298.
[67] Cavendish J. C. Automatic triangulation of arbitrary planar domains for the finite element method. — Int. J. Numer. Methods Eng., 1974, v. 8, p. 679—696.
[68] Chand D. R., Kapur S. S. An algorithm for convex polytopes. — J. ACM, Jan. 1970, v. 17, p. 78—86.
[69] Chazelle B. M. Computational geometry and convexity. — Ph. D. dissertation, Yale Univ., New Haven, CT; см. также: Carnegie-Mellon Univ., Pittsburgh, PA, Tech. Rep. CMU-CS-80-150, 1980.
[70] Chazelle B. M. A theorem on polygon cutting with applications. — In: Proc. 23rd IEEE Annu. Symp. Found. Comput. Sci., 1982, p. 339—349.
[71] Chazelle B. M. The polygon containment problem. — In: Advances of Computing Research, vol. I. F. P. Preparata (ed.). — JAI Press, 1983, p. 1—33.
[72] Chazelle B. M. A decision procedure for optimal polyhedron partitioning. — Inform. Processing Lett., 1983, v. 16, p. 75—78.
[73] Chazelle B. M. An improved algorithm for the fixed-radius neighol problem. — Inform. Processing Lett., 1983, v. 16, p. 193—198.
[74] Chazelle B. M. Filtering search: a new approach to query-answering. — In: Proc. 24th IEEE Annu. Symp. Found. Comput. Sci., Nov. 1983. p. 122—132.

[75] Chazelle B. M. Optimal algorithms for computing depths and layers. In: Proc. 2st Allerton Conf. Commun. Control Comput., Oct. 1983, p. 427—436.
[76] Chazelle B. M. Intersecting is easier than sorting. — In: Proc. 16th ACM Annu. Symp. Theory Comput., 1984, p. 125—134.
[77] Chazelle B. M. How to search in history. — In: Proc. Conf. Found. Comput. Theory. — New York: Springer-Verlag, Aug. 1983, p. 52—63.
[78] Chazelle B. M. Fast searching in a real algebraic manifold with applications to geometric complexity. — Dep. Comput. Sci., Brown Univ., Providence, RI, Tech. Rep. TR-CS-84-13, June 1984.
[79] Chazelle B. M. Convex partitions of polyhedra: A lower bound and worst-case optimal algorithm. — SIAM J. Comput., Aug. 1984, v. 13, p. 488—507.
[80] Chazelle B. M., Cole R., Preparata F. P., Yap C. K. New upper bounds for neighbor searching (будет опубликовано).
[81] Chazelle B. M., Dobkin D. P. Decomposing a polygon into its convex parts. — In: Proc. 11th ACM Annu. Symp. Theory Comput., 1979, p. 38—48.
[82] Chazelle B. M., Dobkin D. P. Detection is easier than computation. — In: Proc. 12th ACM Annu. Symp. Theory Comput., May 1980, p. 146—153.
[83] Chazelle B. M., Drysdale R. L. III, Lee D. T. Computing the largest empty rectangle. — In: Proc. Symp. Theoretic Aspects Comput. Sci., Paris, France, Apr. 1984.
[84] Chazelle B. M., Edelsbrunner H. Optimal solutions for a class of point petrieval problems. — Technische Univ. Graz., Austria, Tech. Rep. IIG (будет опубликовано).
[85] Chazelle B. M., Guibas L. J. Fractional cascading: A data structuring technique with geometric applications. — Manuscript, 1984.
[86] Chazelle B. M., Guibas L. J., Lee D. T. The power of geometric duality.— In: Proc. 24th IEEE Annu. Symp. Found. Comput. Sci., Nov. 1983, p. 217—225.
[87] Chazelle B. M., Incerpi J. Unraveling the segment tree. — Dep. Comput Sci., Brown Univ. Providence, RI. Tech. Rep. CS-83-15, June 1983.
[88] Chazelle B. M., Incerpi J. Triangulating a polygon by divide-and-conquer.— In: Proc. 21st Allerton Conf. Commun. Control Comput., Oct. 1983, p. 447—456.
[89] Chazelle B. M., Lee D. T. On a circle placement problem. — In: Proc. Conf. Inform. Syst. Sci., Princeton, NJ, 1984.
[90] Cheriton D., Tarjan R. E. Finding minimum spanning trees. — SIAM J. Comput., Dec. 1976, p. 724—742.
[91] Chin F., Wang C. A. Optimal algorithms for the intersection and the minimum distance problems between planar polygons. — IEEE Trans. Comput., Dec. 1983, v. C-32, p. 1203—1207.
[92] Chin F., Wang C. A. Minimum vertex distance between separable convex polygons. — Inform. Processing Lett., Jan. 1984, v. 18, p. 41—45.
[93] Clarkson K. L. Fast algorithms for the all nearest neighbors problems. — In: Proc. 24th IEEE Annu. Symp. Found. Comput. Sci., Nov. 1983, p. 226—232.
[94] Cole R. Slowing down sorting networks to obtain faster sorting algorithms. — In: Proc. 25th IEEE Annu. Symp. Found. Comput. Sci., Oct. 1984, p. 255—260.
[95] Cole R., Yap C. K. Geometric retrieval problems. — In: Proc. 24th IEEE Annu. Symp. Found Comput. Sci., Nov. 1983, p. 112—121.
[96] Dantzig G. B. Linear Programming and Extensions. — Princeton, NJ: Princeton Univ. Press, 1963. [Имеется перевод: Данциг Д. Б. Линейное программирование, его применения и обобщения. — М.: Прогресс, 1966.]

[97] Devroye L., Toussaint G. T. A note on linear expected time algorithms for finding convex hulls. — Computing, 1981, v. 26, p. 361—366.
[98] Dewdney A. K. Complexity of nearest neighbor searching in three and higher dimensions. — Univ. Western Ontario, Tech. Rep. 28, London, Ont., Canada, 1977.
[99] Dobkin D. P. A nonlinear lower bound on linear search tree programs for solving knapsack problems. — J. Comput. Syst. Sci., 1976, v. 13, p. 69—73.
[100] Dobkin D. P., Drysdale R. L. III, Guibas L. J. Finding smallest polygons. — In: Advances in Computing Research, vol. 1, F. P. Preparata (ed.). — JAI Press, 1983, p. 181—214.
[101] Dobkin D. P., Edelsbrunner H. Organizing points in two and three dimensions. — IIG. Technische Univ. Graz, Austria, Rep. 130, Feb. 1984.
[102] Dobkin D. P., Edelsbrunner H. Space searching for intersecting objects (manuscript).
[103] Dobkin D. P., Kirkpatrick D. G. Fast detection of polyhedral intersection. — Theoret. Comput. Sci., 1983, v. 27, p. 241—253.
[104] Dobkin D. P., Kirkpatrick D. G. A linear algorithm for determining the separation of convex polyhedra. — J. Algorith. (будет опубликовано).
[105] Dobkin D. P., Kirkpatrick D. G. Fast algorithms for preprocessed polyhedral intersection detection.
[106] Dobkin D. P., Lipton R. J. Multidimensional searching problems. — SIAM J. Comput., 1976, v. 5, No. 2, p. 181—186.
[107] Dobkin D. P., Lipton R. J. A lower bound of $1/2n^2$ on linear search programs for the knapsack problem. — J. Comput. Syst. Sci., 1978, v. 16, p. 413—417.
[108] Dobkin D. P., Lipton R. J. On the complexity of computations under varying sets of primitives. — J. Comput. Syst. Sci., 1979, v. 18, p. 86—91.
[109] Dobkin D. P., Lipton R. J., Reiss S. Linear programming is log-space hard for *P*. — Inform. Processing Lett., Feb. 1979, v. 8, p. 96—97.
[110] Dobkin D. P., Munro J. I. Efficient use of the past. — In: Proc. 21st IEEE Annu. Symp. Found Comput. Sci., Oct. 1980, p. 200—206.
[111] Dobkin D. P, Munro J. I. Optimal time minimal space selections algorithm. — J. ACM, July 1981, v. 28, No. 3, p. 454—461.
[112] Dobkin D. P., Reiss S. P. The complexity of linear programming. — Theoret. Comput. Sci., 1980, v. 11, p. 1—18.
[113] Dobkin D. P., Snyder L. On a general method for maximizing and minimizing among certain geometric problems. — In: Proc. 20th IEEE Annu. Symp. Found Comput. Sci., 1979, p. 9—17.
[114] Drezner Z. On a modified 1-center problem. — Manag. Sci., 1981, v. 27, p. 838—851.
[115] Duda R. O., Hart P. E. Pattern Classification and Scene Analysis. — New York: Wiley, 1973. [Имеется перевод: Дуда Р., Харт П. Распознавание образов и анализ сцен. — М.: Мир, 1976.]
[116] Dunlavey M. R. Query performance of a many-dimensional best-match algorithm — In: Proc. 19th Allerton Conf. Commun. Control Comput., 1981, p. 389—396.
[117] Dyer M. E. A simplified $O(n \log n)$ algorithm for the intersection of 3-polyhedra. — Dep. Math., Middlesbrough, UK Tech Rep. TPMR 80-5, 1980.
[118] Dyer M. E. Linear time algorithms for two- and three-variable linear programs. — SIAM J. Comput., Feb. 1984, v. 13, No. 1, p. 31—45.
[119] Edahiro M., Kokubo I., Asano T. A new point-location algorithm and its practical efficiency — Comparison with existing algorithms. — Dep. Math. Eng. Instrumen. Phys. Univ. Tokyo, Tokyo, Japan, Res. Memo. RMI 83-04, Oct. 1983.

[120] Eddy W. A new convex hull algorithm for planar sets. — ACM Trans. Math. Software., vol. 3, N 4, pp. 398—403, Dec. 1977.
[121] Edelsbrunner H. Optimizing the dynamization of decomposable searching problems. — IIG, Technische Univ. Graz., Austria, Rep. 35, Sept. 1979.
[122] Edelsbrunnner H. A new approach to rectangle intersections. Part I. — Int. J. Comput. Math., 1983, v. 13, p. 209—219.
[123] Edelsbrunner H. A new approach to rectangle intersections. Part II. — Int. J. Comput. Math., 1983, v. 13, p. 221—229.
[124] Edelsbrunner H. Dynamic data structures for orthogonal intersection queries. — IIG, Technische Univ. Graz., Austria, Rep. 59, Oct. 1980.
[125] Edelsbrunner H. A note on dynamic range searching. — Bull. EATCS, 1981, v. 15, p. 34—40.
[126] Edelsbrunner H. Intersection problems in computational geometry. — Ph. D. dissertation, IIG, Technische Univ. Graz, Austria, Rep. 93, 1982.
[127] Edelsbrunner H. On computing the extreme distances between two convex polygons. — IIG, Technische Univ. Graz, Austria, Rep. 96, 1982.
[128] Edelsbrunner H., Guibas L. J., Stolfi J. Optimal point location in a monotone subdivision. — SIAM J. Comput. (будут опубликовано).
[129] Edelsbrunner H., Maurer H. A. On the intersection of orthogonal objects. — Inform. Processing Lett., 1981, v. 13, p. 177—181.
[130] Edelsbrunner H., Maurer H. A. A space-optimal solution of general region location. — Theoret. Comput. Sci., 1981, v. 16, p. 329—336.
[131] Edelsbrunner H., Maurer H. A., Kirkpatrick D. G. Polygonal intersection searching. — Inform. Processing Lett., 1982, v. 14, p. 74—79.
[132] Edelsbrunner H., Maurer H. A., Preparata F. P., Rosenberg A. L., Welzl E., Wood D. Stabbing line segments. — BIT, 1982, v. 22, p. 274—281.
[133] Edelsbrunner H., O'Rourke J., Seidel R. Constructing arrangements of lines and hyperplanes with applications. — In: Proc. IEEE Annu. Symp. Found. Comput. Sci., Nov. 1983; p. 83—91; см. также: IIG, Technische Univ. Graz, Austria, Tech. Rep. F123, Sept. 1983.
[134] Edelsbrunner H., Ottmann T., van Leeuwen J., Wood D. Connected components of orthogonal geometric objects. — Unit for Comput. Sci., McMaster Univ., Hamilton. Ont., Canada, Rep. 81-CS-04, 1981.
[135] Edelsbrunner H., Overmars M. H. On the equivalence of some rectangle problems. — Inform. Processing Lett., May 1982, v. 14, No. 3, p. 124—127.
[136] Edelsbrunner H., Overmars M. H. Batched dynamic solutions to decomposable searching problems. — J. Algorith. (будет опубликовано).
[137] Edelsbrunner H., Overmars M. H., Seidel R. Some methods of computational geometry applied to computer graphics. — IIG, Technische Univ. Graz, Austria, Tech. Rep. F117, June 1983.
[138] Edelsbrunner H., Overmars M. H., Wood D. Graphics in flatland: A case study. — In: Advances in Computing Research, vol. 1, F. P. Preparata (ed.). — JAI Press, 1983, p. 35—59.
[139] Edelsbrunner H., van Leeuwen J. Multidimensional data structures and algorithms, A bibliography. — IIG, Technische Univ. Graz, Austria, Rep. 104, 1983.
[140] Edelsbrunner H., Welzl E. Halfplanar range estimation. — IIG Technische Univ. Graz, Austria, Rep. 98, 1982.
[141] Edelsbrunner H., Welzl E. Halfplanar range search in linear space and $O(n^{0.695})$ query time. — IIG, Technische Univ. Graz, Austria, Rep. 111, 1983.
[142] El Gindy H. An efficient algorithm for computing the weak visibility polygon from an edge in simple polygons, Jan. 1984.
[143] El Gindy H., Avis D. A linear algorithm for computing the visibility polygon from a point.—J. Algorith., June 1981, v. 2, No. 2, p. 186—197.
[144] El Gindy H., Avis D., Toussaint G. T. Applications of a two dimensional

hidden-line algorithm to other geometric problems. — Computing, 1983, v. 31, p. 191—202.
[145] Feng H.-Y. F., Pavlidis T. Decomposition of polygons into simpler components: Feature generation for syntactic pattern recognition. — IEEE Trans. Comput., 1975, v. C-24, p. 636—650.
[146] Forrest A. R. Computational geometry — Achievements and problems. — In: Computer Aided Geometric Design, R. E. Barnhill and R. F. Riesenfeld (eds.). — New York: Academic, 1974, p. 17—44.
[147] Fortune S., Hopcroft J. A note on Rabin's nearest-neighbor algorithm. — Inform. Processing Lett., Jan. 1979, v. 8, No. 1, p. 20—23.
[148] Francis R. L., White J. A. Facility Layout and Location. — Englewood Cliffs, NJ: Prentice-Hall, 1974.
[149] Frederickson G. N., Johnson D. B. Finding kth paths and p-centers by generating and searching good data structures. — J. Algorith., 1983, v. 4, p. 61—80.
[150] Fredman M. L., Weide B. On the complexity of computing the measure of $U[a_i, b_i]$. — Commun. ACM, 1978, v. 21, No. 7, p. 540—544.
[151] Fredman M. L. A lower bound of the complexity of orthogonal range queries. — J. ACM., 1981, v. 28, p. 696—705.
[152] Freeman H. Computer processing of line-drawing images. — Comput. Surveys, 1974, v. 6, p. 57—93.
[153] Freeman H., Loutrel P. P. An algorithm for the two dimensional hidden line problem. — IEEE Trans. Electron. Comput., 1967, v. EC-16, p. 784—790.
[154] Freeman H., Shapira R. Determining the minimum-ares encasing rectangle for an arbitrary closed curve. — Commun. ACM, July 1975, v. 18, p. 409—413.
[155] Friedman N. Some results on the effect of arithmetics on comparison problems. — In: Proc. 13th IEEE Annu. Symp. Switching and Automata Theory 1972, p. 139—143.
[156] Friedman J. H., Bentley J. L., Finkel R. A. An algorithm for finding best match in logarithmic expected time. — ACM Trans. Math. Software, 1977, v. 3, No. 3, p. 209—226.
[157] Friedman J. H., Baskett F., Shustek J. An algorithm for finding nearest neighbors. — IEEE Trans. Comput., 1975, v. C-24, p. 1000—1006.
[158] Gabow H. N., Bentley J. L., Tarjan R. E. Scaling and related techniques for geometry problems. — Proc. 16th ACM Annu. Symp. Theory Comput., Apr. 1984, p. 135—143.
[159] Gallmberti R., Montanari U. An Algorithm for hidden-line elimination. — Commun. ACM, 1969, v. 12, p. 206—211.
[160] Garey M., Graham R. L., Johnson D. S. Some NP-complete problems. — In: Proc. 8th ACM Annu. Symp. Theory Comput., May 1976, p. 10—22.
[161] Garey M. R., Johnson D. S. Computers and Intractability: A Guide to the Theory of NP-Completeness. — San Francisco, CA: Freeman, 1979. [Имеется перевод: Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.]
[162] Garey M., Jonhson D. S., Preparata F. P., Tarjan R. E. Triangulating a simple polygon. — Inform. Processing Lett., 1978, v. 7, No. 4, p. 175—180.
[163] Gilbert P. D. New results on planar triangulations. — Coord. Sci. Lab. Univ. Illinois. — Urbana. IL. Tech. Rep. ACT-15, July 1979.
[164] Gonnet G. H., Munro J. I., Wood D. Direct dynamic structure for some line segment problems. — Comput. Vision, Graphics and Image Processing, 1983, v. 23, p 178—186.
[165] Gonzalez T. Algorithms on sets and related problems. — Dep. Comput. Sci. Univ. Oklahoma. Tech. Rep., 1975.
[166] Gowda I. G., Kirkpatrick D. G., Lee D. T., Naamad A. Dynamic Voronoi

diagrams. — IEEE Trans. Inform. Theory Sept. 1983, v. ГТ-29. No. 5, p. 724—731.
[167] Graham R. L. An efficient algorithm for determining the convex hull of a finite planar set. — Inform. Processing Lett., 1972, v. 1, p. 132—133.
[168] Graham R. L., Yao F. F. Finding the convex hull of a simple polygon. — Stanford Univ., Stanford, CA, Tech. Rep. STAN-CS-81-877, 1981; см. также: J. Algorith., Dec. 1983, v. 4, No. 4, p. 324—331.
[169] Greene D. H. The decomposition of polygons into convex parts. — Advances in Computing Research, vol. 1, F. P. Preparata (ed.). — JAI Press, 1983, p. 235—259.
[170] Grünbaum B. Convex Polytopes. — New York: Wiley Interscience, 1967.
[171] Guibas L. J., Stolfi J. On computing all north-east nearest neighbors in the L_1-metric. — Inform Processing Lett., Nov. 1983, v. 17, p. 219—223.
[172] Güting R. H. Optimal divide-and-conquer to compute measure anz contour for a set of iso-rectangles. — Lehrstuhl Informatik vi. Univ. Dortmund, Tech. Rep., 1982.
[173] Güting R. H. Stabbing c-oriented polygons. — Inform. Processing Lett., Jan. 1983, v. 16, p. 35—40.
[174] Güting R. H., Wood D. Finding rectangle intersections by divide-and-conquer. — Univ. Waterloo., Waterloo, Ont., Canada, Tech. Rep. CS-83-03, 1983.
[175] Hartigan J. A. Clustering Algorithms. — New York: Wiley, 1975.
[176] Hertel S., Mehlhorn K., Mantyla M., Nievergelt J. — Space sweep solves intersection ot two convex polyhedra elegantly. — Acta Informatica (будет опубликовано).
[177] Hwang F. K. An $O(n \log n)$ algorithm fór rectilinear minimal spanning tree. — J. ACM, 1979, v. 26, p. 177—182.
[178] Imai H. Finding connected components on an intersection graph of squares in the Euclidean plane. — Inform. Processing Lett., Oct. 1982, v. 15, No. 3, p. 125—128.
[179] Imai H., Asano T. Finding the connected components and a maximum clique of an intersectoin graph of rectangle in the plane. — J. Algorith., Dec. 1983, v. 4, No. 4, p. 310—323.
[180] Imai H., Asano T. An efficient algorithm for finding a maximum matching of an intersection graph of horizontal and vertical line segments.— In: Papers IECE Tech. Group Circuits and Systems, CAS 83-143.
[181] Imai H., Asano T. Efficient algorithms for geometric graph search problems. — Dep. Math. Eng. Instrumen. Phys. Univ. Tokyo, Tokyo. Japan. Res. Memo. RMI 83-05, Oct. 1983.
[182] Imai H., Asano T. Dynimic orthogonal segment intersection search. — Dep. Math. Eng. Instrumen. Phys. Univ. Tokyo. — Tokyo, Japan, Res. Memo, RMI 84-02, Feb. 1984.
[183] Imai H., Iri M., Murota K. Voronoi diagram in the Laguerre geometry and its applications. — SIAM J. Comput. (будет опубликовано).
[184] Jarvis R. A. On the identification of the convex hull of a finite set of points in the plane. — Inform. Processing Lett., 1973, v. 2, p. 18—21.
[185] Johansen G. H., Gram C. A simple algorithm for building the 3-D convex hull. — BIT, 1983, v. 23, p. 146—160.
[186] Johnson D. S., Preparata F. P. The densest hemisphere problem. — Theoret. Comput. Sci., 1978, v. 6, p. 93—107.
[187] Jozwik A. A recursive method for the investigation of the linear separability of two sets. — Pattern Recog., 1983, v. 11, No. 4, p. 429—431.
[188] Kahn J., Klawe M., Kleitman D. Traditional galleries require fewer watchman. — SIAM J. Algorith. Disc. Method, 1980, v. 4, No. 2, p. 194—206.
[189] Kalantari I., McDonald G. A data structure and an algorithm for nearest point problem. — IEEE Trans. Software Eng., 1983, v. SE-9, No. 5, p. 631—634.

[190] Kariv O., Hakimi S. L. An algorithmic approach to network location problems, Part I: the centers. — SIAM J. Appl. Math., 1979, v. 37, p. 513—538.
[191] Kariv O., Hakimi S. L. An algorithmic approach to netwoork location problems. Pirt II: p-medians. — SIAM J. Appl. Math., 1979, v. 37, p. 539—560.
[192] Katajainen J. On the worst case of a minimal spanning tree algorithm for Euclidean space. — BIT, 1983, v. 23, p. 2—8.
[193] Keil J. M. Decomposing polygons into simpler components. — Ph. D. dissertation. Dep. Comput. Sci.. Univ. Toronto, Toronto, Ont., Canada, 1983.
[194] Keil J. M., Sack J. R. Minimum decompositions of polygonal objects. — In: Computational Geometry. G. T. Toussaint (ed.). — Amsterdam, The Netherlands: North-Holland, 1985.
[195] Khachian L. G. A polynomial algorithm in linear programming. — Sov. Math. Dokl., 1979, v. 20, p. 191—194.
[196] Kirkpatrick D. G. Efficient computation of continuous skeletons. — In: Proc. 20th IEEE Annu. Symp. Found. Comput. Sci., Oct. 1979, p. 18—27.
[197] Kirkpatrick D. G. Optimal search in planar subdivisions. — SIAM J. Comput., Feb. 1983, v. 12, No. 1, p. 28—35.
[198] Kirkpatrick D. G., Seidel R. The ultimate planar convex hull algorithm? — In: Proc. 20th Allerton Conf. Commun. Control Comput., 1982, p. 35—42.
[199] Kirkpatrick D. G., Seidel R. The ultimate planar convex hull algorithm? — Dep. Comput. Sci., Cornell Univ., Ithaca, NY, Tech. Rep. 83-577, Oct. 1983.
[200] Klee V. On the complexity of d-dimensional Voronoi diagrams. — Archiv der Mathematik, 1980, v. 34, p. 75—80.
[201] Klee V., Laskowski M. C. Finding smallest triangles containing a given convex polygon. — J. Algorith. (будет опубликовано).
[202] Klincsek G. T. Minimal triangulations of polygonal domains. — Ann. Discrete Math., 1980, v. 9, p. 121—123.
[203] Knuth D. E. The Art of Computer Programming: Sorting and Searching. Vol. 3.— Reading, MA: Addison-Wesley, 1973. [Имеется перевод: Кнут Д. Искусство программирования для ЭВМ. Сортировка и поиск. Том 3. — М.: Мир, 1978.]
[204] Knuth D. E. Big omicron and big omega and big theta. — SIGACT News, Apr. — June 1976, v. 8.2, p. 18—24.
[205] Kung H. T., Luccio F., Preparata F. R. On finding the maxima of a set of vectors. — J. ACM, 1975, v. 22, p. 469—476.
[206] Larson R. C., Li V. O. K. Finding minimum rectilinear distance paths in the presence of barriers. — Networks, vol. 11, N 3, pp. 285—304, 1981, v. 11, No. 3, p. 285—304.
[207] Lauther L. 4-dimensional binary search tress as a means to speed up associative searches in design rule verification of integrated circuits. — J. Design Automat. Fault-Tolerant Computing, 1978, v. 2, p. 241—247.
[208] Lawson C. L. C^1-compatible interpolation over a triangle. — Jet Propulsion Lab., Tech. Memo, 33-770, May 1976.
[209] Lawson C. L. Integrals of a C^1-compatible triangular surface element. — Jet Propulsion Lab., Tech. Memo. 33-808, Dec. 1976.
[210] Lawson C. L. Software for C^1 surface interpolation. — Jet Propulsion Lab., pub. 77-30, Aug. 1977.
[211] Lee D. T. Proximity and reachability in the plane. — Coord. Sci. Lab., Univ. Illinois, Urbana, IL, Tech. Rep. R-831, 1978.
[212] Lee D. T. Two dimensional Voronoi diagram in the L_p-metric. — J. ACM, Oct. 1980, p. 604—618.
[213] Lee D. T. Farthest neighbor Voronoi diagrams and applications. — Dep. Elec. Eng. Comput. Sci., Northwestern Univ., Evanston, IL, Tech. Rep. 80-11-FC-04, 1980.

[214] Lee D. T. On finding the convex hull of a simple polygon. — Dep. Elec. Eng. Comput. Sci., Northwestern Univ., Evanston, IL, Tech. Rep. 80-03-FC-01, 1980; см. также: Int. J. Comput. Inform. Sci., Apr. 1983, v. 12, No. 2, p. 87—98.
[215] Lee D. T. Shading of regions on vector display devices. — Comput. Graphics, Aug. 1981, v. 15, No. 3, p. 37—44.
[216] Lee D. T. On k-nearest neighbor Voronoi diagrams in the plane. — IEEE Trans. Comput., June 1982, v. C-31, p. 478—487.
[217] Lee D. T. Medial axis transformation of a planar shape. — IEEE Trans. Pattern Anal. Machine Intell., July 1982, v. PAMI-4, No. 4, p. 363—369.
[218] Lee D. T. Visibility of a simple polygon. — Comput. Vision, Graphics and Image Processing, 1983, v. 22. p. 207—221.
[219] Lee D. T. Maximum clique problem of rectangle graphs. — In: Advances in Computing Research, vol. 1, F. P. Preparata (ed.). — JAI Press, 1983, p. 91—107.
[220] Lee D. T. An optimal time and minimal space algorithm for rectangle intersection problems. — Int. J. Comput. Inform. Sci. (будет опубликовано).
[221] Lee D. T., Chen I. M. Display of visible edges of a set of convex polygons. — In: Computational Geometry, G. T. Toussaint (ed.). — Amsterdam, The Netherlands: North-Holland, 1985.
[222] Lee D. T., Drysdale R. L. III. Generalized Voronoi diagram is the plane. — SIAM J. Comput., Feb. 1981, v. 10, No. 1, p. 73—87.
[223] Lee D. T., Lin A. Computing visibility polygon from an edge.— Dep. Elec. Eng. Comput. Sci., Northwestern Univ., Evanston, IL, Tech. Rep. 84-02-FC-01, Jan. 1984.
[224] Lee D. T., Megiddo N. Routing around circles (manuscript, Oct. 1983).
[225] Lee D. T., Preparata F. P. Location of a point in a planar subdivision and its applications. — SIAM J. Comput., Sept. 1977, v. 6. No. 3, p. 594—606.
[226] Lee D. T., Preparata F. P. The all nearest neighbor problem for convex polygons. — Inform. Processing Lett., June 1978, p. 189—192.
[227] Lee D. T., Preparata F. P. An optimal algorithm for finding the kernel of a polygon. — J. ACM. July 1979, p. 415—421.
[228] Lee D. T., Preparata F. P. An improved algorithm for the rectangle enclosure problem. — J. Algorith., Sept. 1982, v. 3, No. 3, p. 218—224.
[229] Lee D. T., Preparata F. P. Euclidean shortest paths in the presence of rectilinear barriers. — Networks, 1984, v. 14, p. 393—410.
[230] Lee D T., Schachter B. Two algorithms for constructing Delaunay triangulations — Int. J. Comput. Inform. Sci., June 1980, v. 9, No. 3, p. 219—242.
[231] Lee D. T., Wong C. K. Worst case analysis for region and partial region searches in multidimensional binary search trees and balanced quad trees. — Acta Informatica, 1977, v. 9, p. 23—29.
[232] Lee D. T., Wong C. K. Voronoi diagrams in L_1-(L_∞-)metrics with 2-dimensional storage applications. — SIAM J. Comput., Feb. 1980, v. 9, No. 1, p. 200—211.
[233] Lee D. T., Wong C. K. Quintary trees: A file structure for multidimensional database systems. — ACM Trans. Database Syst., Sept. 1980, v. 1, No. 3, p. 339—353.
[234] Lee D T., Wong C. K. Finding intersection of rectangles by range search. — J. Algorith., 1981, v. 2, p. 337—347.
[235] Lee D. T., Wu Y. F. Efficient algorithms for Euclidean 1-line center and problems. — In: Proc. ISOLDE III, Boston, MA, 1984.
[236] Lingas A. The power of non-rectilinear holes. — In: Proc. 9th Colloq. Automata, Lang. Programming. — Aarhus, Denmark, 1982.

[237] Lipski W., Jr. Finding a Manhattan path and problems. — Networks, 1983, v. 13, p. 399—409.
[238] Lipski W,, Jr., Lodi E., Luccio F., Mugnai C., Pagli L. On two dimensional data organization II. — Fundamenta Informaticae, p. 245—260, 1979, v. 2, p. 245—260.
[239] Lipski W, Jr., Papadimitriou C. H. A fast algorithm for testing for safety and detection deadlocks in locked transaction systems. — J. Algorith., 1981, v. 2, p. 211—226.
[240] Lipski W., Jr., Preparata F. P. Finding the contour of a union of isooriented rectangles. — J. Algorith., 1980, v. 1, p. 235—246; J. Algorith., 1980, v. 3, p. 301.
[241] Lipski W., Jr., Preparata F. P. Segments, rectangles, contours. — J. Algorith., 1981, v. 2, p. 63—76.
[242] Lipton R. J., Tarjan R. E. Applications of a planar separator theorem. — In: Proc. 18th IEEE Annu. Symp. Found. Comput. Sci., 1977, pp. 162—170; см. также: SIAM J. Comput., Aug. 1980, v. 9, No. 3, p. 615—627.
[243] Lozano-Perez T., Wesley M. A. An algorithm for planning collision free paths among polyhedral obstacles. — Commun. ACM, Oct. 1979, v. 22, No. 10, p. 560—570.
[244] Lueker G. S., Willard D. E. A data structure for dynamic range queries. — Inform. Processing Lett., Dec. 1982, v. 15, No. 5, p. 209—213.
[245] Manber U., Tompa M. Probabilistic, nondeterministic and alternating decision trees. — Univ. Washington, Tech. Rep. 82-03-01, 1982.
[246] Mairson H. G., Stolfi J. Reporting and counting line segment intersections. — Dep. Comput. Sci., Stanford Univ., Stanford, CA, Extended Abstract, 1984.
[247] Masek W. J. Some NP-complete set covering problems. — Unpublished manuscript, Apr. 1979.
[248] Maurer H. A., Ottmann T. Dynamic solutions of decomposable searching problems. — In: Discrete Structures and Algorithms, U. Pape (ed.). — Hanser, 1979, p. 17—24.
[249] McCallum D., Avis D. A linear algorithm for finding the convex hull of a simple polygon. — Inform. Processing Lett., 1979, v. 9, p. 201—206.
[250] McCreight E. M. Efficient algorithms for enumerating intersecting intervals and rectangles. — Xerox Palo Alto Res. Cen., Palo Alto, CA, Tech. Rep. PARC CSL-80-9, 1980.
[251] McCreight E. M. Priority search trees. — Xerox Palo Alto Res. Cen., Palo Alto, CA, Tech. Rep. PARC CSL-81-5, 1981.
[252] McKenna M., Toussaint G. T. Finding the minimum vertex distance between two disjoint convex polygons in linear time. — School Comput. Sci., McGill Univ., Montreal, P. Q., Canada, Tech. Rep. SOCS-8306, Apr. 1983.
[253] McLain D. H. Two-dimensional interpolation from random data. — Comput. J., 1976, v. 19, p. 178—181.
[254] McQueen M. M., Toussaint G. T. On the ultimate convex hull algorithm in practice. — Pattern Recog. Lett. (будет опубликовано).
[255] Megiddo N. The weighted Euclidean 1-center problem. — Dep. Statist., Tel Aviv Univ., Tel Aviv, Israel, 1981.
[256] Megiddo N. On some planar location problems. — Dep. Statist. Tel Aviv Univ., Tel Aviv, Israel, Oct. 1981.
[257] Megiddo N. Linear time algorithm for linear programming in R^3 and related problems. — SIAM J. Comput., Nov. 1983, v. 12, No. 4, p. 759—776.
[258] Megiddo N. Applying parallel computation algorithms in the design of serial algorithms. — J. ACM, Oct. 1983, v. 30, No. 4, p. 852—865.
[259] Megiddo N. Linear programming in linear time when the dimension is fixed. — J. ACM, Jan. 1984, v. 31, No. 1, p. 114—127.
[260] Megiddo N., Supowit K. J. On the complexity of some common geomet-

ric location problems. — SIAM J. Comput., Feb. 1984, v. 13, No. 1, p. 182—196.

[261] Megiddo N., Zemel E., Hakimi S. L. The maximum coverage location problem. — Cen. Math. Stud. Econ. Management Sci., Northwestern Univ., Evanston, IL, Discuss. Paper 490, Aug. 1981.

[262] Mehlhorn K. Lower bounds on the efficiency of static to dynamic transforms of data structures. — Math. Syst. Theory, 1981, v. 15, p. 1—16.

[263] Mehlhorn K., Overmars M. H. Optimal dynamization of decomposable searching problems. — Inform. Processing Lett., Apr. 1981, v. 12, No. 2, p. 93—98.

[264] Minsky M. L., Papert S. Perceptron. — Cambridge, MA: M. I. T. Press, 1966. [Имеется перевод: Минский М., Пейперт С. Персептроны. — М.: Мир, 1971.]

[265] Muller D. E., Preparata F. P. Finding the intersection of two convex polyhedra. — Theoret. Comput. Sci., 1978, v. 7, p. 217—236. [Имеется перевод: Маллер Д., Препарата Ф. Нахождение перечисления двух выпуклых многогранинков. — В кн.: Кибернетический сборник, 20. — М.: Мир, 1983, с. 5—29.]

[266] Naamad A., Hsu W. L., Lee D. T. On maximum empty rectangle problem. — Discrete Appl. Math., 1984, v. 8, p. 267—277.

[267] Nevalaninen O., Ernvall J., Katajainen J. Finding minimal spanning trees in a Euclidean coordinate space. — BIT, 1981, v. 21, p. 46—54.

[268] Newman W. M., Sproull R. F. Principles of Interactive Computer Graphics.— New York: McGraw-Hill, 1979. [Имеется перевод: Ньюмен У. М., Спруэлл Р. Ф. Основы интерактивной машинной графики. — М.: Мир, 1976.]

[269] Nievergelt J., Preparata F. P. Plane-sweeping algorithms for intersecting geometric figures. — Commun. ACM., 1982, v. 25, No. 10, p. 739—747.

[270] Ohtsuki T., Sato M., Tachibana M., Torii S. Minimum partitioning of rectilinear regions. — Trans. Inform. Processing Soc. Japan, 1983.

[271] O'Rourke J. The complexity of computing minimum convex covers for polygons. — In: Proc. 20th Allerton Conf. Commun. Control Comput., Oct. 1982, p. 75—84.

[272] O'Rourke J., Aggarwal A., Maddila S., Baldwin M. An optimal algorithm for finding minimal enclosing triangles. — Dep. Elec. Eng. Comput. Sci., Johns Hopkins Univ., Baltimore, MD, 1984, Tech. Rep. JHU/EECS-84/08, May 1984.

[273] O'Rourke J., Chien C-B., Olson T., Naddor D. A new linear algorithm for intersecting convex polygons. — Comput. Graph. Image Processing, 1982, v. 19, p. 384—391.

[274] O'Rourke J., Supowit K. J. Some NP-hard polygon decomposition problems. — IEEE Trans. Inform. Theory. Mar. 1983, v. IT-29, No. 2, p. 181—190.

[275] Ottmann T., Wood D. Dynamic sets of points. — Dep. Comput. Sci., Univ. Waterloo, Waterloo, Ont., Canada, Tech. Rep. CS-82-56, Nov. 1982.

[276] Overmars M. H. Dynamization of order decomposable set problems. — J. Algorith., Sept. 1981, v. 2, p. 245—260; см. также: J. Algorith., Sept. 1983, v. 4, p. 301.

[277] Overmars M. H. Range searching in a set of line segments. — Univ. Utrecht, Utrecht, The Netherlands, Tech. Rep. RUU-CS-83-6, Feb. 1983.

[278] Overmars M. H. The locus approach. — Univ. Utrecht, Utrecht, The Netherlands, Tech. Rep. RUU-CS-83-12, 1983.

[279] Overmars M. H., van Leeuwen J. Two general methods for dynamizing decomposable searching problems. — Computing, 1981, v. 26, p. 155—166.

[280] Overmars M. H., van Leeuwen J. Some principles for dynamizing decomposable searching problems. — Inform. Processing Lett., 1981, v. 12, p. 49—54.

[281] Overmars M. H., van Leeuwen J. Maintenance of configurations in the plane. — J. Comput. Syst. Sci., 1981, v. 23, p. 166—204.
[282] Overmars M. H., van Leeuwen J. Dynamization of decomposable searching problems yielding good worst-case bounds. — Lecture Notes in Computer Science 104. — New York: Springer-Verlag, 1981, p. 224—233.
[283] Overmars M. H., van Leeuwen J. Worst-case insertion and deletion methods for decomposable searching problems. — Inform. Processing Lett., 1981, v. 12, p. 168—173.
[284] Papadimitriou C. H. The Euclidean traveling salesman problem is NP-complete. — Theoret. Comput. Sci., 1977, v. 4, p. 237—244.
[285] Papadimitriou C. H. Worst-case and probabilistic analysis of a geometric location problem. — SIAM J. Comput., 1981, v. 10, p. 542—557.
[286] Pavlidis T. Algorithms for Graphics and Image Processing. — Berlin: Springer-Verlag, 1982.
[287] Post M. J. A minimum spannnig ellipse algorithm. — In: Proc. 22nd IEEE Annu. Symp. Found. Comput. Sci., Oct. 1981, p. 115—122.
[288] Post M. J. Minimum spanning ellipsoids. — In: Proc. 16th Symp. Theory Comput., Apr. 1984, p. 108—116.
[289] Powell M. J. D., Sabin M. A. Pairwise quadratic approximation on triangles. — ACM Trans. Math. Software, 1977, v. 3, No. 4, p. 316—325.
[290] Preparata F. P. The medial axis of a simple polygon. — In: Proc. 6th Symp. Math. Found. Comput. Sci., Lecture Notes in Computer Science 53. — New York: Springer-Verlag, 1977, p. 443—450.
[291] Preparata F. P. An optimal real time algorithm for planar convex hulls. — Commun. ACM, 1979, v. 22, p. 402—405.
[292] Preparata F. P. A new approach to planar point location. — SIAM J. Comput., Aug. 1981, v. 10, No. 3, p. 473—482.
[293] Preparata F. P., Hong S. J. Convex Hulls of infinite sets of points in two and three dimensions.—Commun. ACM. Feb. 1977, v. 20, No. 2, p. 87—93.
[294] Preparata F. P., Muller D. E. Finding the intersection of a set of N half-spaces in time $O(N \log N)$. — Theoret. Comput. Sci., 1979, v. 8, p. 45—55. [Имеется перевод: Препарата Ф., Маллер Д. Нахождение пересечения полупространств за время $O(n \log n)$. — В кн.: Кибернетический сборник, 21. — М.: Мир, 1984, с. 55—68.]
[295] Preparata F. P., Shamos M. J. Computational Geometry. — New York: Springer-Verlag, 1985. [В издательстве «Мир» готовится перевод книги.]
[296] Rabin M. O. Proving simultaneous positivity o linear forms. — J. Comput. Syst. Sci., 1972, v. 6, p. 639—650.
[297] Raghavan V., Yu C. Y. A note on a multidimensional searching problem. — Inform. Processing Lett., Aug. 1977, v. 6, No. 4, p. 133—135.
[298] Reingold E. M. On the optimality of some set algorithms. — J. ACM, Oct. 1972, v. 19, No. 4, p. 649—659.
[299] Riesenfeld R. Applications of b-spline approximation to geometric problems of computer-aided design. — Dep. Comput. Sci., Univ. Utah. Salt Lake City, UT, Tech. Rep. UTEC-CSc-73-126, 1973.
[300] Roger C. A. Packing and Covering. — Cambridge, England: Cambridge University Press, 1964. [Имеется перевод: Роджерс К. Укладки и покрытия. — М.: Мир, 1968.]
[301] Rosenfeld A. Picture Processing by Computers. — New York: Academic, 1969. [Имеется перевод: Розенфельд А. Распознавание и обработка изображений с помощью вычислительных машин. — М.: Мир, 1972.]
[302] Sack J. R. An $O(n \log n)$ algorithm for decomposing simple rectilinear polygons into convex quadrilaterals. — In: Proc. 2th Allerton Conf. Commun. Control Comput., 1982, p. 64—74.
[303] Sack J. R., Toussaint G. T. A linear time algorithm for decomposing rectilinear star-shaped polygons into convex quadrilaterals. — In: Proc. 19th Allerton Conf. Commun. Control Comput., 1981, p. 21—30.

[304] Saxe J. B., Bentley J. L. Transforming static data structures into dynamic structures. — In: Proc. 20th IEEE Annu. Symp. Found. Comput. Sci., Oct. 1979, p. 148—168.
[305] Schlag M., Luccio F., Maestrini P., Lee D. T., Wong C. K. A visibility problem in VLSI layout compaction. — Advances in Computing Research, vol. 2, F. P. Preparata (ed.). — JAI Press (будет опубликовано).
[306] Schonhage A., Paterson M., Pippenger N. Finding the median. — J. Comput. Syst. Sci., 1976, v. 13, p. 184—199.
[307] Schoone A A. van Leeuwen J. Triangulating a star-shaped polygon. — Univ. Utrecht, Utrecht, The Netherlands, Tech. Rep. RUV-CS-80-3, Apr. 1980.
[308] Schwartz J. T. Finding the minimum distance between two convex polygons. — Inform. Processing Lett., 1981, v. 13, No. 4, p. 168—170.
[309] Schwartz J. T., Sharir M. On the piano movers problem. — Dep. Comput. Sci., Courant Inst. Math. Sci., New York Univ., New York, NY, Tech. Rep. 41, Feb. 1982.
[310] Seidel R. A convex hull algorithm optimal for points in even dimensions. — M. S. thesis. Dep. Comput. Sci., Univ. British Columbia, Vancouver, B. C., Canada, Tech. Rep. 81-14, 1981.
[311] Seidel R. The complexity of Voronoi diagrams in higher dimensions. — In: Proc. 20th Allerton Conf. Commun. Control and Comput., 1982, p. 94—95; см. также: Technische Univ. Graz, Graz, Austria, Tech. Rep. F94, July 1982.
[312] Seidel R. A method for lower bounds for certain geometric problems. — Dep. Comput. Sci., Cornell Univ., Ithaca, NY, Tech. Rep. 84-592, Feb. 1984.
[313] Shamos M. I. Geometric complexity. — In: Proc. 7th ACM Annu. Symp. Theory Comput., May 1975, p. 224—233.
[314] Shamos M. I. Geometry and statistics: Problems at the interface. — In: Algorithms and Complexity, J. F. Traub (ed.). — New York: Academic, 1976, p. 251—280.
[315] Shamos M. I. Computational geometry. — Ph. D. dissertation, Dep. Comput. Sci., Yale Univ., New Haven, CT, 1978.
[316] Shamos M. I., Hoey D. Closest-point problems. — In: Proc. 16th IEEE Annu. Symp. Found. Comput. Sci., Oct. 1975, p. 151—162.
[317] Shamos M. I , Hoey D. Geometric intersection problems. — In: Proc. 17th IEEE Annu. Symp. Found Comput. Sci., Oct. 1976, p. 208—215.
[318] Sharir M., Schorr A. On shortest paths in polyhedral spaces. — In: Proc. 16th ACM Annu. Symp. Theory Comput., Apr. 1984, p. 144—153.
[319] Silverman B. W., Titterington D. M. Minimum covering ellipses. — SIAM J. Sci. Statist. Comput., Dec. 1980, v. 1, No. 4, p. 401—409.
[320] Six H. W., Wood D. The rectangle intersection problem revisited. — BIT, 1980, v. 20, p. 426—433.
[321] Six H. W., Wood D. Counting and reporting untersections of *d*-ranges.— IEEE Trans. Comput., 1982, v. C-31, p. 181—187.
[322] Snyder W. E.. Tang D. A. Finding the extrema of a region. — IEEE Trans. Pattern Recog. Mach. Intell., May 1980, v. PAMI-2, p. 266—269; см. также: IEEE Trans. Pattern Recog. Mach. Intell., May 1982, v. PAMI-4, p 309.
[323] Soisalon-Soininen E., Wood D. An optimal algorithm to compute the closure of a set of iso-rectangles. — J. Algorith., June 1984, v. 5, No. 2, p. 199—214.
[324] Steele J. M., Yao A. C. Lower bounds for algebraic decision trees. — J. Algorith., 1982, v. 3, p. 1—8.
[325] Supowit K. J. Grid heuristics for some geometric covering problems. — In: Advances in Computing Research, vol. 1, F. P. Preparata (ed.). — JAI Press, pp. 215—233, 1983, p. 215—233.

[326] Sutherland I., Sproull R., Schumacker R. A characterizition of ten hidden-surface algorithms. — Comput. Surveys, 1974, v. 6, No. 1, p. 1—55.
[327] Tompa T. An optimal solution to a wire-routing problem. — J. Comput. Syst. Sci., 1981, v. 23, p. 127—150.
[328] Toussaint G. T. Pattern recognition and geometrical complexity. — In: Proc. 5th Conf. Pattern Recog., Dec. 1980, p. 1324—1347.
[329] Toussaint G. T. Computational geometric problems in pattern recognition.—In: Pattern Recognition Theory and Applications, J. Kitter (ed.).— Oxford, England: Nato ASI, Apr. 1981.
[330] Toussaint G. T. Solving geometric problems with the rotating calipers. — In: Proc. IEEE MELECON'83, Athens, Greece, May 1983.
[331] Toussaint G. T. An optimal algorithm for computing the minimum vertex distance between two crossing convex polygons. — In: Proc. 21st Allerton Conf. Commun. Control and Comput., Oct. 1983, p. 457—458.
[332] Toussaint G. T. Computing largest empty circle with location constraints. — Int. J. Comput. Inform. Sci., Oct. 1983, v. 12, No. 5, p. 347—358.
[333] Toussaint G. T. A historical note on convex hull finding algorithms. — Pattern Recog. Lett. (будет опубликовано).
[334] Toussaint G. T., Avis D. On a convex hull algorithm for polygons and its applications to triangulation problems. — Pattern Recog., 1982, v. 15, p. 23—29.
[335] Vaishnavi V. Computing point enclosures. — IEEE Trans. Comput., Jan. 1982, v. C-31, p. 22—29.
[336] Vaishnavi V., Wood D. Data structures for the rectangle containment and enclosure problems. — Comput. Graph. Image Processing, 1980, v. 13, p. 372—384.
[337] Vaishnavi V., Wood D. Rectilinear line segment intersection, layered segment trees, and dynamization. — J. Algorith., 1982, v. 3, p. 160—176.
[338] van Emde Boas P. On the $\Omega(n \log n)$ lower bound for convex hull and maximal vector determination. — Inform. Processing Lett., 1980, v. 10, p. 132—136.
[339] van Leeuwen J., Maurer H. A. Dynamic systems of static data structures. — Technische Univ. Graz, Graz, Austria, Rep. 42, 1980.
[340] van Leeuwen J., Overmars M. H. The art of dynamizing. — In: Mathematical Foundations of Computer Science, Lecture Notes in Computer Science, v. 118, J. Gruska and M. Chytil (eds.). — Heidelberg, Germany: Springer-Verlag, 1981, p. 121—131.
[341] van Leeuwen J., Wood D. Dynamization of decomposable searching problems. — Inform. Processing Lett., 1980, v. 10, p. 51—56.
[342] van Leeuwen J., Wood D. The measure problem for rectangular ranges in d-space. — J. Algorith., 1981, v. 2, p. 282—300.
[343] Watson D. F. Computing the n-dimensional Delaunay tessellation with applications to Voronoi Polytopes. — Comput. J., v. 24, No. 2, p. 167—172.
[344] Willard D. E. Predicate-oriented database search algorithms. — Ph. D. dissertation, Harvard Univ., Cambridge, MA, 1978.
[345] Willard D. E. Polygon retrieval. — SIAM J. Comput., 1982, v. 11, p. 149—165.
[346] Willard D. E. New data structures for orthogonal queries. — SIAM J. Comput. (будет опубликовано).
[347] Willard D. E., Lueker G. S. Adding range restriction capability to dynamic data structures. — J. ACM (будет опубликовано).
[348] Yang C. C., Lee D. T. A note on all nearest neighbor problem for convex polygons. — Inform. Processing Lett., Apr. 1979, v. 8, p. 193—194.
[349] Yao A. C. On the complexity of comparison problems using linear functions. — In: Proc. 16th Annu. Symp. Theory Comput., 1975, p. 85—89.

[350] Yao A. C. A lower bound to finding convex hulls. — J. ACM, 1981, v. 28, p. 780—787.
[351] Yao A. C On constructing minimum spanning tree in *k*-dimensional space and related problems. — SIAM J. Comput., 1982, v. 11, No. 4, p. 721—736.
[352] Yao A. C., Rivest R. L. On the polyhedral decision problem. — SIAM J. Comput., 1980, v. 9, p. 343—347.
[353] Yao F. F. A 3-space partition and its applications. — In: Proc. 15th ACM Annu. Symp. Theory Comput., Apr. 1983, p. 258—263.
[354] Yuval G Finding nearest neighbours. — Inform. Processing Lett., 1976, v. 5, No. 3, p. 63—65.

ЛИТЕРАТУРА, ДОБАВЛЕННАЯ ПРИ ПЕРЕВОДЕ

[1*] Абрайтис Л. Б. Автоматизация проектирования топологии цифровых интегральных микросхем. — М.: Радио и связь, 1985.
[2*] Акимова И. Я. Задача оптимального размещения и обобщения одной теоремы Фейеша Тота. — Изв. АН СССР. Техн. кибернет., 1982, № 2.
[3*] Акимова И. Я. Применение диаграмм Вороного в комбинаторных задачах. Обзор. — Изв. АН СССР. Техн. кибернет., 1984, № 2.
[4*] Александров А. Д. Выпуклые многогранники. — М. — Л.: Гостехиздат, 1950.
[5*] Басакер Р., Саати Т. Конечные графы и сети. — М.: Наука, 1974.
[6*] Бахман Ф., Шмидт Э. *n*-угольники. — М.: Мир, 1973.
[7*] Болтянский В. Г., Гохберг И. Ц. Теоремы и задачи комбинаторной геометрии. — М.: Наука, 1965.
[8*] Болтянский В. Г., Солтан П. С. Комбинаторная геометрия различных классов выпуклых множеств. — Кишинев: Штиинца, 1978.
[9*] Буснюк Н. Н., Сарванов В. И. О графах разбиения многоугольников. I. — Изв. АН БССР, сер. физ.-мат. наук, 1985, № 6.
[10*] Буснюк Н. Н., Сарванов В. И. О графах разбиения многоугольников. 2. — Изв. АН БССР, сер. физ.-мат. наук, 1986, № 5.
[11*] Вейль Г. Элементарная теория выпуклых многогранников. — В кн.: Матричные игры. — М.: Физматгиз, 1961.
[12*] Берже М. Геометрия. Т. 1, 2. — М.: Мир, 1984.
[13*] Вороной Г. Ф. Собрание сочинений.— Киев: Изд-во АН УССР, 1952, т. 2.
[14*] Гильберт Д., Кон-Фоссен С. Наглядная геометрия. — М.: Наука, 1981.
[15*] Грюнбаум Б. Этюды по комбинаторной геометрии и теории выпуклых тел. — М.. Наука, 1971.
[16*] Делоне Б. Н., Долбилин Н. П., Рыжков С. С., Штогрин М. И. Новое построение теории решетчатых покрытий *n*-мерного пространства равными шарами. — Изв. АН СССР, сер. матем., 1970, т. 34.
[17*] Делоне Б. Н., Долбилин Н. П., Штогрин М. И. Комбинаторная и метрическая теория планигонов. — Тр. Матем. ин-та. — Л.: Наука, 1978, т. 148.
[18*] Делоне Б. Н., Сандакова Н. Н. Теория стереоэдров. — Тр. Матем. ин-та. — М.: Изд-во АН СССР, 1961, т. 64.
[19*] Донеддю А. Евклидова планиметрия. — М.: Наука, 1978.
[20*] Дорошко К. М. Задачи о магистралях на плоскости. — ДАН БССР, 1985, т. 29, № 10.
[21*] Корнеенко Н. М. Поиск трансверсальных прямых для множеств выпуклых фигур на плоскости. — Изв. АН БССР, сер. физ.-мат. наук, 1986, № 5.

[22*] Корнеенко Н. М., Матвеев Г. В., Метельский Н. Н., Тышкевич Р. И. О разбиениях многоугольников. — Изв. АН БССР, сер. физ.-мат. наук, 1978, т. 23, № 1.
[23*] Ломакина З. Д. Полиэдр Вороного П(n) при $n = 5$ и максимальные группы целочисленных 5×5-матриц. — Тр. Матем. ин-та. — М.: Наука, 1980, т. 152.
[24*] Метельский Н. Н. Метод вычисления расстояний между множествами точек на плоскости. — Изв. АН БССР, сер. физ.-мат. наук, 1985, № 3.
[25*] Минковский Г. Общие теоремы о выпуклых многогранниках. — Успехи матем. наук, 1936, вып. 1, 2.
[26*] Муртаф Б. Современное линейное программирование. — М.: Мир, 1984.
[27*] Никайдо Х. Выпуклые структуры и математическая экономика. — М.: Мир, 1972.
[28*] Пападимитриу Х., Стайглиц К. Комбинаторная оптимизация. Алгоритмы и сложность. — М.: Мир, 1985.
[29*] Петренко А. И., Тетельбаум А. Я., Забалуев Н. Н. Топологические алгоритмы трасировки многослойных печатных плат. — М.: Радио и связь, 1983.
[30*] Рейнгольд Э., Нивергельт Ю., Део Н. Комбинаторные алгоритмы. Теория и практика. — М.: Мир, 1980.
[31*] Рыжков С. С., Барановский Е. П. С-типы n-мерных решеток и пятимерные примитивные параллелоэдры (с приложением к теории покрытий). — Тр. Матем. ин-та. — М., Наука, 1976, т. 137.
[32*] Саати Т. Целочисленные методы оптимизации и связанные с ними экстремальные проблемы. — М.: Мир, 1973.
[33*] Солтан П. С. Экстремальные задачи на выпуклых множествах. — Кишинев: Штиинца, 1976.
[34*] Фейеш Тот Л. Расположения на плоскости, на сфере и в пространстве. — М.: Физматгиз, 1958.
[35*] Фокс А., Пратт М. Вычислительная геометрия. Применение в проектировании и на производстве. — М.: Мир, 1982.
[36*] Фоли Дж., вэн Дэм А. Основы интерактивной машинной графики. Т. 1, 2. — М.: Мир, 1985.
[37*] Хадвигер Г., Дебреннер Г. Комбинаторная геометрия плоскости. — М.: Наука, 1965.
[38*] Хачиян Л. Г. Полиномиальные алгоритмы в линейном программировании. — ЖВМ и МФ, 1980, № 1.
[39*] Ху Т. Целочисленное программирование и потоки в сетях. — М.: Мир, 1974.
[40*] Чарни В. С. Линейные преобразования и выпуклые множества. — Киев: Вища школа, 1978.
[41*] Шкляревский Д. О., Ченцов Н. Н., Яглом И. М. Геометрические оценки и задачи из комбинаторной геометрии — М.: Наука, 1974.
[42*] Штрогин М. И. Правильные разбиения Дирихле — Вороного для второй триклинной группы. — Тр. Матем. ин-та. — М.: Наука, 1973, т. 123.
[43*] Яглом И. М. О комбинаторной геометрии. — М.: Знание, 1971.
[44*] Яглом И. М., Болтянский В. Г. Выпуклые фигуры. — М. — Л.: Гостехиздат, 1951.
[45*] Rosenfeld A. Picture processing: 1985. Survey. — Computer vision, graphics and image processing, 1986, v. 34, No. 2.

Простые монотонные формулы для функции голосования [1]

Л. Вэльянт [2]

Показано, что сложность реализации монотонных симметрических функций от n переменных монотонными формулами ограничена сверху величиной $O(n^{5.3})$.

1. ВВЕДЕНИЕ

Пусть $X=\{x_1, \ldots, x_n\}$ — множество булевых переменных, причем $n=2m$. По определению функция с порогом k (от переменных из X) равна 1 тогда и только тогда, когда k или более ее переменных принимают значение 1 [2]. Ограничимся рассмотрением функции голосования MAJ (majority), которая является функцией с порогом m (от переменных из X). Легко видеть, что любая пороговая функция от n переменных может быть получена подстановкой констант вместо переменных из функции голосования, зависящей не более чем от $2n$ переменных.

Пользуясь техникой динамического программирования, для функции MAJ легко получить формулу, имеющую сложность $\exp(O(\log n)^2)$. При этом не используются тождества булевой алгебры: (i) $x^2=x$; (ii) $xy+x=x$, и, следовательно, то же самое справедливо для монотонной арифметической модели. Шамир и Снир [7] доказали, что в последней модели любая формула для соответствующей функции действительно имеет сложность $\exp(\Omega(\log n)^2)$.

В булевой алгебре формула полиномиальной сложности впервые получена в работе [3]. Работы [4—6] привели к наилучшей известной сейчас верхней оценке $O(n^{3.37})$ [3]. Все эти конструкции используют отрицание. Из недавнего результата

---

[1]) Valiant L. G. Short monotone formulae for the majority function.—Journal of Algorithms, 1984, v. 5, p. 363—366.

[2]) Aiken Computation Laboratory, Harvard University, Cambridge, Massachusetts.

[3]) Эта оценка относится к формулам в базисе из всех двуместных булевых операций. Результат данной статьи еще больше выигрывает, если его сравнивать с формулами в базисе $\{\&, \vee, \bar{\ }\}$, для которых известная верхняя оценка сложности имеет вид $O(n^{4.62})$ [3]. — *Прим. перев.*

Айтаи, Комлоша и Семереди [1] о существовании сортирующих схем глубины $O(\log n)$ вытекает полиномиальная сложность монотонной булевой формулы для функции голосования, однако этот полином имеет очень высокую степень.

Цель данной статьи — доказать существование для функции голосования монотонной булевой формулы сложности $O(n^{5.3})$. Достоинство данной конструкции не только в том, что она уменьшает показатель степени по крайней мере на порядок, но и в ее исключительной простоте. Она показывает удивительную вычислительную мощь монотонной булевой алгебры.

2. РЕЗУЛЬТАТЫ

Мы определим сейчас последовательность $A_0, A_1, \ldots, A_i, \ldots$ распределений вероятностей для монотонных булевых формул над множеством переменных X. Все формулы из A_i с ненулевыми вероятностями будут иметь сложность не больше 2^{2i}. Мы покажем, что при достаточно большом t формула, случайным образом выбранная из A_t, в подавляющем большинстве случаев реализует MAJ.

Распределение A_i определяется с помощью следующей вероятностной конструкции (зависящей от параметра α) для формул $F \in A_i$:

(i) Если $i=0$, то F — либо одна из переменных, либо нуль. Вероятность того, что F есть x_j, при любом j равна $2\alpha/(2m-1)$. Вероятность того, что F есть 0, равна $1-(2\alpha n)/(2m-1)$.

(ii) Если $i>0$, то из A_{i-1} независимо выбирают формулы G^1, G^2, G^3, G^4 и полагают $F=(G^1 \vee G^2)(G^3 \vee G^4)$.

Теорема. *Пусть* $\alpha=(3-\sqrt{5})/2\approx 0.38$ *и* $t=\log_2 n(1+\log_\gamma 2)$, *где* γ — *любое число, удовлетворяющее условию*: $\gamma<4\alpha$. *Тогда при достаточно большом* $n=2m$ *справедливы следующие утверждения*:

(i) *Пусть* $\mathbf{x}_0$ — *набор значений переменных из* X, *содержащий не более* $m-1$ *единиц, а* $\mathbf{x}_1$ — *набор значений переменных из* X, *содержащий не менее* m *единиц. Тогда для формулы* F, *выбранной случайным образом из* A_t, *выполняются неравенства*

$$\mathrm{Prob}\,(F(\mathbf{x}_0)=1)<2^{-n-1}, \quad \mathrm{Prob}\,(F(\mathbf{x}_1)=0)<2^{-n-1}.$$

(ii) *Для формулы* F, *выбранной случайным образом из* A_t, *выполняется неравенство*

$$\mathrm{Prob}\,(F\equiv \mathrm{MAJ})\geqslant 1/2.$$

Доказательство. Вторая часть непосредственно следует из первой, так как вероятность того, что F отличается от MAJ, не

превосходит величины

$$\sum_{\mathbf{x}} \mathrm{Prob}\,(F(\mathbf{x}) \neq \mathrm{MAJ}\,(\mathbf{x})),$$

где суммирование ведется по всем 2^n наборам значений $\mathbf{x}$ переменных из X; а ведь из (i) вытекает, что каждое слагаемое не превосходит 2^{-n-1} и, таким образом, вся сумма не превосходит 1/2.

Для доказательства первой части положим $f_i = \mathrm{Prob}(F(\mathbf{x}_0)=1)$ и $h_i = \mathrm{Prob}\,(F(\mathbf{x}_1)=0)$ при условии, что формула F случайным образом выбрана из A_i. Из рекуррентной конструкции для F немедленно следует, что при $i \geqslant 1$

$$f_i = 1 - (1 - f_{i-1})^{22} = f_{i-1}^4 - 4f_{i-1}^3 + 4f_{i-1}^2, \tag{1}$$

$$h_i = 1 - (1 - h_{i-1}^2)^2 = -h_{i-1}^4 + 2h_{i-1}^2. \tag{2}$$

В промежутке (0, 1) эти рекуррентные соотношения имеют только по одной неподвижной точке: $f_i = \alpha$, $h_i = 1 - \alpha$. Отметим, кроме того, что производная функции f_i по f_{i-1} в точке α равна 4α и производная функции h_i по h_{i-1} в точке $1 - \alpha$ тоже равна 4α.

Идея конструкции состоит в следующем. Мы выбираем A_0 так, чтобы $f_0 = \alpha - \Omega(n^{-1})$ и $h_0 = 1 - \alpha - \Omega(n^{-1})$ соответственно. Соотношения (1) и (2) показывают, что до тех пор, пока $f_i < \alpha - \Omega(1)$ и $h_i < 1 - \alpha - \Omega(1)$, их сдвиги от α и $1 - \alpha$ на каждом шаге являются величинами первого порядка, а после этого их отклонения от нуля являются величинами второго порядка. Это служит гарантией того, что достаточно взять $t = O(\log n)$.

Более точно заметим, что $f_0 = \mathrm{Prob}\,(F(\mathbf{x}_0) = 1)$ при условии, что F выбрана из A_0. Поэтому

$$f_0 \leqslant 2\alpha(m-1)/(2m-1) = \alpha - \alpha/(n-1). \tag{3}$$

Аналогично $h_0 = \mathrm{Prob}\,(F(\mathbf{x}_1) = 0)$ и

$$h_0 \leqslant 1 - 2\alpha m/(2m-1) = 1 - \alpha - \alpha/(n-1). \tag{4}$$

Чтобы убедиться в том, что начальные сдвиги являются величинами первого порядка, заметим следующее: если $f_{i-1} = \alpha - \varepsilon$, то $f_i = \alpha - \varepsilon f_i'(\alpha) + O(\varepsilon^2)$. Таким образом, если $\gamma < f_i'(\alpha) = 4\alpha$, то существует такое ε_0, что при всех $\varepsilon < \varepsilon_0$

$$f_{i-1} = \alpha - \varepsilon \Rightarrow f_i < \alpha - \gamma\varepsilon. \tag{5}$$

При этом же условии

$$h_{i-1} = 1 - \alpha - \varepsilon \Rightarrow h_i < 1 - \alpha - \gamma\varepsilon. \tag{6}$$

Из (3)—(6) следует, что

$$f_i < \alpha - \varepsilon_0 \quad \text{и} \quad h_i < 1 - \alpha - \varepsilon_0,$$

если только i удовлетворяет неравенству $(n^{-1})\gamma^i \geqslant \varepsilon_0$ (т. е. $i = (\log_2 n + \log_2 \varepsilon_0)/\log_2 \gamma$).

За $O(1)$ следующих шагов обе величины f_i и h_i могут быть уменьшены до любой константы, например до 2^{-5} [1]).

Наконец, заметим, что $f_i < 8f_{i-1}^2$ и $h_i < 2h_{i-1}^2$. Отсюда следует, что при $k = 2^{i-j}$

$$f_i \leqslant (8f_j)^k \leqslant 2^{-2k}, \quad \text{если} \quad f_j = 2^{-5}.$$

Таким образом, $i - j = \log_2 n$ следующих итераций достаточно, чтобы уменьшить $f_j = 2^{-5}$ до $f_i < 2^{-n-1}$, как и требовалось. То же верно для h_i.

Итак, $(\log_2 n)/(\log_2 \gamma) + O(1)$ итераций достаточно, чтобы уменьшить f_i и h_i до $\alpha - \Omega(1)$ и $1 - \alpha - \Omega(1)$; $O(1)$ последующих итераций достаточно, чтобы уменьшить их до 2^{-5}, и $\log_2 n$ последних итераций достаточно, чтобы уменьшить их до 2^{-n-1}. Сложность полученной формулы равна $O(n^{2(1+\log_\gamma 2)}) = O(n^{5.3})$. □

ЛИТЕРАТУРА

[1] Ajtai M., Komlós J., Szemerédi E. An $O(n \log n)$ sorting network. — In: Proc. 15th ACM Symp. of Theory of Computing, 1983, p. 1—9.

[2] Хасин Л. С. Оценки сложности реализации монотонных симметрических функций формулами в базисе $\vee$ &, $\neg$. — ДАН СССР, 1969, т. 189, № 4, с. 752—755.

[3] Храпченко В. М. О сложности реализации симметрических функций формулами. — Матем. заметки, 1972, т. 11, № 1, с. 109—120.

[4] Paterson M. S. New bounds on formula size. — Lecture Notes in Computer Science, 1977, No. 48, p. 17—26.

[5] Peterson G. L. An upper bound on the size of formulae for symmetric Boolean functions. — Dept. of Computer Science Tech. Report 78-03-01, University of Washington, Seattle, 1978.

[6] Pippenger N. Short formulae for symmetric functions. — IBM Research Report RC-5143, Yorktown Heights, N. Y., 1974.

[7] Shamir E., Snir M. On the depth complexity of formulas. — Math. Systems Theory, 1980, v. 13, No. 2, p. 301—322. [Имеется перевод: Шамир Э., Снир М. О глубине формул. — В кн.: Кибернетический сборник, вып. 19.— М.: Мир, 1983, с. 71—96.]

---

[1]) В промежутке $[2^{-5}, \alpha - \varepsilon_0]$ величина $f_i - f_{i-1} = f_{i-1}^4 - 4f_{i-1}^3 + 4f_{i-1}^2 - f_{i-1}$ принимает наибольшее значение на одном из концов. Поэтому найдется такое $\delta > 0$, что $f_i - f_{i-1} < -\delta$. Но тогда достаточно $(\alpha - \varepsilon_0 - 2^{-5})$ шагов, чтобы уменьшить f_i от $\alpha - \varepsilon_0$ до 2^{-5}. — *Прим. перев.*

Проверка чисел на простоту и суммы Якоби [1)]

Х. Коэн, Х. Ленстра, мл.

Приводится теоретически и алгоритмически упрощенная версия алгоритма проверки простоты чисел, недавно полученного Аллеманом и Румели. Новый алгоритм хорошо работает на практике. Это первый существующий тест проверки простоты, который без труда исследует числа с сотнями десятичных цифр.

1. ВВЕДЕНИЕ

Большинство современных методов проверки, является ли данное число n простым, основано на теореме Ферма и ее обобщениях. Эта теорема утверждает, что

(1.1) Если n простое, то
$a^n \equiv a \bmod n$ для всех $a \in \mathbb{Z}$.

Таким образом, чтобы доказать, что число составное, достаточно найти единственное целое a, для которого $a^n \not\equiv a \bmod n$; здесь $a^n \bmod n$ может быть эффективно вычислено повторными возведениями в квадрат и умножениями по модулю n. Однако для доказательства того что n простое, нам нужно обращение (1.1). В связи с этим возникают две проблемы. Первая заключается в том, что прямое обращение (1.1) неверно: составные числа

$$n = 561 = 3 \cdot 11 \cdot 17, \qquad n = 1105 = 5 \cdot 13 \cdot 17,$$
$$n = 1729 = 7 \cdot 13 \cdot 19, \qquad n = 2465 = 5 \cdot 17 \cdot 19$$

также обладают тем свойством, что $a^n \equiv a \bmod n$ для всех $a \in \mathbb{Z}$. Такие составные числа называются *числами Кармайкла*, и, вероятно, их бесконечно много.

Вторая проблема состоит в том, что даже если бы обращение (1.1) было верно, это не очень помогло бы, поскольку проверка всех целых $a \pmod n$ вычислительно неосуществима даже для сравнительно небольших n.

[1)] Cohen H., Lenstra H. W., Jr. Primary Testing and Jacobi Sums. — Mathematics of Computation, 1984, v. 42, No. 165. p. 297—330.

Для решения первой проблемы мы заменяем (1.1) более сильным утверждением. Обсудим два способа для этого.

Первый зависит от *символа Якоби* $\left(\frac{a}{n}\right)$, который определен для a, $n \in \mathbb{Z}$, n положительное, НОД$(2a, n) = 1$; см. [5, разд. 9] [1]). Он может быть эффективно вычислен с помощью квадратичного закона взаимности. Из определения $\left(\frac{a}{n}\right)$ следует

(1.2) Если n нечетное простое, то
$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) = \pm 1 \bmod n \text{ для всех } a \in \mathbb{Z}, \text{ НОД}(a, n) = 1.$$

Обращение (1.2) также верно [14, 23]. Точнее, если n нечетное и составное, $n > 1$, то сравнение (1.2) выполняется не более чем для половины всех $a \pmod n$, НОД$(a, n) = 1$.

Другое усиление теоремы Ферма, которое допускает обращение, таково:

(1.3) Если n простое, то для любого коммутативного кольца R имеем $(a + b)^n \equiv a^n + b^n \bmod nR$ для всех a, $b \in R$.

Здесь nR обозначает идеал $\{x + x + \ldots + x$ (n членов): $x \in R\}$ в R. Для доказательства (1.3) нужно только заметить, что биномиальные коэффициенты $\binom{n}{i}$, $0 < i < n$, делятся на n, если n простое. При $R = \mathbb{Z}$ мы получаем (1.1) из (1.3), полагая $b = 1$ и используя индукцию по a.

Можно показать, что обращение (1.3) также верно: если $n > 1$ и сравнение в (1.3) верно для всех коммутативных колец R и всех a, $b \in R$, то n простое. Фактически достаточно взять $R = \mathbb{Z}[X]$, $a = X$, $b = 1$.

Тест проверки простоты, который мы опишем в этой статье, комбинирует (1.2) и (1.3): сравнения, на которых основан наш тест, получаются из (1.3) и обобщают (1.2).

Перед нами все еще стоит вторая проблема: вычислительно невозможно ни проверить сравнение в (1.2) для всех $a \pmod n$, НОД$(a, n) = 1$, ни проверить сравнение в (1.3) для всех R, a, b. Чтобы обойти эту трудность, было предложено несколько методов. Первый должен пожертвовать уверенностью: если n проходит тест в (1.2) для 100 случайно выбранных значений $a \in \{1, 2, \ldots, n-1\}$, то почти наверняка n простое. Более сильный тест этого типа, принадлежащий Миллеру и Рабину, читатель может найти в [19, 21, 8].

Второй метод связан с будущим развитием аналитической теории чисел: если обобщенная гипотеза Римана верна и n не-

---

[1]) См. также: Виноградов И. М. Основы теории чисел. — М.: 1977.—*Прим. перев.*

четное целое >1, которое проходит тест в (1.2) для всех простых a, не делящих n, $a \leqslant 70(\log n)^2$, то n — простое число (ср. [19, 24]). Но даже если бы обобщенная гипотеза Римана была доказана, практическое значение этого метода находилось бы под вопросом. Для обычных 100-разрядных чисел этот метод примерно в 500 раз медленнее, чем алгоритм, описанный в данной статье; хотя асимптотически он быстрее.

Предлагаемый метод в настоящее время единственный, который ведет к строгим доказательствам простоты. Он состоит в испытании числа n серией тестов, подобных (1.2) и (1.3), со следующими двумя свойствами. Во-первых, если n простое, оно проходит все тесты. Во-вторых, если n проходит тесты, то накапливается информация о возможных делителях n. Эта информация непосредственно ведет к заключению, что 1 и n — единственные делители n, так что n простое.

Для описания типа получаемой информации обозначим через H группу и через ψ отображение из множества делителей n в H с тем свойством, что $\psi(rr') = \psi(r)\psi(r')$, если rr' делит n. Если n проходит тесты, то отсюда вытекает, что при подходящем выборе H и ψ имеем

(1.4) $\psi(r)$ есть *степень* $\psi(n)$ для каждого делителя r числа n.

Поэтому оказывается, что мы пытаемся доказать простоту n с помощью следующего тривиального критерия простоты:

(1.5) Целое число $n > 1$ простое тогда и только тогда, когда все делители n есть степени n.

Приведенное выше общее описание алгоритма применимо, в частности, к тестам Лукаса и Лемера, улучшенным Бриллхартом, Лемером и Селфриджем [2] и обобщенным Уильямсом (см. ссылки в [26]). В этих тестах полагают $H = (\mathbb{Z}/s\mathbb{Z})^*$, группу обратимых элементов в $\mathbb{Z}/s\mathbb{Z}$, где s — целое число, которое строится из известных простых делителей $n^t - 1$ для $t = 1, 2, 3, 4, 6$, и полагают $\psi(r) = (r \bmod s)$ для r, делящих n. Если (1.4) верно при этом выборе H и ψ и s достаточно велико, например $s > n^{1/2}$, то легко найти все делители n и, в частности, решить, является ли n простым. В [16, разд. 8] показано, как могут быть использованы бо́льшие значения t. Обсуждение этих тестов с точки зрения теории алгебраических чисел читатель может найти в [17]; здесь H возникает как группа Галуа подходящего расширения поля рациональных чисел $\mathbb{Q}$ и ψ есть символ Артина.

Тест простоты, который был недавно изобретен Адлеманом и Румели [1, разд. 4], также подходит под приведенное выше описание, хотя это может быть неясно из того вида, в котором

он сформулирован в [1]. В этом алгоритме проверяют набор сравнений, включающих суммы Якоби в круговых полях. Используя высшие законы взаимности из теории алгебраических чисел, показывают, что любое n, удовлетворяющее всем этим сравнениям, также удовлетворяет (1.4) при $H=(\mathbb{Z}/s\mathbb{Z})^*$, $\psi(r)=(r \bmod s)$ с некоторым вспомогательным числом s, взаимно простым с n. Это число s есть свободное от квадратов целое, большее $n^{1/2}$, и выбирается таким образом, что

$$a^t \equiv 1 \bmod s \text{ для всех } a \in \mathbb{Z},\ \text{НОД}(a, s)=1,$$

где t — сравнительно малое свободное от квадратов положительное целое число.

В этой статье мы даем теоретически и алгоритмически упрощенную версию теста Адлемана и Румели. Теоретическое упрощение достигнуто, как и в [16], рассмотрением сумм Гаусса вместо сумм Якоби. Это позволяет нам пройти мимо высших законов взаимности, которые были использованы в [1]. Наш подход имеет дополнительное преимущество, заключающееся в работе также и с не свободными от квадратов числами t и s.

С алгоритмической точки зрения суммы Гаусса, появляющиеся в нашем тесте, состоят в подчиненном отношении к суммам Якоби из [1], поскольку последние принадлежат к значительно меньшим кольцам. По этой причине важно переформулировать наш тест посредством сумм Якоби. Это делается с помощью техники, которая известна из теории круговых полей. Переформулировка заключается в сравнениях, включающих суммы Якоби, проверить которые легче, чем сравнения, возникающие в [1].

Далее будет видно, что утверждения вида (1.4) играют важную роль в этой статье. Выбор $H=(\mathbb{Z}/s\mathbb{Z})^*$, $\psi(r)=(r \bmod s)$ был уже упомянут. Далее мы рассмотрим $H=\mathbb{C}^*$, мультипликативную группу ненулевых комплексных чисел, и ψ, равное характеру, определенному в разд. 6. Наконец, для нескольких малых простых чисел p мы возьмем $H=\mathbb{Z}_p^*$, группу p-адических единиц, рассматриваемую в разд. 5; в этом случае ψ определяется равенством $\psi(r)=r^{p-1}$.

В. Дюбюк запрограммировал тест Адлемана и Румели для компьютера DEC KL-10 в Массачусетском технологическом институте. Он использовал его для доказательства простоты 62-цифрового числа в течение 6 ч. Это неудачное сравнение с предыдущими тестами, описанными Уильямсом [26]. Фактически Уильямсу никогда не встречалось простое число такого размера, которое заняло бы более 20 мин для доказательства простоты на компьютере Amdahl 470-V7. С другой стороны, прежние тесты для достаточно больших n. Следует

также принять во внимание, что алгоритм Дюбюка использует стандартные программы большой точности из Маклиспа, что, конечно, не самое эффективное возможное средство.

Наш алгоритм был выполнен на вычислительной системе CDC Cyber 170-750 в вычислительном центре SARA в Амстердаме. Были написаны две программы, одна на Паскале, другая на Фортране; обе программы использовали программы большой точности в Компассе. Программа на Паскале является первой существующей программой проверки простоты, которая легко может работать с числами до 100 десятичных разрядов и делает это примерно в пределах 45 с. Программа на Фортране может работать с числами, содержащими в записи до 200 цифр, и делает это примерно в пределах 10 мин.

Алгоритм этой статьи был предназначен для достижения наибольшей эффективности на практике. Однако трудно установить строгую верхнюю оценку для времени работы. Время работы алгоритма из [1, разд. 4] было проанализировано Померансом и Одлизко (см. [1, теорема 1, 3]). Они доказали, что для каждого $n > e^e$ алгоритм заканчивает работу в пределах $O(k(\log n)^{c \log\log\log n})$ шагов с вероятностью не менее $1-2^{-k}$ для каждого $k \geqslant 1$; здесь c — абсолютная эффективно вычислимая постоянная. Можно показать, что та же верхняя оценка верна для подходящей версии нашего алгоритма, ср. (11.6) (b). Для другой версии верхняя оценка $O((\log n)^{c \log\log\log n})$ может быть строго доказана при допущении справедливости расширенной гипотезы Римана. Мы не входим в детали этого анализа, поскольку существует иной алгоритм, для которого эта верхняя оценка может быть доказана без каких-либо недоказанных допущений. Этот алгоритм, также принадлежащий Адлеману и Румели, описан в [1, разд. 5], а его упрощенная версия — в [16, разд 5]. Однако это не имеет практического значения.

Данная статья черпает некоторое количество технических приемов из алгебры и теории чисел, которые не использовались традиционно в тестах простоты. Мы поэтому попытались сделать изложение по возможности более целостным. Содержание статьи состоит в следующем.

Краткое описание нашего алгоритма в трех стадиях дано в разд. 2; разд. 3 посвящен последней стадии, разд. 4 — первой. Центральная стадия описана в разд. 5—11. В разд. 5 и 6 мы собрали свойства p-адических чисел и характеров, которые нам необходимы. В разд. 7 мы показали, как суммы Гаусса можно использовать для обобщения теста в (1.2). Переформулировка посредством сумм Якоби описана в разд. 8 и 9. В разд. 10 мы увидим, как алгоритмы, связанные с конечными полями, ведут к дополнительным улучшениям при некоторых условиях. Наконец, в разд. 11 описывается центральная стадия алгоритма про-

верки простоты. Детальное описание всего алгоритма с вычислительной точки зрения содержится в разд. 12. Проведенное на практике осуществление обсуждается в разд. 13.

Мы обозначим через $\mathbb{Z}$, $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{C}$ кольцо целых чисел, кольцо целых p-адических чисел (см. разд. 5), поле рациональных чисел и поле комплексных чисел соответственно. Кратность вхождения простого числа p в m обозначается через $v_p(m)$ для $m \in \mathbb{Z}$, $m \neq 0$ (ср разд. 5). Под $r|m$ мы подразумеваем, что r делитель m, т. е. *положительное* целое, делящее m. Кольца подразумеваются коммутативными с 1, и подкольца имеют ту же 1. Группа обратимых элементов кольца R обозначается через R^*. Обозначения ζ_n, U_m, σ_x, G см. в разд. 7.

2. ОБЩАЯ СХЕМА АЛГОРИТМА

Мы даем краткое описание трех стадий нашего алгоритма проверки простоты. Пусть n — целое число, простоту которого надо проверить, и предположим, что $n > 1$.

Стадия 1. Выбрать два положительных целых числа t и s со следующими свойствами:

(2.1) t мало (см. разд. 4),

(2.2) $s > n^{1/2}$ (или $s > n^{1/3}$, см. разд. 3),

(2.3) $a^t \equiv 1 \bmod s$ для всех $a \in \mathbb{Z}$, НОД$(a, s) = 1$,

(2.4) полное разложение t и s на простые сомножители известно.

См. в разд. 4 подробности относительно выбора t и s.

Продолжая стадию 1, проверить, что НОД$(st, n) = 1$, используя алгоритм Евклида; если НОД$(st, n) \neq 1$, то простой множитель n находят по (2.4), и алгоритм останавливается.

Стадия 2. Подвергнуть n серии тестов, подобных тесту в (1.2). Если оно не проходит какой-либо из этих тестов, то n составное и алгоритм останавливается. В противном случае пытаться доказать следующее утверждение, используя информацию, полученную из тестов:

(2.5) для каждого делителя r числа n существует $i \in \{0, 1, \ldots, t-1\}$, такое, что $r \equiv n^i \bmod s$.

Существует теоретическая возможность того, что эта попытка окажется безуспешной по причине нехватки времени. В этом случае можно указать алгоритму остановиться с выдачей сообщения о том, что он оказался неспособен решить, является n простым или нет.

Более детальное описание стадии 2 см. в разд. 11.

Стадия 3. Если (2.5) доказано, использовать (2.5) и (2.2) для полного разложения n и, следовательно, решить, простое n или нет. В разд. 3 мы увидим, как это можно сделать.

Замечание. Из описания стадии 3 не должно создаться впечатление, что алгоритм полезен при разложении n на множители, если n составное, поскольку практически все составные числа будут исключены на стадии 1 или 2.

3. ФИНАЛЬНАЯ СТАДИЯ АЛГОРИТМА

Предположим, что (2.5) доказано и что $s > n^{1/2}$. Чтобы полностью разложить n, достаточно найти все делители $r \leqslant n^{1/2}$ числа n. Такой делитель удовлетворяет неравенству $r < s$ и, согласно (2.5), сравним с $n^i \bmod s$ при некотором $i \in \{0, 1, \ldots, t-1\}$. Следовательно, если мы определим r_i из $r_i \equiv n^i \bmod s$, $0 \leqslant r_i < s$, $0 \leqslant i < t$, и проверим, какие из r_i делят n, то получим полное разложение на простые сомножители числа n.

Допустим далее, что кроме (2.5) известна лишь более слабая версия $s > n^{1/3}$ в (2.2). Тогда разложение n на простые сомножители находят применением следующего результата к $d = r_i$, $i = 0, 1, \ldots, t-1$; заметим, что НОД$(r_i, s) = 1$, поскольку на стадии 1 мы проверили, что НОД$(st, n) = 1$.

(3.1) **Теорема.** *Пусть d, s, n — положительные целые числа, удовлетворяющие условиям* НОД$(d, s) = 1$ *и* $s > n^{1/3}$. *Тогда существует не более* 11 *делителей числа n, которые сравнимы с d по модулю s, и существует эффективный алгоритм, определяющий все эти делители.*

Доказательство этой теоремы и описание алгоритма читатель найдет в [15]. Время работы алгоритма, измеренное в битовых операциях, есть $O((\log n)^3)$, если $d < s < n$. Его практическое значение пока не исследовано.

4. ВЫБОР ВСПОМОГАТЕЛЬНЫХ ЧИСЕЛ

Для положительного целого числа t определим

$$e(t) = 2, \text{ если } t \text{ нечетно},$$

$$e(t) = 2 \prod_{\substack{q \text{ простое} \\ q-1 \mid t}} q^{v_q(t)+1}, \text{ если } t \text{ четно},$$

где $v_q(t)$ определено в введении. Напомним, что для вспомогательных чисел t и s должно выполняться условие

$$a^t \equiv 1 \bmod s \quad \text{для всех} \quad a \in \mathbb{Z}, \ \text{НОД}(a, s) = 1.$$

(4.1) **Предложение.** *Пусть t и s — положительные целые числа. Условие* (2.3) *выполняется тогда и только тогда, когда s делит $e(t)$.*

Доказательство. Для нечетных t это доказывается взятием $a=-1$ в (2.3). Пусть теперь t четно. Мы можем, очевидно, предположить, что s равно степени простого числа: $s=q^m$, q простое и $m \geqslant 1$. В этом случае предложение легко выводится из следующего хорошо известного результата [5, разд. 5]. Если q нечетное или $m \leqslant 2$, то $(\mathbb{Z}/q^m\mathbb{Z})^*$ — циклическая группа порядка $(q-1)q^{m-1}$; если $m \geqslant 3$, то $(\mathbb{Z}/2^m\mathbb{Z})^*$ — прямая сумма группы порядка 2 и циклической группы порядка 2^{m-2}. Это доказывает предложение (4.1).

(4.2) Мы сейчас опишем выбор t и s на стадии 1.

Сначала выбирают положительное целое число t, для которого $e(t) > n^{1/2}$ или $e(t) > n^{1/3}$, в зависимости от того, какой алгоритм используется на стадии 3. Теоретически это можно сделать последовательным испытанием $t=1, 2, 3 \ldots$. На практике удобнее использовать таблицу, вычисленную раз и навсегда, которая дает значения $e(t)$ для некоторых удачно выбранных целых t. Примером служит табл. 1; значения $e(t)$ в ее нижней части округлены. Из табл. 1 видно, что при $n < 10^{100}$ можно взять $t=5040$, если на стадии 3 используется безыскусственный алгоритм, в то время как достаточно $t=1680$, если используется алгоритм из (3.1).

Для значения t, которое выбрано, мы выписываем полное разложение $e(t)$ на простые сомножители. Это делается выписыванием всех простых q, для которых $q-1$ делит t, вместе с показателем $m(q)$ числа q в $e(t)$; этот показатель может быть прочитан из определения $e(t)$. Удобно также выписать разложения на простые сомножители чисел $q-1$, поскольку они нужны на стадии 2. Для $=5040=2^4\ 3^2\cdot 5\cdot 7$ все это сделано в табл. 2. Эта таблица, конечно, является побочным продуктом вычислений, ведущих к табл. 1.

Теперь мы должны выбрать s. Один способ сделать это состоит в следующем. Сначала положим $s=e(t)$. Если s имеет множителем степень простого числа $q^{m(q)}$, для которой $s/q^{m(q)}$ все еще больше $n^{1/2}$ (или $n^{1/3}$ в зависимости от стадии 3), то мы выбираем такое $q^{m(q)}$ с наибольшим возможным q и заменяем s на $s/q^{m(q)}$. Это повторяется до тех пор, пока не станет невозможным.

Опишем лучший способ выбора s. Запишем $e(t)=\prod_{q\in E} q^{m(q)}$. Мы ограничиваемся делителями s числа $e(t)$ формы $s=\prod_{q\in S} q^{m(q)}$, где $S\subset E$. Как мы увидим в разд. 11, каждое $q\in S$ приводит к некоторому объему работы на стадии 2 ал-

Таблица 1

Значения $e(t)$

t	$e(t)$
2	24
$12 = 2^2 \cdot 3$	65 520
$60 = 2^2 \cdot 3 \cdot 5$	$6.814 \cdot 10^9$
$180 = 2^2 \cdot 3^2 \cdot 5$	$2.601 \cdot 10^{15}$
$840 = 2^3 \cdot 3 \cdot 5 \cdot 7$	$8.644 \cdot 10^{24}$
$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$	$1.147 \cdot 10^{31}$
$1680 = 2^4 \cdot 3 \cdot 5 \cdot 7$	$2.697 \cdot 10^{33}$
$2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$	$4.866 \cdot 10^{40}$
$5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$	$1.532 \cdot 10^{52}$
$15120 = 2^4 \cdot 3^3 \cdot 5 \cdot 7$	$2.254 \cdot 10^{79}$
$55440 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	$4.320 \cdot 10^{106}$
$110880 = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	$2.109 \cdot 10^{137}$
$720720 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$2.599 \cdot 10^{237}$
$1441440 = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$1.669 \cdot 10^{301}$
$4324320 = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$7.928 \cdot 10^{455}$
$24504480 = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$4.795 \cdot 10^{656}$
$73513440 = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$7.082 \cdot 10^{966}$
$367567200 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$6.208 \cdot 10^{1501}$
$1396755360 = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$4.016 \cdot 10^{1913}$
$6983776800 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$7.471 \cdot 10^{3010}$

Таблица 2

Разложение на простые сомножители e (5040),
$5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$

$q^m(q)$	$q-1$	$q^m(q)$	$q-1$	$q^m(q)$	$q-1$
2^6	1	31	$2 \cdot 3 \cdot 5$	181	$2^2 \cdot 3^2 \cdot 5$
3^3	2	37	$2^2 \cdot 3^2$	211	$2 \cdot 3 \cdot 5 \cdot 7$
5^2	2^2	41	$2^3 \cdot 5$	241	$2^4 \cdot 3 \cdot 5$
7^2	$2 \cdot 3$	43	$2 \cdot 3 \cdot 7$	281	$2^3 \cdot 5 \cdot 7$
11	$2 \cdot 5$	61	$2^2 \cdot 3 \cdot 5$	337	$2^4 \cdot 3 \cdot 7$
13	$2^2 \cdot 3$	71	$2 \cdot 5 \cdot 7$	421	$2^2 \cdot 3 \cdot 5 \cdot 7$
17	2^4	73	$2^3 \cdot 3^2$	631	$2 \cdot 3^2 \cdot 5 \cdot 7$
19	$2 \cdot 3^2$	113	$2^4 \cdot 7$	1009	$2^4 \cdot 3^2 \cdot 7$
29	$2^2 \cdot 7$	127	$2 \cdot 3^2 \cdot 7$	2521	$2^3 \cdot 3^2 \cdot 5 \cdot 7$

горитма. Время, требуемое на эту работу, пропорционально числу $w(q)$, зависящему от q. Числа $w(q)$ зависят от выполнения стадии 2 и лучше всего определяются эмпирически. Для некоторого безыскусственного выполнения хорошее приближение к $w(q)$ дается суммой

$$\sum_{\substack{p \text{ простое} \\ p \mid q-1}} \varphi\left(p^{v_p(q-1)}\right)^2,$$

где φ — функция Эйлера [4, разд. 5.5]. Для того чтобы минимизировать время работы, мы должны теперь выбрать S так, чтобы $\sum_{q \in S'} w(q)$ была столь малой, насколько возможно, при ограничении $s > n^{1/2}$ или $n^{1/3}$. Полагая $S' = E - S$, мы видим, что следует максимизировать $\sum_{q \in S'} w(q)$ при условии

$$\sum_{q \in S'} \log\left(q^{m(q)}\right) < \log\left(e(t)\right) - \left(\tfrac{1}{2} \text{ или } \tfrac{1}{3}\right) \log n.$$

Это пример *проблемы рюкзака*. Хорошо известный метод приближенного решения этой проблемы приводит к следующему способу выбора s. Сначала положим $s = e(t)$. Если s имеет множителем степень простого числа $q^{m(q)}$, для которой $s/q^{m(q)}$ все еще больше, чем $n^{1/2}$ или $n^{1/3}$, то мы выбираем такое число $q^{m(q)}$с максимально возможной величиной $w(q)/\log(q^{m(q)})$ и заменяем s на $s/q^{m(q)}$. Это повторяется до тех пор, пока возможно. Более тонкие методы решения проблемы рюкзака см. в [18].

Конечное значение s есть делитель $e(t)$, так что, согласно предложению (4.1), условие (2.3) выполнено. Условия (2.2) и (2.4) также выполнены, и ниже мы увидим, какое содержание имеет (2.1). Этим заканчивается описание алгоритма (4.2).

Мы сейчас обсудим, насколько малым может быть взято значение t, чтобы выполнялось $e(t) > n^{1/2}$ или $n^{1/3}$. Из

$$e(t) \leqslant 2t \prod_{d \mid t} (d+1)$$

и элементарных оценок функции делителя [4, теорема 317] мы получаем следующую нижнюю оценку:

$$t > (\log n)^{(1-\varepsilon)(\log\log\log n)/2}$$

для всех $\varepsilon > 0$ и всех n, больших некоторой границы, зависящей от ε. Следующая теорема показывает, что этот результат наилучший возможный, за исключением величины константы в показателе.

(4.3). **Теорема.** *Существует эффективно вычислимая положительная постоянная c, такая, что для всех $n > e^e$ найдется*

положительное целое число t, удовлетворяющее неравенствам

$$t < (\log n)^{c \log\log\log n}, \quad e(t) > n^{1/2}.$$

Это уточнение результата Прахара [20], принадлежащее Померансу и Одлизко. Доказательство см. в [1, разд. 6]. Померанс и Одлизко доказали, что t может быть выбрано даже свободным от квадратов; это было необходимо для теста Адлемана и Румели [1].

5. p-АДИЧЕСКИЕ ЧИСЛА

Пусть p — простое число. В этом разделе мы напомним без доказательств несколько основных свойств *p-адических чисел*. Более полное описание см. в [22, гл. 2] и [6].

p-адическое целое число есть последовательность

$$(a_i \bmod p^i)_{i=1}^{\infty}, \quad (a_i \bmod p^i) \in \mathbb{Z}/p^i\mathbb{Z},$$

такая, что $a_{i+1} \equiv a_i \bmod p^i$ для всех $i \geqslant 1$. Множество целых p-адических чисел образует кольцо, обозначаемое через $\mathbb{Z}_p$, с покоординатным сложением и умножением. Мы рассматриваем $\mathbb{Z}$ как подкольцо $\mathbb{Z}_p$, отождествляя $a \in \mathbb{Z}$ с $(a \bmod p^i)_{i=1}^{\infty} \in \mathbb{Z}_p$.

Пусть $m \in \mathbb{Z}$, $m \geqslant 1$. Отображение $\mathbb{Z}_p \to \mathbb{Z}/p^m\mathbb{Z}$, которое переводит $(a_i \bmod p^i)_{i=1}^{\infty}$ в $(a_m \bmod p^m)$, есть сюръективный кольцевой гомоморфизм с ядром, равным $p^m\mathbb{Z}_p$. Это показывает, что $\mathbb{Z}_p/p^m\mathbb{Z}_p \simeq \mathbb{Z}/p^m\mathbb{Z}$, поэтому p-адические целые числа, взятые по модулю p^m, образуют обычные целые числа по модулю p^m.

Пусть E — конечная абелева группа порядка, равного степени p. Для $a = (a_i \bmod p^i)_{i=1}^{\infty} \in \mathbb{Z}_p$ и $\zeta \in E$ элемент ζ^{a_m} группы E не зависит от m при достаточно больших m, и мы обозначаем его ζ^a. Эта операция из $\mathbb{Z}_p$ над E удовлетворяет известным правилам

$$(\zeta\eta)^a = \zeta^a\eta^a, \quad \zeta^{a+b} = \zeta^a\zeta^b,$$
$$\zeta^{ab} = (\zeta^a)^b, \qquad \zeta^1 = \zeta$$

при $\zeta, \eta \in E$, $a, b \in \mathbb{Z}_p$, поэтому она превращает E в *модуль* над $\mathbb{Z}_p$; см. [10, гл. III, разд. 1].

Целое p-адическое число a есть *обратимый элемент* $\mathbb{Z}_p$ тогда и только тогда, когда $a \not\equiv 0 \bmod p$; следовательно, $\mathbb{Z}_p^* = \mathbb{Z}_p - p\mathbb{Z}_p$. Каждое ненулевое p-адическое целое число a может быть единственным способом записано в виде $a = p^m u$, $m \in \mathbb{Z}$, $m \geqslant 0$, $u \in \mathbb{Z}_p^*$; в этом случае запишем $v_p(a) = m$, и пусть $v_p(0) = \infty$. Это обобщает функцию v_p, которая была определена в ведении на $\mathbb{Z} - \{0\}$.

Множество $1+p\mathbb{Z}_p=\{a\in\mathbb{Z}_p\colon a\equiv 1 \bmod p\}$ есть подгруппа в $\mathbb{Z}_p^*$. Пусть $a=(a_i)_{i=1}^{\infty}\in 1+p\mathbb{Z}_p$. Тогда каждое a_i имеет порядок, равный степени p в $(\mathbb{Z}/p^i\mathbb{Z})^*$; поэтому для $x\in\mathbb{Z}_p$ мы можем определить $a^x=(a_i^x)_{i=1}^{\infty}$. Это превращает $1+p\mathbb{Z}_p$ в $\mathbb{Z}_p$-модуль. Обозначая $a^{\mathbb{Z}_p}=\{a^x\colon x\in\mathbb{Z}_p\}$, мы имеем

(5.1) $\quad a^{\mathbb{Z}_p}=1+p^m\mathbb{Z}_p$ при $m=v_p(a-1)$

при условии, что $m\geqslant 1$ и $m\geqslant 2$ в случае $p=2$.

Имеют место следующие изоморфизмы групп:

(5.2) $\quad \mathbb{Z}_p^*\simeq(\mathbb{Z}/(p-1)\mathbb{Z})\times(1+p\mathbb{Z}_p)\simeq$
$\quad\simeq(\mathbb{Z}/(p-1)\mathbb{Z})\times\mathbb{Z}_p$ при $p\geqslant 3$,

(5.3) $\quad \mathbb{Z}_2^*=1+2\mathbb{Z}_2\simeq\{1,-1\}\times(1+4\mathbb{Z}_2)\simeq(\mathbb{Z}/2\mathbb{Z})\times\mathbb{Z}_2$;

см. [22, разд. II.3], [6, гл. 15, разд. 7].

6. ХАРАКТЕРЫ

Пусть q — простое число. *Характер* χ по модулю q есть групповой гомоморфизм из $(\mathbb{Z}/q\mathbb{Z})^*$ в $\mathbb{C}^*$. Расширим такой характер до отображения $\mathbb{Z}/q\mathbb{Z}-\mathbb{C}$, полагая $\chi(0 \bmod q)=0$, и положим $\chi(a)=\chi(a \bmod q)$ для $a\in\mathbb{Z}$. Множество всех характеров по модулю q образует группу по умножению. Обозначим эту группу X_q.

Хорошо известно, что $(\mathbb{Z}/q\mathbb{Z})^*$ — циклическая группа порядка $q-1$. Пусть образующий элемент g выбран. Отображая χ в $\chi(g)$, получаем изоморфизм между X_q и группой корней $(q-1)$-й степени из единицы. Отсюда легко следует

(6.1) Если $x, y\in(\mathbb{Z}/q\mathbb{Z})^*$ таковы, что $\chi(x)=\chi(y)$ для всех $\chi\in X_q$, то $x=y$.

Пусть $q-1=\prod_{p \text{ простое}} p^{k(p)}$ — разложение $q-1$ на простые сомножители, $k(p)=v_p(q-1)$. Для каждого простого p, такого, что $k(p)\geqslant 1$, мы выбираем характер $\chi_{p,q}\in X_q$ порядка $p^{k(p)}$; этот характер получают, полагая $\chi_{p,q}(g)=\zeta_{p^{k(p)}}$ равным примитивному корню степени $p^{k(p)}$ из единицы Запишем

(6.2) $\quad Y_q=\{\chi_{p,q}\colon p \text{ простое}, p\mid q-1\}$.

Легко видеть, что Y_q порождает группу X_q.

(6.3) **Теорема.** *Пусть t и s — положительные целые числа, удовлетворяющие* (2.3), *и пусть n — целое число, $n>1$,*

НОД$(n, st) = 1$. *Обозначим*

$$Y_s = \bigcup_{q \mid s,\ q \text{ простое}} Y_q,$$

где Y_q *определяются по* (6.2). *Допустим, что любое простое число* $p \mid t$ *удовлетворяет следующему условию*:

(6.4) *Для каждого простого делителя* r *числа* n *существует* $l_p(r) \in \mathbb{Z}_p$, *такое, что* $r^{p-1} = (n^{p-1})^{l_p(r)}$ *в группе* $1 + p\mathbb{Z}_p$.

Допустим, более того, что каждый $\chi \in Y_s$ *удовлетворяет следующему условию*:

(6.5) *Для каждого простого делителя* r *числа* n $\chi(r) = \chi(n)^{l_p(r)}$, *где* $l_p(r)$ *то же, что в* (6.4), *и* p *такое, что порядок* χ *есть степень* p.

Тогда выполнено (2.5), *т. е. для каждого делителя* r *числа* n *существует* $i \in \{0, 1, \ldots, t-1\}$, *такое, что* $r \equiv n^i \bmod s$.

Замечание. Заметим, что $l_p(r)$ в (6.4) однозначно определено, если оно существует, по (5.2), (5.3). В самом деле, мы имеем $l_p(r) = \log_p r / \log_p n$, где $\log_p$ обозначает p-адический логарифм [25, разд. 5.1]. В (6.5) имеет смысл говорить о $l_p(r)$, ибо при $\chi = \chi_{p,q}$ число p делит t по (4.1).

Доказательство. Согласно (2.3), $n^t \equiv 1 \bmod s$, поэтому достаточно рассмотреть *простые* делители r числа n. Фиксируем такое r, и пусть $l(r)$ — неотрицательное целое число, удовлетворяющее сравнениям $l(r) \equiv l_p(r) \bmod p^{h(p)}$ для каждого простого $p \mid t$; здесь $h(p)$ обозначает положительное целое число, которое выбирается достаточно большим, чтобы последующие доводы имели смысл. В частности, мы предполагаем, что порядок каждого $\chi_{p,q} \in Y_s$ делит $p^{h(p)}$. Тогда по (6.5) мы имеем

$$\chi_{p,q}(r) = \chi_{p,q}(n)^{l_p(r)} = \chi_{p,q}(n)^{l(r)} = \chi_{p,q}(n^{l(r)})$$

для каждого $\chi_{p,q} \in Y_s$. Пусть теперь $q \mid s$ — фиксированное простое число. Тогда характеры $\chi_{p,q}$ порождают X_q, поэтому $\chi(r) = \chi(n^{l(r)})$ для всех $\chi \in X_q$. Согласно (6.1), это означает, что $r \equiv n^{l(r)} \bmod q$. Положим $m(q) = v_q(s)$. Мы утверждаем, что

(6.6) $$r \equiv n^{l(r)} \bmod q^{m(q)}.$$

При $m(q) = 1$ это было только что доказано. Допустим поэтому, что $m(q) \geqslant 2$. Тогда, согласно (4.1) и определению $e(t)$, q делит t, поэтому (6.4) выполнено для $p = q$. Отсюда следует

$$r^{q-1} = (n^{q-1})^{l_q(r)} \equiv (n^{q-1})^{l(r)} \bmod q^{m(q)};$$

здесь $h(q)$ предполагается столь большим, что

$$(n^{q-1})\, q^{h(q)} \equiv 1 \bmod q^{m(q)}.$$

Теперь мы знаем, что q-адическое целое число $a = rn^{-l(r)}$ удовлетворяет сравнениям

$$a \equiv 1 \bmod q, \quad a^{q-1} \equiv 1 \bmod q^{m(q)}.$$

Из последнего сравнения следует, что мультипликативный порядок числа a по модулю $q^{m(q)}$ делит $q-1$, а из первого, что он равен степени q. Значит, этот порядок равен 1, т. е. $a \equiv 1 \bmod q^{m(q)}$. Это доказывает (6.6).

Поскольку (6.6) выполняется для любого простого числа q, делящего s, то мы можем заключить, что $r \equiv n^{l(r)} \bmod s$. Здесь $l(r)$ может быть приведено по модулю t, поскольку $n^t \equiv 1 \bmod s$ в силу (2.3). Это доказывает теорему (6.3).

(6.7) *Замечание.* Если (6.4) выполнено, то, очевидно, для любого делителя r числа n существует $l_p(r) \in \mathbb{Z}_p$, такое, что $r^{p-1} = (n^{p-1})^{l_p(r)}$, и мы имеем

$$l_p(r_1 r_2) = l_p(r_1) + l_p(r_2) \text{ для } r_1 r_2, \text{ делящего } n, \; l_p(n) = 1.$$

7. СУММЫ ГАУССА

Для каждого положительного целого числа m обозначим через U_m группу корней m-й степени из единицы в $\mathbb{C}$ и через ζ_m примитивный корень m-й степени из единицы; т. е. ζ_m порождает U_m.

В этом разделе мы фиксируем простое число q, простое число p и положительное целое k, такое, что p^k делит $q-1$. Далее, n — целое число, $n > 1$, и НОД$(n, pq) = 1$.

Мы полагаем $A = \mathbb{Z}[\zeta_{p^k}, \zeta_q]$, кольцо, порожденное ζ_{p^k} и ζ_q, и $K = \mathbb{Q}(\zeta_{p^k}, \zeta_q)$, поле дробей из A. Пусть B — подкольцо $A[1/q]$ в K. Каждый элемент K имеет единственное представление вида

$$\sum_{0 \leqslant i < (p-1)p^k,\; 0 \leqslant j < q-1} a_{ij} \zeta_{p^k}^i \zeta_q^j$$

с $a_{ij} \in \mathbb{Q}$ (см. [10, гл. VIII, разд. 3]). Для умножения двух таких выражений используют правила

$$\zeta_{p^k}^{(p-1)p^{k-1}} = -\sum_{i=0}^{p-2} \zeta_{p^k}^{ip^{k-1}}, \quad \zeta_q^{q-1} = -\sum_{i=0}^{q-2} \zeta_q^i.$$

Ограничивая коэффициенты a_{ij} кольцом $\mathbb{Z}$, получаем кольцо A. Элемент из K принадлежит B тогда и только тогда, когда зна-

менатели всех его коэффициентов a_{ij} есть степени q; он принадлежит главному идеалу nB в B тогда и только тогда, когда, кроме того, числители этих коэффициентов делятся на n.

Для $x \in \mathbb{Z}$, $x \not\equiv 0 \bmod p$ обозначим через σ_x автоморфизм поля K, для которого $\sigma_x(\zeta_{p^k}) = (\zeta_{p^k})^x$ и $\sigma_x(\zeta_q) = \zeta_q$ (см. [10, гл. VIII, разд. 3]). Пусть

$$G = \{\sigma_x : 1 \leqslant x \leqslant p^k, \quad x \not\equiv 0 \bmod p\}.$$

Это группа Галуа K над $\mathbb{Q}(\zeta_q)$. Она изоморфна $(\mathbb{Z}/p^k\mathbb{Z})^*$ при изоморфизме, отображающем σ_x в $(x \bmod p^k)$. Обозначим через $\mathbb{Z}[G]$ групповую алгебру G над $\mathbb{Z}$ (см. [10, гл. V, разд. 1]). Для $u \in B^*$ и $\alpha = \Sigma_{\sigma \in G} n_\sigma \sigma \in \mathbb{Z}[G]$ определим $u^\alpha \in B^*$ равенством

$$u^\alpha = \prod_{\sigma \in G} \sigma(u)^{n_\sigma}.$$

Эта операция из $\mathbb{Z}[G]$ на B удовлетворяет правилам

$$(uv)^\alpha = u^\alpha v^\alpha, \quad u^{\alpha+\beta} = u^\alpha \cdot u^\beta,$$
$$u^{\alpha\beta} = (u^\alpha)^\beta, \qquad u^1 = u$$

для u, $v \in B^*$, α, $\beta \in \mathbb{Z}[G]$, $1 = \sigma_1 \in \mathbb{Z}[G]$; поэтому она превращает B^* в модуль над $\mathbb{Z}[G]$.

Пусть χ — характер по модулю q порядка p^k. *Сумма Гаусса* $\tau(\chi)$, ассоциированная с χ, есть элемент A, определенный равенством

$$\tau(\chi) = \sum_{x=1}^{q-1} \chi(x) \zeta_q^x. \tag{7.1}$$

Мы имеем

$$\tau(\chi)\tau(\chi^{-1}) = \chi(-1)q \tag{7.2}$$

(см. [25, лемма 6.1(b)], [7, гл. 5, предложение 7]); поэтому $\tau(\chi)^{-1} = \chi(-1)\tau(\chi^{-1})/q \in B$. Отсюда следует, что $\tau(\chi) \in B^*$, поэтому выражение $\tau(\chi)^{n-\sigma_n}$ имеет смысл в следующей лемме.

(7.3) **Лемма.** *Если n простое, то*

$$\tau(\chi)^{n-\sigma_n} \equiv \chi(n)^{-n} \bmod nB.$$

Доказательство. Из (1.3) мы получаем

$$\chi(n)^n \tau(\chi)^n \equiv \sum_{x=1}^{q-1} \chi(nx)^n \zeta_q^{nx} \bmod nB \equiv$$
$$\equiv \sum_{y=1}^{q-1} \chi(y)^n \zeta_q^y \,(\text{с } y \equiv nx \bmod q) = \tau(\chi)^{\sigma_n},$$

и лемма следует из деления этого сравнения на обратимый элемент $\chi(n)^n \tau(\chi)^{\sigma_n}$. Это доказывает (7.3).

(7.4) Эта лемма приводит к тестам, которые были упомянуты в разд. 2, стадия 2. Чтобы увидеть связь с (1.2), рассмотрим случай, когда χ *квадратичный*, т. е. имеет порядок $p^k = 2$. Тогда q — нечетное простое число, χ — символ Лежандра: $\chi(x) = \left(\frac{x}{q}\right)$. Из (7.2) видим, что $\tau(\chi)^2 = a$, где $a = \left(\frac{-1}{q}\right) q$. Автоморфизм σ_n тождественный, поэтому сравнение леммы эквивалентно $a^{(n-1)/2} \equiv \left(\frac{n}{q}\right) \bmod n$. Это то же самое, что (1.2), поскольку $\left(\frac{n}{q}\right) = \left(\frac{a}{n}\right)$ в силу квадратичного закона взаимности, который фактически может быть доказан таким способом.

Вернемся к общему случаю. Мы будем выяснять, что, наоборот, может быть сказано относительно n, если известно, что сравнение в (7.3) выполнено. Для практических целей важно ввести некоторые дополнительные степени свободы, что выражено в следствии.

(7.5) **Следствие.** *Если n простое, то*

$$\tau(\chi)^{(n-\sigma_n)\beta} \equiv \chi(n)^{-n\beta} \bmod \mathfrak{n}$$

для любого $\beta \in \mathbb{Z}[G]$ и любого идеала $\mathfrak{n}$ в B, такого, что $x \in \mathfrak{n}$.

Доказательство. Возведем сравнение в (7.3) в степень β; это допустимо, поскольку $\sigma[nB] = nB$ для всех $\sigma \in G$. Далее воспользуемся тем, что $nB \subset \mathfrak{n}$. Это доказывает (7.5).

Мы будем делать следующие допущения относительно β и $\mathfrak{n}$:

(7.6) $\zeta_p^\beta \neq 1$,

(7.7) $\mathfrak{n} \cap \mathbb{Z} = n\mathbb{Z}, \quad \sigma_n(\mathfrak{n}) = \mathfrak{n}$.

Читатель может думать, что $\beta = 1$ и $\mathfrak{n} = nB$. Если $\beta = \sum_x n_x \sigma_x \in \mathbb{Z}[G]$, то (7.6) эквивалентно

$$\sum_x n_x x \not\equiv 0 \bmod p.$$

Отображение, переводящее ζ в ζ^β, есть *автоморфизм* группы U_{p^k}, если выполнено (7.6). Условие (7.7) будет исследовано в разд. 10.

(7.8) **Теорема.** *Пусть χ — характер по модулю q порядка p^k, и предположим, что*

(7.9) $\tau(\chi)^{(n-\sigma_n)\beta} \equiv \zeta \bmod \mathfrak{n}$ *при некотором $\zeta \in U_{p^k}$ некотором $\beta \in \mathbb{Z}[G]$, удовлетворяющем* (7.6), *и некотором идеале $\mathfrak{n}$ в B, удовлетворяющем* (7.7).

Допустим далее, что выполнено условие (6.4). *Тогда* χ *удовлетворяет* (6.5), *т. е.* $\chi(r)=\chi(n)^{l_p(r)}$ *для каждого делителя* r *числа* n *с* $l_p(r)$, *как в* (6.4) *и в* (6.7).

Замечание. При заданных β и $\mathfrak{n}$ сравнение (7.9) верно для по крайней мере одного $\zeta \in U_{p^k}$; это следует из (7.17).

Доказательство. По (7.6) и НОД$(n, p)=1$ мы можем записать $\zeta=\eta^{-n\beta}$ для некоторого $\eta \in U_{p^k}$. Пусть $i \in \mathbb{Z}$, $i \geqslant 0$. Возведем обе части сравнения

$$\tau(\chi)^{(n-\sigma_n)\beta} \equiv \eta^{-n\beta} \bmod \mathfrak{n} \tag{7.10}$$

в степень $\sum_{l=0}^{i-1} n^{i-1-l}\sigma_n^l$; это допустимо, поскольку $\sigma_n(\mathfrak{n})=\mathfrak{n}$. Пользуясь тем, что

$$(n-\sigma_n)\sum_{l=0}^{i-1} n^{i-1-l}\sigma_n^l = n^i-\sigma_n^i, \qquad \eta^{\sigma_n}=\eta^n,$$

и полагая $u=\tau(\chi)^\beta$, находим

$$u^{n^i-\sigma_n^i} \equiv \eta^{-in^i\beta} \bmod \mathfrak{n} \tag{7.11}$$

для каждого $i \in \mathbb{Z}$, $i \geqslant 0$. При $i=(p-1)p^k$ получаем

$$u^{n^{(p-1)p^k-1}} \equiv 1 \bmod \mathfrak{n}. \tag{7.12}$$

Пусть теперь r — *простой* делитель n. Тогда мы знаем из (7.5), что (7.10) выполнено с n, η, $\mathfrak{n}$, замененными на r, $\chi(r)$, rB, поэтому то же выполняется для (7.11). Полагая $i=p-1$, мы получаем

$$u^{r^{p-1}-\sigma_r^{p-1}} \equiv \chi(r)^{-(p-1)r^{p-1}\beta} \bmod rB. \tag{7.13}$$

Скомбинируем (7.11) и (7.13) по модулю идеала $\mathfrak{r}=rB+\mathfrak{n}$, который содержит и rB, и $\mathfrak{n}$.

Согласно (6.4), имеем $r^{p-1}=(n^{p-1})^{l_p(r)}$ для некоторого $l_p(r) \in \mathbb{Z}_p$. Выберем $m \in \mathbb{Z}$, $m \geqslant 0$, такое, что

$$m \equiv l_p(r) \bmod p^k. \tag{7.14}$$

Из

$$r^{p-1}-n^{(p-1)m}=\left((n^{p-1})^{l_p(r)-m}-1\right)n^{(p-1)m}$$

следует, что

$$v_p\left(r^{p-1}-n^{(p-1)m}\right) \geqslant v_p\left((n^{p-1})^{p^k}-1\right), \tag{7.15}$$

и, в частности, поскольку правая часть больше k,

(7.16) $\quad r^{p-1} \equiv n^{(p-1)m} \bmod p^k, \quad \sigma_r^{p-1} = \sigma_n^{(p-1)m}.$

Применим (7.11) к $i = (p-1)m$ и поделим его на (7.13); это допустимо, поскольку обе части (7.13) обратимы в B. Используя (7.16), находим тогда, что

$$u^{n^{(p-1)m} - r^{(p-1)}} \equiv (\chi(r)\eta^{-m})^{(p-1)r^{p-1}\beta} \bmod \mathfrak{r}.$$

Положим a равным наибольшему делителю числа $n^{(p-1)p^k} - 1$, который не делится на p. Если мы возведем сравнение в степень a, то по (7.15) показатель слева будет делиться на $n^{(p-1)p^k} - 1$, поэтому по (7.12) получим

$$1 \equiv (\chi(r)\eta^{-m})^{(p-1)r^{p-1}\beta a} \bmod \mathfrak{r}.$$

Предположим теперь, что справедлива следующая лемма.

(7.17) **Лемма.** *Если* $\zeta \in U_{p^k}$ *удовлетворяет сравнению* $\zeta \equiv 1 \bmod \mathfrak{r}$, *то* $\zeta = 1$.

Тогда мы находим

$$(\chi(r)\eta^{-m})^{(p-1)r^{p-1}\beta a} = 1.$$

Из $(p-1)r^{p-1}a \not\equiv 0 \bmod p$ и (7.6) следует теперь, что $\chi(r) = \eta^m$, поэтому $\chi(r) = \eta^{i_p(r)}$ согласно (7.14). Это доказано для *простых* делителей r числа n. По мультипликативности (ср. (6.7)) это выполняется для *любого* делителя r числа n. В частности, поскольку $l_p(n) = 1$, мы получаем $\chi(n) = \eta$, откуда $\chi(r) = \chi(n)^{l_p(r)}$ для всех r, делящих n. Это доказывает (7.8).

Доказательство леммы (7.17). Справедливо равенство многочленов

$$\prod_{\zeta \neq 1} (X - \zeta) = (X^{p^k} - 1)/(X - 1) = \sum_{i=0}^{p^k - 1} X^i,$$

причем произведение пробегает по всем $\zeta \in U_{p^k}$, $\zeta \neq 1$. Подставляя 1 вместо X, находим

$$\prod_{\zeta \neq 1} (1 - \zeta) = p^k.$$

Поэтому, если лемма неверна, то $p^k \in \mathfrak{r} = rB + \mathfrak{n}$, откуда $p^k = rx + y$ при некоторых $x \in B$, $y \in \mathfrak{n}$. При умножении на n/r это даст $p^k n/r \in \mathfrak{n}$, поэтому $p^k n/r \in n\mathbb{Z}$ согласно (7.7). Но r — простое число, делящее n, а p — простое число, не делящее n, значит, это невозможно. Это доказывает (7.17).

Мы сейчас разовьем несколько методов, которые могут быть использованы для доказательства того, что условие (6.4), которое встречается в (6.3) и (7.8), выполняется. Иной способ, как сделать это, можно найти в разд. 10 (см. (10.7)). В первых двух наших методах требуется, чтобы $p \geqslant 3$.

(7.18) **Предложение.** *Если $p \geqslant 3$ и $n^{p-1} \not\equiv 1 \bmod p^2$, то условие* (6.4) *выполняется.*

Доказательство. Согласно (5.1), из условия следует, что $(n^{p-1})^{\mathbb{Z}_p} = 1 + p\mathbb{Z}_p$. Поскольку $r^{p-1} \in 1 + p\mathbb{Z}_p$ для всех делителей r числа n, то (6.4) выполнено. Это доказывает (7.18).

(7.19) **Теорема.** *Пусть χ — характер по модулю q порядка p^k, и предположим, что $p \geqslant 3$. Допустим, что* (7.9) *выполнено для примитивного корня ζ степени p^k из единицы. Тогда p удовлетворяет условию* (6.4).

Доказательство. Как и в доказательстве (7.8), обозначим $\zeta = \eta^{-n\beta}$; $\eta \in U_{p^k}$. Поскольку ζ — примитивный корень степени p^k из единицы, то же верно для η. Пусть $u = \tau(\chi)^{\beta}$. Применяя (7.11) к $i = (p-1)p^{k-1}$, находим, что

$$u^{n^{(p-1)p^{k-1}}-1} \equiv \eta^{p^{k-1}\beta} \bmod \mathfrak{n}. \tag{7.20}$$

Пусть r — простое число, делящее n. Заменяя n, η, $\mathfrak{n}$ на r, $\chi(r)$, rB, как в доказательстве (7.8), мы получаем

$$u^{r^{(p-1)p^{k-1}}-1} \equiv \chi(r)^{p^{k-1}\beta} \bmod rB. \tag{7.21}$$

Комбинируем (7.20) и (7.21) по модулю $\mathfrak{r} = rB + \mathfrak{n}$. Пусть ω обозначает порядок $(u \bmod \mathfrak{r})$ в группе $(B/\mathfrak{r})^*$. Так как η — примитивный корень степени p^k из единицы, то из (7.6) и (7.17) следует, что $\eta^{p^{k-1}\beta} \not\equiv 1 \bmod \mathfrak{r}$. Поэтому из (7.20) следует, что ω не делит $n^{(p-1)p^{k-1}} - 1$, но делит $p\left(n^{(p-1)p^{k-1}} - 1\right)$. Следовательно, мы имеем

$$v_p(\omega) = 1 + v_p\left(n^{(p-1)p^{k-1}} - 1\right).$$

Из (7.21) мы видим, что ω делит $p\left(r^{(p-1)p^{k-1}} - 1\right)$, значит

$$v_p(\omega) \leqslant 1 + v_p\left(r^{(p-1)p^{k-1}} - 1\right).$$

Следовательно,

$$v_p\left(r^{(p-1)p^{k-1}} - 1\right) \geqslant v_p\left(n^{(p-1)p^{k-1}} - 1\right). \tag{7.22}$$

Заметим, что равенство имеет место тогда и только тогда, когда $\chi(r)^{p^{k-1}} \neq 1$,

Из (7.22), (5.1) и неравенства $p \geqslant 3$ получаем

$$r^{(p-1)p^{k-1}} = \left(n^{(p-1)p^{k-1}}\right)^l$$

при некотором $l \in \mathbb{Z}_p$. Поскольку, согласно (5.2), $\mathbb{Z}_p^*$ не содержит элементов порядка p, отсюда непосредственно следует, что $r^{p-1} = (n^{p-1})^l$. Это доказывает (7.19).

В оставшейся части этого раздела мы положим $p = 2$, и, следовательно, n нечетное. В этом случае важную роль играют *квадратичные* характеры. Для таких характеров удобно заменить условие (7.9), если ζ — примитивный корень второй степени из единицы (т. е. $\zeta = -1$), на условие вида $a^{(n-1)/2} \equiv -1 \bmod n$ (ср. (7.14)).

(7.23) **Лемма.** *Пусть $a \in \mathbb{Z}$, и предположим, что $a^{(n-1)/2} \equiv -1 \bmod n$. Тогда для любого делителя r числа n мы имеем $v_2(r-1) \geqslant v_2(n-1)$, и равенство справедливо тогда и только тогда, когда $\left(\frac{a}{r}\right) = -1$. В частности, $\left(\frac{a}{n}\right) = -1$.*

Доказательство. Нетрудно видеть, что достаточно рассмотреть простые делители r числа n. Поэтому пусть r — простое число, делящее n, и пусть ω — порядок $(a \bmod r)$ в группе $(\mathbb{Z}/r\mathbb{Z})^*$. Из $a^{(n-1)/2} \equiv -1 \bmod r$ следует, что $v_2(\omega) = v_2(n-1)$, и, поскольку ω делит $r-1$, отсюда вытекает, что $v_2(r-1) \geqslant v_2(n-1)$. Неравенство строгое тогда и только тогда, когда ω делит $(r-1)/2$, т. е тогда и только тогда, когда $a^{(r-1)/2} \equiv 1 \bmod r$, что эквивалентно $\left(\frac{a}{r}\right) = 1$. Это доказывает (7.23).

(7.24) **Предложение.** *Предположим, что $n \equiv 1 \bmod 4$ и что существует $a \in \mathbb{Z}$, для которого $a^{(n-1)/2} \equiv -1 \bmod n$. Тогда условие* (6.4) *выполняется для $p = 2$.*

Доказательство. Пусть $r \mid n$ — простое число. По (7.23) мы имеем $v_2(r-1) \geqslant v_2(n-1)$ и $v_2(n-1) \geqslant 2$ в силу предположения. Из (5.1) теперь следует $r \in n^{\mathbb{Z}_2}$, что и требовалось доказать. Это доказывает (7.24).

(7.25) **Предложение.** *Предположим, что $n \equiv 3 \bmod 8$ и что $2^{(n-1)/2} \equiv 1 \bmod n$.* Тогда условие (6.4) выполнено для $p = 2$.

Доказательство. Пусть $r \mid n$ — простое число. По (7.23) либо $r \equiv 1 \bmod 4$ и $\left(\frac{2}{r}\right) = 1$, либо $r \equiv 3 \bmod 4$ и $\left(\frac{2}{r}\right) = -1$. Поскольку $\left(\frac{2}{r}\right) = 1$ для $r \equiv \pm 1 \bmod 8$ и $\left(\frac{2}{r}\right) = -1$ для $r \equiv \pm 3 \bmod 8$, то либо $r \equiv 1 \bmod 8$, либо $r \equiv 3 \equiv n \bmod 8$. Поэтому одно из чисел $v_2(r-1)$ и $v_2(rn^{-1}-1)$ больше или равно 3. Но $3 = v_2(n^2-1)$, поэтому из (5.1) следует, что r или rn^{-1} принадлежит $(n^2)^{\mathbb{Z}_2}$,

Следовательно, r принадлежит $n^{2\mathbb{Z}_2} \cup n^{1+2\mathbb{Z}_2} = n^{\mathbb{Z}_2}$, что и требовалось доказать. Это доказывает (7.25).

Замечание. Если $n \equiv 3 \bmod 8$ и $2^{(n-1)/2} \not\equiv -1 \bmod n$, то n, очевидно, не простое в силу (1.2).

Случай $n \equiv 7 \bmod 8$, который не охвачен (7.24) или (7.25), наиболее удобно рассматривать с помощью предложения (10.8). В качестве альтернативы можно использовать следующую теорему, являющуюся аналогом (7.19). Мы пользуемся обозначениями, введенными в начале этого раздела.

(7.26) **Теорема.** *Пусть χ — характер по модулю q порядка p^k с $p = 2$ и $k \geqslant 2$. Предположим, что* (7.9) *выполнено для примитивного корня ζ степени 2^k из единицы, а также, что $q^{(n-1)/2} \equiv -1 \bmod n$. Тогда условие* (6.4) *выполнено для $p = 2$.*

Замечание. Допустим, что n простое и что (7.9) выполняется для примитивного корня ζ степени 2^k из единицы. Мы утверждаем, что тогда выполнено дополнительное условие $q^{(n-1)/2} \equiv -1 \bmod n$. Чтобы доказать это, заметим сначала, что $\zeta = \chi(n)^{-n\beta}$ по (7.5) и (7.17), так что $\chi(n)$ есть примитивный корень степени 2^k из единицы и $\chi(n)^{2^{k-1}} = -1$. Пусть ψ — квадратичный характер $\chi^{2^{k-1}}$. Тогда $\psi(n) = -1$ и $\psi(-1) = \chi(-1)^{2^{k-1}} = 1$, поэтому по (7.2) и (7.3) имеем $q^{(n-1)/2} = \tau(\psi)^{n-1} \equiv \psi(n) = -1 \bmod n$, что и требовалось доказать.

Следовательно, n составное, если оно не проходит дополнительный тест $q^{(n-1)/2} \equiv -1 \bmod n$.

Доказательство (7.26). В случае $n \equiv 1 \bmod 4$ теорема непосредственно следует из (7.24). Предположим поэтому, что $n \equiv 3 \bmod 4$. Как и в предыдущем замечании, положим $\psi = \chi^{2^{k-1}}$. Пусть r — простой делитель n. Рассуждая так же, как в доказательстве (7.1), находим, что

$$v_2(r^{2^{k-1}} - 1) \geqslant v_2(n^{2^{k-1}} - 1) \tag{7.27}$$

(ср. (7.22)), причем знак равенства имеет место тогда и только тогда, когда $\psi(r) = -1$. Поскольку $k \geqslant 2$, имеем $v_2(n^{2^{k-1}} - 1) \geqslant 3$; тогда, согласно (5.1), получаем $r^{2^{k-1}} = n^{2^{k-1}l}$ для некоторого $l \in \mathbb{Z}_2$. По (5.3) единственные корни из единицы в $\mathbb{Z}_2$ есть ± 1, поэтому $r = \pm n^l$. Замечание о знаке равенства в (7.27) влечет за собой, что l нечетно тогда и только тогда, когда $\psi(r) = -1$. Это также может быть сформулировано в виде $\psi(r) = (-1)^l$.

Заметим, что $\psi(r) = \left(\frac{q}{r}\right)$, применяя (7.4) с ψ, r в роли χ, n и используя то, что $\psi(-1) = 1$. Итак, из дополнительного усло-

вия $q^{(n-1)/2} \equiv -1 \bmod n$ и леммы (7.23) следует, что $v_2(r-1) \geqslant v_2(n-1)$, причем равенство выполняется тогда и только тогда, когда $\psi(r) = -1$. Поскольку $n \equiv 3 \bmod 4$, это также может быть сформулировано как $r \equiv \psi(r) \bmod 4$. Из $r \equiv \psi(r) = (-1)^l \equiv n^l \bmod 4$ следует теперь, что в равенстве $r = \pm n^l$ должен быть знак плюс. Это доказывает (7.26).

(7.28) *Замечание.* Усложнения, которые возникают в случае $p = 2$, исчезают, если для $p = 2$ мы ограничиваемся равенством $k = 1$, т. е. *квадратичными* характерами. В этом случае (6.4) можно заменить более простым условием $v_2(r-1) \geqslant v_2(n-1)$ для всех $r|n$ (ср. [16, разд. 2]). Из рассмотрения только квадратичных характеров вытекает, что вспомогательное число t, выбранное на стадии 1 алгоритма (см. разд. 2 и 4), должно удовлетворять дополнительному условию $t \not\equiv 0 \bmod 4$.

8. СУММЫ ЯКОБИ ДЛЯ НЕЧЕТНЫХ p

Пусть q, p, k, n, χ, B, G, $\tau(\chi)$ такие же, как в предыдущем разделе; мы сохраняем обозначения ζ_m, U_m, σ_x. Наша цель состоит в переформулировке условия (7.9) таким образом, чтобы оно относилось только к элементам подкольца $\mathbb{Z}[\zeta_{p^k}]$ в B.

Пусть a и b — два целых числа. *Сумма Якоби* $J(\chi^a, \chi^b)$, ассоциированная с характерами χ^a и χ^b, есть элемент $\mathbb{Z}(\zeta_{p^k}]$, определенный по формуле

$$(8.1) \qquad J(\chi^a, \chi^b) = \sum_{x=0}^{q-1} \chi^a(x)\chi^b(1-x).$$

В B мы имеем

$$(8.2) \qquad J(\chi^a, \chi^b) = \tau(\chi^a)\tau(\chi^b)/\tau(\chi^{a+b}),$$

если $a + b \not\equiv 0 \bmod p^k$, где сумма Гаусса определена в (7.1). Доказательство (8.2) см. в [25, лемма 6.2(d)] или в [7, гл. 5, предложение 9]. Если $ab(a+b) \not\equiv 0 \bmod p$, то (8.2) можно записать в виде

$$(8.3) \qquad J(\chi^a, \chi^b) = \tau(\chi)^{\sigma_a + \sigma_b - \sigma_{a+b}}.$$

Заметим, что из условия $ab(a+b) \not\equiv 0 \bmod p$ вытекает нечетность p.

В дальнейшем мы обозначаем через $[y]$ наибольшее целое число, не превосходящее y, если y — вещественное число. При $p \geqslant 3$ полагаем

$$(8.4) \qquad M = \{x \in \mathbb{Z}: 1 \leqslant x \leqslant p^k,\ x \not\equiv 0 \bmod p\}.$$

(8.5) **Теорема.** *Предположим, что* $p \geqslant 3$. *Пусть* a, b — *целые числа, удовлетворяющие соотношениям*

(8.6) $$(a+b)^p \not\equiv a^p + b^p \bmod p^2, \quad ab(a+b) \not\equiv 0 \bmod p,$$

и пусть $\mathfrak{m}$ — *идеал в* $\mathbb{Z}[\zeta_{p^k}]$, *для которого*

(8.7) $$\mathfrak{m} \cap \mathbb{Z} = n\mathbb{Z}, \quad \sigma_n(\mathfrak{m}) = \mathfrak{m}.$$

Определим $\alpha \in \mathbb{Z}[G]$ *выражением*

$$\alpha = \sum_{x \in M} \left[\frac{nx}{p^k}\right] \sigma_x^{-1}.$$

Если при этих обозначениях

(8.8) $$J(\chi^a, \chi^b)^\alpha \equiv \zeta \bmod \mathfrak{m} \text{ при некотором } \zeta \in U_{p^k},$$

то (7.9) *выполняется. Если* (8.8) *не выполняется, то* n *составное.*

(8.9) *Замечания.* (a) Заметим, что $J(\chi^a, \chi^b)^\alpha$ принадлежит $\mathbb{Z}[\zeta_{p^k}]$, поскольку коэффициенты α неотрицательны.

(b) В доказательстве мы увидим, что если (8.8) выполняется, то (7.9) верно с тем же ζ. Это важно для (7.19).

(c) Если $3 \leqslant p < 6 \cdot 10^9$, $p \notin \{1093, 3511\}$, то условие (8.6) выполнено для $a = b = 1$ по [13]. Из $(p-1)^p \not\equiv p - 1 \bmod p^2$ следует, что в любом случае (8.6) имеет место при некотором $a \leqslant p - 2$ с $b = 1$.

(d) Примером идеала $\mathfrak{m}$ в $\mathbb{Z}[\zeta_{p^k}]$, удовлетворяющего (8.7), служит $\mathfrak{m} = n\mathbb{Z}[\zeta_{p^k}]$. В разд. 10 мы обсудим различные способы выбора $\mathfrak{m}$.

Доказательство (8.5). Пусть $\mathfrak{n}$ — идеал в B, порожденный $\mathfrak{m}$. Из

$$\mathfrak{n} = \left\{ \left(\sum_{j=0}^{q-2} a_j \zeta_q^j \right) \cdot q^d : \ a_j \in \mathfrak{m} \ (0 \leqslant j \leqslant q-2), \ d \in \mathbb{Z} \right\}$$

и НОД$(q, n) = 1$ нетрудно получить, что

(8.10) $$\mathfrak{n} \cap \mathbb{Z}[\zeta_{p^k}] = \mathfrak{m}.$$

Из (8.7) следует теперь, что $\mathfrak{n}$ удовлетворяет (7.7).

Определим $\beta \in \mathbb{Z}[G]$ выражением

(8.11) $$\beta = \sum_{x \in M} \left(\left[\frac{(a+b)x}{p^k}\right] - \left[\frac{ax}{p^k}\right] - \left[\frac{bx}{p^k}\right] \right) \sigma_x^{-1}$$

с. 4 из (8.4). Ниже будет доказана следующая лемма.

(8.12) **Лемма.** *Пусть* a, $b \in \mathbb{Z}$ *удовлетворяют* (8.6), *и пусть* α, $\beta \in \mathbb{Z}[G]$ *определены в* (8.5) *и* (8.11). *Тогда мы имеем*

$$(n - \sigma_n)\beta = (\sigma_a + \sigma_b - \sigma_{a+b})\alpha$$

в $\mathbb{Z}[G]$, *и* β *удовлетворяет условию* (7.6): $\zeta_p^\beta \neq 1$.

Пользуясь этой леммой, мы видим из (8.3), что

$$J(\chi^a, \chi^b)^\alpha = \tau(\chi)^{(\sigma_a+\sigma_b-\sigma_{a+b})\alpha} = \tau(\chi)^{(n-\sigma_n)\beta},$$

поэтому по (8.10) сравнение (8.8) эквивалентно

$$\tau(\chi)^{(n-\sigma_n)\beta} \equiv \zeta \bmod \mathfrak{n} \text{ при некотором } \zeta \in U_{p^k}.$$

Поскольку β и $\mathfrak{n}$ удовлетворяют (7.6) и (7.7), теперь непосредственно видно, что (8.8) влечет за собой (7.9). Второе утверждение теоремы очевидно из (7.5). Это доказывает (8.5).

Доказательство (8.12). Определим $\theta \in \mathbb{Z}[G]$:

$$\theta = \sum_{x \in M} x\sigma_x^{-1},$$

причем M из (8.4). Пусть $m \in \mathbb{Z}$, $m \not\equiv 0 \bmod p$. Полагая $x \equiv my \bmod p^k$, мы видим, что

$$\sigma_m\theta = \sum_{y \in M} r(my)\sigma_y^{-1},$$

где $r(my)$ — элемент M, сравнимый с my по модулю p^k. Из $r(my) = my - [my/p^k]p^k$ следует теперь, что

$$(8.13) \qquad (m - \sigma_m)\theta = p^k \sum_{y \in M} \left[\frac{my}{p^k}\right]\sigma_y^{-1}.$$

Применяя это к $m = n$, a, b, $a + b$, мы находим, что $(n - \sigma_n)\theta = p^k\alpha$,

$$(8.14) \qquad (\sigma_a + \sigma_b - \sigma_{a+b})\theta = ((a + b - \sigma_{a+b}) - (a - \sigma_a) - \\ - (b - \sigma_b))\theta = p^k\beta,$$

и поэтому

$$p^k(n - \sigma_n)\beta = (\sigma_a + \sigma_b - \sigma_{a+b})(n - \sigma_n)\theta = \\ = p^k(\sigma_a + \sigma_b - \sigma_{a+b})\alpha.$$

Поделив на p^k, мы получаем первое утверждение (8.12).

Второе утверждение эквивалентно

$$(8.15) \qquad \sum_{x \in M}\left(\left[\frac{(a+b)x}{p^k}\right] - \left[\frac{ax}{p^k}\right] - \left[\frac{bx}{p^k}\right]\right)x^{-1} \not\equiv 0 \bmod p.$$

Здесь мы рассматриваем выражение слева как элемент $\mathbb{Z}_p$, чтобы придать x^{-1} смысл; то же относится к подобным выраже-

ниям ниже. Чтобы доказать (8.15), покажем сначала, что

$$(8.16)\qquad v_p\Big(\sum_{x\in M} x^{1-p}\Big) = k-1.$$

Значения, принимаемые выражением $(x^{1-p} \bmod p^k)$ при $x \in M$, есть в точности элементы $H = \{y \in (\mathbb{Z}/p^k\mathbb{Z})^*: y \equiv 1 \bmod p\}$, каждое берется $p-1$ раз. Это верно, поскольку H есть подгруппа индекса $p-1$ в циклической группе $(\mathbb{Z}/p^k\mathbb{Z})^*$. Поэтому имеем

$$\sum_{x\in M} x^{1-p} \equiv (p-1)\sum_{y\in H} y \bmod p^k \equiv$$
$$\equiv (p-1)\Big(p^{k-1} + \tfrac{1}{2}p^k(p^{k-1}-1)\Big) \bmod p^k,$$

откуда следует (8.16).

Если $x, y \in \mathbb{Z}$ сравнимы по модулю p^k, то $x^p \equiv y^p \bmod p^{k+1}$ по биномиальной теореме. Отсюда следует, что существует кольцевой гомоморфизм $\mathbb{Z}[G] \to \mathbb{Z}/p^{k+1}\mathbb{Z}$, отображающий σ_x в $(x^p \bmod p^{k+1})$ при $x \in M$. Применяя этот кольцевой гомоморфизм к (8.14), получаем сравнение

$$(a^p + b^p - (a+b)^p)\sum_{x\in M} x^{1-p} \equiv$$
$$\equiv p^k \sum_{x\in M}\left(\left[\frac{(a+b)x}{p^k}\right] - \left[\frac{ax}{p^k}\right] - \left[\frac{bx}{p^k}\right]\right)x^{-p} \bmod p^{k+1}.$$

По (8.6) и (8.16) показатель p в выражении слева в точности равен k. Следовательно, это также верно для выражения справа, поэтому

$$\sum_{x\in M}\left(\left[\frac{(a+b)x}{p^k}\right] - \left[\frac{ax}{p^k}\right] - \left[\frac{bx}{p^k}\right]\right)x^{-p} \not\equiv 0 \bmod p.$$

Поскольку $x^{-p} \equiv x^{-1} \bmod p$, это то же самое, что (8.15). Это завершает доказательство (8.12).

Альтернативное доказательство (8.15) исходит из сравнения

$$\sum_{x\in M}\left[\frac{mx}{p^k}\right]x^{-1} \equiv m\left(m^{(p-1)p^{k-1}} - 1\right)/p^k \bmod p^k,$$

которое справедливо для любого $m \in \mathbb{Z}$, $m \not\equiv 0 \bmod p$. Это сравнение доказывают, вычисляя $\prod_{x\in M} mx$ двумя различными способами.

Замечание. Элементы θ, $\beta \in \mathbb{Z}[G]$, которые мы использовали в этом разделе, есть известные операторы из теории круговых полей. См., например, [11, гл. IV, разд. 4], [25, разд. 6.2], где они встречаются в связи с теоремой Стикельбергера о разложении на множители сумм Гаусса и Якоби.

9. СУММЫ ЯКОБИ ДЛЯ $p = 2$

В этом разделе мы проделаем для $p = 2$ то, что сделали в предыдущем разделе для $p \geqslant 3$. Обозначения не меняются; в частности, наше предположение НОД$(n, pq) = 1$ влечет за собой, что n нечетно при $p = 2$. Мы различаем случаи $k = 1$, $k = 2$, $k \geqslant 3$.

(9.1) **Теорема.** *Пусть $p = 2$ и $k = 1$. Если в этом случае мы имеем*

(9.2) $q^{(n-1)/2} \not\equiv \zeta \bmod n$ *при некотором* $\zeta \in \{1, -1\}$, *тогда* (7.9) *выполняется. Если* (9.2) *не выполнено, то n составное.*

Доказательство. Первое утверждение следует из $\tau(\chi)^2 = \chi(-1)q$ (см. (7.2)) при $\beta = 1$ и $\mathfrak{n} = nB$ в (7.9). Второе утверждение следует из (7.5). Это доказывает (9.1).

(9.3) **Теорема.** *Пусть $p = 2$, $k = 2$ и $n \equiv 1 \bmod 4$. Пусть $\mathfrak{m}$ — идеал в $\mathbb{Z}[\zeta_4]$, для которого $\mathfrak{m} \cap \mathbb{Z} = n\mathbb{Z}$. Если в этом случае мы имеем*

(9.4) $J(\chi, \chi)^{(n-1)/2} q^{(n-1)/4} \equiv \zeta \bmod \mathfrak{m}$ *при некотором* $\zeta \in U_4$,

то (7.9) *выполняется. Если* (9.4) *не выполнено, то n составное.*

Доказательство. Пусть $\mathfrak{n}$ — идеал в B, порожденный $\mathfrak{m}$. Как и в доказательстве теоремы (8.5), мы имеем $\mathfrak{n} \cap \mathbb{Z}[\zeta_4] = \mathfrak{m}$. Из $n \equiv 1 \bmod 4$ следует, что σ_n — тождественный автоморфизм, поэтому $\mathfrak{n}$ удовлетворяет (7.7).

По (8.2) и (7.2) мы имеем

$$J(\chi, \chi) = \tau(\chi)^2/\tau(\chi^2), \quad \tau(\chi^2)^2 = \chi^2(-1)q = q,$$

и поэтому

$$\tau(\chi)^{n-\sigma_n} = \tau(\chi)^{n-1} = J(\chi, \chi)^{(n-1)/2} q^{(n-1)/4}.$$

Следовательно, (9.4) есть то же самое, что (7.9) с $\beta = 1$ и $\mathfrak{n}$ таким, как выше. Второе утверждение теоремы снова следует из (7.5). Это доказывает (9.3).

(9.5) **Теорема.** *Пусть $p = 2$, $k = 2$ и $n \equiv 3 \bmod 4$. Если в этом случае мы имеем*

(9.6) $J(\chi, \chi)^{(n+1)/2} q^{(n-3)/4} \equiv \zeta \bmod n\mathbb{Z}[\zeta_4]$ *для некоторого* $\zeta \in U_4$,

то (7.9) *выполняется. Если* (9.6) *не выполнено, то n составное.*

Замечание. Нет необходимости рассматривать произвольные идеалы $\mathfrak{m}$ в $\mathbb{Z}[\zeta_4]$, удовлетворяющие (8.7) в этой теореме, поскольку из (10.5) следует, что единственный такой $\mathfrak{m}$ есть $n\mathbb{Z}[\zeta_4]$.

Доказательство (9.5). По (7.2) имеем

$$\tau(\chi)\tau(\chi^{-1}) = \chi(-1)q, \quad \tau(\chi^2)^2 = q,$$

и поэтому в силу (8.2)

$$\begin{aligned}\tau(\chi)^{n-\sigma_n} &= \tau(\chi)^{n+1}/(\tau(\chi)\tau(\chi^{-1})) = \\ &= J(\chi, \chi)^{(n+1)/2} q^{(n+1)/4}/(\chi(-1)q) = \\ &= \chi(-1) J(\chi, \chi)^{(n+1)/2} q^{(n-3)/4}.\end{aligned}$$

Следовательно, (9.6) есть то же самое, что (7.9) с $\beta = 1$, $\mathfrak{n} = nB$ и с ζ, замененным на $\chi(-1)\zeta$. Это влечет за собой (9.5).

В оставшейся части этого раздела мы предполагаем, что $p = 2$ и $k \geqslant 3$. *Тройная сумма Якоби* $J(\chi, \chi, \chi)$ есть элемент $\mathbb{Z}[\zeta_{2^k}]$, определенный по формуле

(9.7) $$J(\chi, \chi, \chi) = J(\chi, \chi) J(\chi, \chi^2).$$

Чтобы пояснить обозначение, отметим, что

$$J(\chi, \chi, \chi) = \sum_{x, y, z \in \mathbb{Z}/q\mathbb{Z},\ x+y+z=1} \chi(x)\chi(y)\chi(z)$$

(см. [7, гл. 5, разд. 4]), но это не будет нужно в дальнейшем. Из (9.7) и (8.2) мы видим, что

(9.8) $$J(\chi, \chi, \chi) = \tau(\chi)^3/\tau(\chi^3) = \tau(\chi)^{3-\sigma_3}.$$

Пусть

(9.9) $$M = \{x \in \mathbb{Z}: 1 \leqslant x \leqslant 2^k, \quad x \equiv 1 \text{ или } 3 \bmod 8\}.$$

Заметим, что M, взятое по модулю 2^k, есть подгруппа в $(\mathbb{Z}/2^k\mathbb{Z})^*$. Квадратные скобки [ ] такие же, как в разд. 8.

(9.10) **Теорема.** *Пусть $p = 2$, $k \geqslant 3$ и $n \equiv 1$ или $3 \bmod 8$. Пусть $\mathfrak{m}$ — идеал в $\mathbb{Z}[\zeta_{2^k}]$, для которого*

$$\mathfrak{m} \cap \mathbb{Z} = n\mathbb{Z}, \quad \sigma_n(\mathfrak{m}) = \mathfrak{m}.$$

Определим $\alpha \in \mathbb{Z}[G]$:

$$\alpha = \sum_{x \in M} \left[\frac{nx}{2^k}\right] \sigma_x^{-1}.$$

Если при этих обозначениях мы имеем

(9.11) $J(\chi, \chi, \chi)^{\alpha} \equiv \zeta \bmod \mathfrak{m}$ *при некотором* $\zeta \in U_{2^k}$,

то (7.9) *выполняется Если* (9.11) *не выполнено, то* $\mathfrak{n}$ *составное*

Доказательство. Определим $\beta \in \mathbb{Z}[G]$:

(9.12) $$\beta = \sum_{x \in M} \left[\frac{3x}{2^k}\right] \sigma_x^{-1}$$

с M из (9.9). Ниже мы докажем, что

(9.13) $\quad (n-\sigma_n)\beta=(3-\sigma_3)\alpha$

для $n\equiv 1$ или $3 \bmod 8$ и что β удовлетворяет условию (7.6):

(9.14) $\quad (-1)^\beta\neq 1.$

Допуская это, мы доказываем теорему точно так же, как доказали теорему (8.5) из (8.12). Единственное отличие состоит в том, что (8.3) заменено на (9.8).

Чтобы доказать (9.13), мы определим $\theta\in\mathbb{Z}[G]$:

$$\theta=\sum_{x\in M} x\sigma_x^{-1}.$$

Имеем

(9.15) $$(m-\sigma_m)\theta=2^k\sum_{x\in M}\left[\frac{mx}{2^k}\right]\sigma_x^{-1}$$

для $m\in\mathbb{Z}$, $m\equiv 1$ или $3 \bmod 8$

по тем же соображениям, которые использовались для доказательства (8.13). Применяя это к $m=n$ и $m=3$, находим, что

(9.16) $\quad (n-\sigma_n)\theta=2^k\alpha, \quad (3-\sigma_3)\theta=2^k\beta;$

это влечет за собой (9.13). Чтобы доказать (9.14), применим к (9.16) кольцевой гомоморфизм $\mathbb{Z}[G]\to\mathbb{Z}$, который отображает каждое $\sigma_x\in G$ в 1. Это ведет к

(9.17) $$2\sum_{x\in M}x=2^k\sum_{x\in M}\left[\frac{3x}{2^k}\right],$$

поэтому

(9.18) $$\sum_{x\in M}\left[\frac{3x}{2^k}\right]=2^{k-2}-1.$$

Это — нечетное число, и, следовательно $(-1)^\beta=-1$, что и требовалось доказать. Это завершает доказательство (9.10).

(9.19) **Теорема.** *Пусть* $p=2$, $k\geqslant 3$ *и* $n\equiv 5$ *или* $7 \bmod 8$. *Пусть* $\mathfrak{m}$ — *идеал в* $\mathbb{Z}[\zeta_{2^k}]$, *для которого*

$$\mathfrak{m}\cap\mathbb{Z}=n\mathbb{Z},\quad \sigma_n[\mathfrak{m}]=\mathfrak{m}.$$

Определим $\alpha\in\mathbb{Z}[G]$:

$$\alpha=\sum_{x\in M}\left[\frac{nx}{2^k}\right]\sigma_x^{-1}$$

и положим $\varphi=\chi^{2^{k-3}}$. *Если при этих обозначениях мы имеем*

(9.20) $\quad J(\chi,\chi,\chi)^\alpha J(\varphi,\varphi^3)^2\equiv\zeta \bmod \mathfrak{m}$ *при некотором* $\zeta\in U_{2^k}$,

то (7.9) *выполняется. Если* (9.20) *не выполнено, то* n *составное.*

Доказательство. Пусть β определено по формуле (9.12). Ниже мы докажем, что

$$\tau(\chi)^{(n-\sigma_n)\beta} = \chi(-1) J(\chi, \chi, \chi)^{\alpha} J(\varphi, \varphi^3)^2. \tag{9.21}$$

Из этого равенства теорема (9.19) вытекает по тем же соображениям, которые были использованы в доказательстве теоремы (8.5). Заметим, что по (9.14) β удовлетворяет условию (7.6).

Чтобы доказать (9.21), применим (9.15) к $m = -n$; это допустимо, поскольку $-n \equiv 1$ или $3 \bmod 8$. Мы находим, что

$$(-n - \sigma_{-n})\theta = 2^k \sum_{x \in M} \left[\frac{-nx}{2^k}\right] \sigma_x^{-1} =$$
$$= -2^k \left(\alpha + \sum_{x \in M} \sigma_x\right).$$

Комбинирование с (9.16) приводит к

$$(n + \sigma_{-n})\beta = (3 - \sigma_3)\left(\alpha + \sum_{x \in M} \sigma_x\right) =$$
$$= (3 - \sigma_x)\alpha + 2 \sum_{x \in M} \sigma_x,$$

поэтому

$$\tau(\chi)^{(n+\sigma_{-n})\beta} = J(\chi, \chi, \chi)^{\alpha} \tau(\chi)^{2 \sum_{x \in M} \sigma_x}.$$

По (7.2) и (9.18) имеем

$$\tau(\chi)^{(\sigma_n + \sigma_{-n})\beta} = (\chi(-1) q)^{\beta} = \chi(-1) q^{2^{k-2}-1}.$$

Поделив, получаем

$$\tau(\chi)^{(n-\sigma_n)\beta} = \chi(-1) J(\chi, \chi, \chi)^{\alpha} \tau(\chi)^{2\Sigma_{x \in M}\sigma_x} / q^{2^{k-2}-1}.$$

Чтобы доказать (9.21), достаточно показать, что

$$\tau(\chi)^{2\Sigma_{x \in M}\sigma_x} = q^{2^{k-2}-1} J(\varphi, \varphi^3)^2. \tag{9.22}$$

Это, как легко видеть, является следствием соотношений Хассе — Давенпорта (см. [12, гл. 2, теорема 10.1]). Мы даем прямое доказательство, применяя индукцию по k. При $k = 3$ имеем $\chi = \varphi$, поэтому по (8.2), (7.2) и $\varphi^4(-1) = 1$ находим, что

$$qJ(\varphi, \varphi^3)^2 = q(\tau(\varphi)\tau(\varphi^3))^2 / \tau(\varphi^4)^2 = (\tau(\varphi)\tau(\varphi^3))^2,$$

и это же самое, что (9.22). Пусть теперь $k > 3$. Положим $\psi = \varphi^4 = \chi^{2^{k-1}}$; это квадратичный характер по модулю q. Из $8 \mid 2^{k-1}$

следует, что $\chi\psi = \chi^y$ для некоторого $y \in M$. Поэтому имеем

$$\tau(\chi)^{2\Sigma_{x\in M}\sigma_x} = (\tau(\chi)\tau(\chi, \psi))^{\Sigma_{x\in M}\sigma_x}.$$

Допустим на время, что

$$\tau(\chi)\tau(\chi\psi) = \chi(4)^{-1}\tau(\psi)\tau(\chi^2). \tag{9.23}$$

Применяя $\sum_{x\in M}\sigma_x$ и используя то, что $\psi = \psi^x$ для $x \in M$, находим

$$\tau(\chi)^{2\Sigma_{x\in M}\sigma_x} = \chi(2)^{-2\Sigma_{x\in M}x}\tau(\psi)^{2^{k-2}}\tau(\chi^2)^{\Sigma_{x\in M}\sigma_x}.$$

Согласно (9.17), первый множитель в правой части равен 1. Поскольку ψ квадратичный и $\psi(-1) = 1$, мы видим из (7.2), что второй множитель равен $q^{2^{k-3}}$. Третий множитель может быть записан как $\tau(\chi^2)^{2\Sigma_{x\in M'}\sigma_x}$, где

$$M' = \{x\colon\ 1 \leqslant x \leqslant 2^{k-1},\ x \equiv 1 \text{ или } 3 \bmod 8\},$$

и по индуктивному предположению это равно $q^{2^{k-3}-1}J(\varphi, \varphi^3)^2$, что завершает шаг индукции.

Тождество в (9.23) есть частный случай соотношений Хассе — Давенпорта; оно может быть непосредственно доказано следующим образом [5, разд. 20.4]. Имеем

$$J(\chi, \chi) = \sum_{x=0}^{q-1}\chi(x)\chi(1-x) =$$

$$= \sum_{x=0}^{q-1}\chi(x^2 - x) = \sum_{y\in\mathbb{Z}/q\mathbb{Z}}\chi(y)m(y),$$

где $m(y)$ — количество элементов $x \in \mathbb{Z}/q\mathbb{Z}$, для которых $y = x - x^2$; это 0, 1 или 2 в соответствии с тем, что дискриминант $1 - 4y$ полинома $X^2 - X + y$ не есть квадрат, есть 0 или ненулевой квадрат в $\mathbb{Z}/q\mathbb{Z}$, поэтому во всех случаях $m(y) = 1 + ((1-4y)/q) = 1 + \psi(1-4y)$. Следовательно,

$$J(\chi, \chi) = \sum_{y\in\mathbb{Z}/q\mathbb{Z}}\chi(y)(1 + \psi(1-4y)) =$$

$$= \sum_{y\in\mathbb{Z}/q\mathbb{Z}}\chi(y) + \sum_{z\in\mathbb{Z}/q\mathbb{Z}}\chi(z/4)\psi(1-z) =$$

$$= 0 + \chi(4)^{-1}\sum_{z\in\mathbb{Z}/q\mathbb{Z}}\chi(z)\psi(1-z) = \chi(4)^{-1}J(\chi, \psi).$$

По (8.2) это то же самое, что

$$\tau(\chi)^2/\tau(\chi^2) = \chi(4)^{-1}\tau(\chi)\tau(\psi)/\tau(\chi\psi),$$

и отсюда вытекает (9.23). Это завершает доказательство (9.19).

(9.24) *Замечания.* (a) Из доказательства теорем в этом разделе мы видим, что если (9.2), (9.4), (9.6), (9.11) или (9.20) выполнено для некоторого $\zeta \in U_{2^k}$, то (7.9) верно с ζ, замененным на $\pm\zeta$. Заметим, что для $k \geqslant 2$ корень степени 2^k из единицы $\pm\zeta$ примитивен тогда и только тогда, когда ζ примитивен. Это важно для (7.26).

(b) Число $\chi(-1) \in \{1, -1\}$, появляющееся во многих формулах этого раздела, равно -1 тогда и только тогда, когда $k = v_2(q-1)$, что часто имеет место в приложениях.

10. ВЫБОР ИДЕАЛА

В этом разделе p обозначает простое число, k — положительное целое число, ζ_{p^k} — примитивный корень степени p^k из единицы в $\mathbb{C}$ и n — целое число, $n > 1$, $n \not\equiv 0 \bmod p$. Через f мы обозначаем порядок элемента $(n \bmod p^k)$ в группе $(\mathbb{Z}/p^k\mathbb{Z})^*$ и полагаем σ_n равным автоморфизму кольца $\mathbb{Z}[\zeta_{p^k}]$, для которого $\sigma_n(\zeta_{p^k}) = \zeta_{p^k}^n$.

В разд. 11 мы увидим, что в нашем алгоритме простоты мы должны проверить (8.8), (9.2), (9.4), (9.6), (9.11) и (9.20) для нескольких выборов p, k, q. Каждый раз это требует вычисления по модулю некоторого идеала $\mathfrak{m}$ в $\mathbb{Z}[\zeta_{p^k}]$, удовлетворяющего соотношениям

(10.1) $\quad \mathfrak{m} \cap \mathbb{Z} = n\mathbb{Z}, \quad \sigma_n[\mathfrak{m}] = \mathfrak{m}.$

Это вычисление легче проделать, если кольцо $\mathbb{Z}[\zeta_{p^k}]/\mathfrak{m}$ меньше, значит, если $\mathfrak{m}$ больше. В этом разделе мы увидим, как выбрать $\mathfrak{m}$ настолько большим, насколько возможно. Методы, которые мы опишем, обычно успешны, если n просто, даже если мы еще не имеем *доказательства* того, что n простое. Однако если n составное, то эти методы вряд ли работают. Поэтому целесообразно использовать их, если только n, вероятно, простое, в том смысле, что оно прошло несколько тестов типа (1.2).

(10.2) Первый метод взят из [1, разд. 4, A.5]. Применяем алгоритм Берлекэмпа [8, разд. 4.6.2] для нахождения многочлена $h \in \mathbb{Z}[T]$ степени f со старшим коэффициентом 1, такого, что $(h \bmod n)$ делит $\sum_{i=0}^{p-1} T^{ip^{k-1}}$ в $(\mathbb{Z}/n\mathbb{Z})[T]$. Если n простое, то такой многочлен h существует и $(h \bmod n)$ неприводим (ср. [25, гл. 2]). Теперь мы полагаем $\mathfrak{m}$ равным идеалу в $\mathbb{Z}[\zeta_{p^k}]$, порожденному n и $h(\zeta_{p^k})$. Тогда $\mathbb{Z}[\zeta_{p^k}]/\mathfrak{m}$ может быть отождествлено с множеством всех выражений:

$$\sum_{i=0}^{f-1} a_i \zeta^i, \quad a_i \in \mathbb{Z}/n\mathbb{Z} \quad (0 \leqslant i < f).$$

где $\bar{\zeta}=(\zeta_{p^k} \bmod \mathfrak{m})$ есть нуль многочлена $(h \bmod n)$. Это кольцо имеет n^f элементов, и, если n простое, оно является полем F_{h^f}. Имеем $\mathfrak{m} \cap \mathbb{Z}=n\mathbb{Z}$, поскольку это ядро естественного отображения $\mathbb{Z} \to \mathbb{Z}[\zeta_{p^k}]/\mathfrak{m}$. Можно показать, что условие $\sigma_n[\mathfrak{m}]=\mathfrak{m}$ должно выполняться автоматически, если h получено с помощью алгоритма Берлекэмпа; однако это в любом случае можно легко определить проверкой, является ли $\bar{\zeta}^n$ нулем $(h \bmod n)$. Отметим, что если n простое, то условие $\sigma_n[\mathfrak{m}]=\mathfrak{m}$ выполнено для всех идеалов $\mathfrak{m}$ в $\mathbb{Z}[\zeta_{p^k}]$, содержащих n. Чтобы увидеть это, используем (1.3) для того, чтобы показать, что $\sigma_n(\alpha) \equiv \alpha^n \bmod \mathfrak{m}$ для всех $\alpha \in \mathbb{Z}[\zeta_{p^k}]$; тогда $\sigma_n[\mathfrak{m}] \subset \mathfrak{m}$, и равенство справедливо, поскольку σ_n имеет конечный порядок.

Если $f=(p-1)p^{k-1}$, то описанный выше метод приводит к $\mathfrak{m}=n\mathbb{Z}[\zeta_{p^k}]$, и из (10.5) следует, что это на самом деле единственный идеал в $\mathbb{Z}[\zeta_{p^k}]$, удовлетворяющий (10.1). Методы, описанные в этом разделе, полезны поэтому только при $f<(p-1)p^{k-1}$. Это случается, например, если $p=2$ и $k \geqslant 3$, поскольку в этом случае $(\mathbb{Z}/p^k\mathbb{Z})^*$ не циклична.

Если $f<(p-1)p^{k-1}$, то коэффициенты h обычно довольно велики. Это превращает на практике деление на h в сложную операцию, и то же самое справедливо поэтому для умножения в кольце $\mathbb{Z}[\zeta_{p^k}]/\mathfrak{m}$, по крайней мере для $f \not\equiv 1$. Второй способ построения $\mathfrak{m}$ не имеет этого недостатка. Он заключается в следующем.

(10.3) Сначала строят кольцо F с n^f элементами, которое содержит $\mathbb{Z}/n\mathbb{Z}$ в качестве подкольца, причем F — поле, если n простое. Например, можно взять

$$F=(\mathbb{Z}/n\mathbb{Z})[T]/g \cdot (\mathbb{Z}/n\mathbb{Z})[T],$$

где g — многочлен степени f в $(\mathbb{Z}/n\mathbb{Z})[T]$ со старшим коэффициентом 1, который неприводим, если n простое; последнее свойство может быть проверено с помощью теста неприводимости, описанного в [8, упр. 4.6.2.16]. Обозначая через ξ образ T в F, имеем

$$F=\left\{\sum_{i=0}^{f-1} a_i\xi^i\colon\ a_i \in \mathbb{Z}/n\mathbb{Z}\,(0 \leqslant i < f)\right\}$$

с $g(\xi)=0$. Чтобы облегчить умножение в F, следует выбрать g таким, чтобы его коэффициенты были «невелики», и это обычно может быть сделано на практике.

Важно, что F конструируется так, что мы можем распознавать, принадлежит ли данный элемент F группе обратимых элементов F^*. В приведенном примере мы можем сделать это

путем вычисления НОД с g в $(\mathbb{Z}/n\mathbb{Z})[T]$ при помощи алгоритма Евклида; это может не получиться лишь в том случае, если на некоторой стадии найдется нетривиальный общий делитель числа n и некоторого старшего коэффициента; в этом случае n разлагается на множители [1, разд. 5].

После того как F получено, конструируют кольцевой гомоморфизм ρ: $F \to F$, такой, что если n простое, то $\rho(\alpha) = \alpha^n$ для всех $\alpha \in F$. Для F, описанного выше, это делают, проверяя, что $g(\xi^n) = 0$, и полагая

$$\rho\left(\sum_{i=0}^{f-1} a_i \xi^i\right) = \sum_{i=0}^{f-1} a_i \xi^{in};$$

если $g(\xi^n) \neq 0$, то n составное.

Далее выбирают элемент $\beta \in F$, $\beta \neq 0$, такой, что $\beta^{(n^f-1)/p} \neq 1$. Нахождение такого элемента не должно быть трудным делом, поскольку если n простое, то случайное $\beta \in F - \{0\}$ обладает этим свойством с вероятностью $(p-1)/p$.

Если n простое, то

$$\beta^{n^f-1} = 1, \quad \beta^{(n^f-1)/p} - 1 \in F^*, \quad \rho(\beta) = \beta^n. \tag{10.4}$$

Теперь проверяют, что β в самом деле обладает этими свойствами, и вычисляют $\bar{\zeta} = \beta^{(n^f-1)/p^k}$. Тогда $\bar{\zeta}$ является нулем многочлена

$$\sum_{i=0}^{p-1} X^{ip^{k-1}} = \left(X^{p^k} - 1\right)/\left(X^{p^{k-1}} - 1\right),$$

поэтому мы можем определить кольцевой гомоморфизм λ: $\mathbb{Z}[\zeta_{p^k}] \to F$, полагая $\lambda(\zeta_{p^k}) = \bar{\zeta}$. Имеем $\rho(\bar{\zeta}) = \bar{\zeta}^n$, и поэтому $\lambda \circ \sigma_n = \rho \circ \lambda$.

Наконец, мы полагаем $\mathfrak{m}$ равным ядру гомоморфизма λ. Поскольку $\mathbb{Z}/n\mathbb{Z} \subset F$, имеем $\mathfrak{m} \cap \mathbb{Z} = n\mathbb{Z}$. Мы доказываем, что $\sigma_n[\mathfrak{m}] = \mathfrak{m}$. Для $\alpha \in \mathfrak{m}$ имеем $\lambda(\sigma_n(\alpha)) = \rho(\lambda(\alpha)) = \rho(0) = 0$, поэтому $\sigma_n(\alpha) \in \mathfrak{m}$. Следовательно, $\sigma_n[\mathfrak{m}] \subset \mathfrak{m}$, и равенство получается так же, как и прежде. Мы заключаем, что $\mathfrak{m}$ удовлетворяет (10.1). Из (10.5) (см. ниже) вытекает, что λ сюръективно, так что $\mathbb{Z}[\zeta_{p^k}]/\mathfrak{m} \simeq F$.

Этим заканчивается описание второго метода построения $\mathfrak{m}$. Для явного нахождения образующих $\mathfrak{m}$ потребовалась бы некоторая дополнительная работа, но на самом деле они не нужны: чтобы проверить сравнение по модулю $\mathfrak{m}$, достаточно применить λ и проверить соответствующее равенство в F.

Если $f = 1$, то во втором методе можно просто взять $F = \mathbb{Z}/n\mathbb{Z}$ и ρ равным тождественному отображению. Заметим,

что $f=1$ тогда и только тогда, когда $n \equiv 1 \bmod p^k$. Это не есть редкий случай, поскольку на практике p^k мало.

Если один из наших двух методов успешно конструирует идеал $\mathfrak{m}$, удовлетворяющий (10.1), то $\mathfrak{m}$ в самом деле максимально возможный, даже если n не простое. Это непосредственно вытекает из следующего предложения.

(10.5) **Предложение.** *Пусть $\mathfrak{m}$ — идеал в $\mathbb{Z}[\zeta_{p^k}]$, удовлетворяющий* (10.1). *Тогда число элементов $\mathbb{Z}[\zeta_{p^k}]/\mathfrak{m}$ не меньше n^f.*

Доказательство. Из $\mathfrak{m} \cap \mathbb{Z} = n\mathbb{Z}$ следует, что $\mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}[\zeta_{p^k}]/\mathfrak{m}$. Обозначим $\bar{\zeta} = (\xi_{p^k} \bmod \mathfrak{m})$. Достаточно показать, что отображение $(\mathbb{Z}/n\mathbb{Z})^f \to \mathbb{Z}[\zeta_{p^k}]/\mathfrak{m}$, переводящее $(a_i)_{i=0}^{f-1}$ в $\sum_{i=0}^{f-1} a_i \bar{\zeta}_i$, инъективно. Предположим поэтому, что $\sum_{i=0}^{f-1} a_i \bar{\zeta}^i = 0$. Из $\sigma_n[\mathfrak{m}] = \mathfrak{m}$ мы видим, что σ_n индуцирует автоморфизм $\mathbb{Z}[\zeta_{p^k}]/\mathfrak{m}$, который отображает $\bar{\zeta}$ в $\bar{\zeta}^n$. Применяя повторно этот автоморфизм, находим

$$(10.6) \qquad \sum_{i=0}^{f-1} a_i \bar{\zeta}^{in^j} = 0 \text{ для } 0 \leqslant j < f.$$

Из тождества $\prod_{x=1}^{p^k-1}(1-\zeta_{p^k}^x) = p^k$ в доказательстве (7.17) и из НОД $(p, n) = 1$ следует, что $1 - \bar{\zeta}^x \in (\mathbb{Z}[\zeta_{p^k}]/\mathfrak{m})^*$ для всех $x \in \mathbb{Z}$, $x \not\equiv 0 \bmod p^k$. Поэтому определитель Вандермонда

$$\det(\bar{\zeta}^{in^j})_{0 \leqslant i,\, j < f} = \prod_{0 \leqslant i < j < f} (\bar{\zeta}^{n^j} - \bar{\zeta}^{n^i})$$

обратим в $\mathbb{Z}[\zeta_{p^k}]/\mathfrak{m}$, и по (10.6) следует, что $a_i = 0$ для $0 \leqslant i < f$. Это доказывает (10.5).

Привлекательной чертой нашего второго метода построения $\mathfrak{m}$ является то, что он дает нам легкий способ проверки условия (6.4).

(10.7) **Предложение.** *Пусть F — кольцо с n^f элементами, которое содержит $\mathbb{Z}/n\mathbb{Z}$ в качестве подкольца. Допустим, что F содержит элемент β, удовлетворяющий* (10.4) *для некоторого кольцевого гомоморфизма ρ: $F \to F$. При $p=2$ и $n \equiv 3 \bmod 4$ предположим, что $k \geqslant 2$. Тогда ρ удовлетворяет условию* (6.4).

Доказательство. Положим $\bar{\zeta} = \beta^{(n^f-1)/p^k}$. Из доказательства (10.5) мы видим, что $\det(\rho^j(\bar{\zeta}^i))_{0 \leqslant i,\, j < f} \in F^*$, и, следовательно, $1, \bar{\zeta}, \bar{\zeta}^2, \ldots, \bar{\zeta}^{f-1}$ — базис F над $\mathbb{Z}/n\mathbb{Z}$. Таким образом, по терминологии [16, разд. 8] F есть расширение Галуа ранга f над

$\mathbf{Z}/n\mathbf{Z}$ с группой $\langle\rho\rangle$. Мы можем теперь применить [16, теорема 8.4] с s, равным наибольшей степени p, делящей n^f-1, и $\alpha=\beta^{(n^f-1)/s}$. Тогда мы находим, что для каждого $r|n$ существует $i\in\mathbf{Z}$, такое, что $r\equiv n^i \bmod s$; следовательно, по (5.1) $rn^{-i}\in 1+s\mathbf{Z}_p=(n^f)^{\mathbf{Z}_p}$ и (6.4) вытекает непосредственно. Это доказывает (10.7).

Для вывода последнего результата этого раздела мы предположим, что $n\equiv 3 \bmod 4$. Пусть $u\in\mathbf{Z}/n\mathbf{Z}$ выбрано так, что $u^2+4\in(\mathbf{Z}/n\mathbf{Z})^*$, и пусть F — кольцо:

$$(\mathbf{Z}/n\mathbf{Z})[T]/(T^2-uT-1).$$

Обозначим ξ класс вычетов T, и пусть ρ — автоморфизм F, $\rho(\xi)=u-\xi$. Заметим, что $\rho(\xi)=-\xi^{-1}$.

Если n простое и $(u^2+4)/n=-1$, то F — *поле*, в котором ξ и $\rho(\xi)$ сопряжены, поэтому $\rho(\xi)=\xi^n$ по теории конечных полей и $\xi^{n+1}=-1$. Следующее предложение показывает нам, что можно сказать, если $\xi^{n+1}=-1$. Читатель, интересующийся функциями Лукаса [26], должен заметить, что $\xi^{n+1}=-1$ эквивалентно $\xi^{(n+1)/2}+\rho(\xi)^{(n+1)/2}=0$, поскольку $n\equiv 3 \bmod 4$.

(10.8) **Предложение.** *Допустим, что* $n\equiv 3 \bmod 4$ *и что в предыдущих обозначениях* $\xi^{n+1}=-1$. *Тогда* $p=2$ *удовлетворяет условию* (6.4).

Доказательство. Это непосредственное следствие (10.7) с $k=2$, $f=2$ и $\beta=\xi$ и доказывает (10.8).

Мы оставляем читателю вывод (10.8) прямо из свойств функции Лукаса и доказательство того, что допущения (10.8) также влекут за собой, что $(u^2+4)/n=-1$.

11. ЦЕНТРАЛЬНАЯ СТАДИЯ АЛГОРИТМА

В этом разделе мы дадим более детальное описание второй стадии нашего теста простоты, чем то, которое было дано в разд. 2.

(11.1) Пусть n — целое число, которое надо проверить на простоту, $n>1$, и пусть t и s — целые числа, удовлетворяющие (2.1)—(2.4), и НОД$(st,n)=1$. Мы описываем алгоритм, который ведет либо к доказательству того, что n составное, либо к доказательству того, что выполняется (2.5).

(a) Сначала для каждой степени простого числа p^k, делящей t, выбирают идеал $\mathfrak{m}=\mathfrak{m}_{p,k}$ в $\mathbf{Z}[\zeta_{p^k}]$, удовлетворяющий (10.1). Это делают, либо полагая $\mathfrak{m}=n\mathbf{Z}[\zeta_{p^k}]$, либо используя один из методов, описанных в разд. 10.

(b) Далее полагают Y_s таким, как в (6.3), и проверяют, что каждый $\chi = \chi_{p,q} \in Y_s$ удовлетворяет (7.9). Если p нечетное, то это делают, выбирая a, b, как в (8.6), вычисляя сумму Якоби $J(\chi^a, \chi^b)$ и проверяя, что выполнено (8.8); если (8.8) не выполнено для некоторой пары p, q, то n составное по (8.5), и алгоритм останавливается. Если $p = 2$, то продолжают подобным образом, заменяя (8.8) на то из утверждений (9.2), (9.4), (9.6), (9.11) или (9.20), которое применимо.

(c) Наконец, проверяют, что каждое простое p, делящее t, удовлетворяет условию (6.4). Процедура, с помощью которой это делается, описана в (11.2) для нечетных p и в (11.5) для $p = 2$. Если это было сделано, то из (7.8) вытекает, что каждый $\chi \in Y_s$ удовлетворяет (6.5). Из теоремы (6.3) можно теперь вывести желаемое заключение, что (2.5) выполняется. Это конец второй стадии.

(11.2) Пусть n, t, s такие, как в (11.1), и пусть p нечетное простое, делящее t. Мы описываем процедуру, которая приводит либо к доказательству того, что n составное, либо к доказательству того, что p удовлетворяет условию (6.4).

Если в (11.1)(a) использовался алгоритм (10.3) для построения $\mathfrak{m}$, то достаточно применять (10.7). В противном случае можно поступить следующим образом.

(a) Сначала проверяют, что $n^{p-1} \not\equiv 1 \bmod p^2$. Если это выполнено, то (6.4) удовлетворяется в силу (7.18) и процедура останавливается.

(b) Далее проверяют, существует ли простое q, делящее s, с $q - 1$, делящимся на p, такое, что $\chi = \chi_{p,q}$ удовлетворяет (7.9) с *примитивным* корнем ζ степени p^k из единицы; здесь $k = v_p(q-1)$. Вычисления, которые необходимы для проверки этого, уже были выполнены на стадии (b) алгоритма (11.1) (ср. замечание (8.9)(b)). Если такое простое q действительно существует, то (6.4) выполняется по (7.19) и процедура останавливается.

(c) Допустим теперь, что (a) и (b) оказались неспособными установить (6.4). Тогда сначала проверяют, является ли n p-й степенью целого числа. Если это имеет место, то, очевидно, n составное и процедура останавливается.

(d) Далее определяют простое число q (не обязательно делящее s), для которого

(11.3) $$q \equiv 1 \bmod p, \quad n^{(q-1)/p} \not\equiv 1 \bmod q.$$

Такое простое число q может быть найдено испытанием всех простых чисел последовательно (ср. замечание (11.4)(a) ниже).

(e) Теперь, если q делит s, мы объявляем, что n составное (см. (11.4)(b)) и процедура останавливается. Допустим, нако-

нец, что q не делит s. Тогда сначала проверяют, что q не делит n. Далее полагают χ равным характеру по модулю q порядка p и проверяют, используя (8.5), выполняется ли (7.9) с *примитивным* $\zeta \in U_p$. Если это имеет место, то (6.4) удовлетворяется по (7.19), а если нет, то мы объявляем, что n составное (см. (11.4) (b)). Во всех случаях процедура останавливается.

(11.4) *Замечания.* (a) Если n не есть p-я степень, то плотность множества простых q, удовлетворяющих (11.3), есть $1/p$. Чтобы увидеть это, заметим, что для простого q, не делящего n, условие (11.3) эквивалентно условию, что q полностью расщепляется в $\mathbb{Q}(\zeta_p)$, но не в $\mathbb{Q}(\zeta_p, n^{1/p})$; далее можно применить хорошо известную теорему о том, что плотность множества полностью расщепляющихся простых в нормальном числовом поле степени d над $\mathbb{Q}$ равна $1/d$ (см. [11, гл. VIII]).

Отсюда следует, что простое $q \equiv 1 \bmod p$ удовлетворяет (11.3) с вероятностью $(p-1)/p$. Поэтому желаемое q нетрудно найти. Если предположить справедливость обобщенной гипотезы Римана, то можно доказать, что наименьшее простое q, удовлетворяющее (11.3), не превосходит величины $cp^2(\log p + \log n)^2$ при некоторой абсолютной эффективно вычислимой постоянной c согласно [9, следствие 1.3]. Без недоказанных гипотез удовлетворительная верхняя оценка для q неизвестна. Следовательно, мы не можем дать удовлетворительной верхней границы для времени работы части (d) процедуры (11.2).

(b) Чтобы оправдать утверждения, сделанные в (11.2) (e), предположим, что n простое и что q простое, удовлетворяющее (11.3), q не делит n. Пусть χ такой, как в (11.2) (e), если q не делит s, и $\chi = \chi_{p,q}$, если q делит s. Обозначим порядок χ через p^k. Тогда из (11.3) следует, что $\chi(n)$ —примитивный корень степени p^k из единицы, поэтому из (7.5) вытекает, что χ удовлетворяет (7.9) с *примитивным* $\zeta \in U_{p^k}$.

Следовательно, если обнаруживается, что (7.9) не выполнено с примитивным ζ, то можно заключить, что n составное. Это применяется, в частности, если q делит s, поскольку в этом случае в (11.2) (b) было обнаружено, что $\chi = \chi_{p,q}$ не удовлетворяет (7.9) с примитивным ζ. Это доказывает утверждения в (11.2) (e).

(c) Процедура (11.2) вполне эффективна на практике, несмотря на теоретические трудности, упомянутые в (11.4) (a). В действительности редко случается, что части (c), (d) и (e) процедуры необходимы. Это случается, например, если n — простое число, которое сравнимо с p-й степенью по модулю p^2s. Если n с большой вероятностью должно быть простым, то про-

цедуру можно ускорить за счет пропуска части (c) и ограничения поиска в (d) по простым q, не делящим s.

(11.5) Пусть n, t, s такие, как в (11.1), и предположим, что t *четное*. Мы описываем процедуру, которая либо доказывает, что $p=2$ удовлетворяет (6.4), либо доказывает, что n составное.

Сначала предположим, что $n \equiv 1 \bmod 4$. В этом случае определяют целое число a, удовлетворяющее $\left(\frac{a}{n}\right)=-1$, испытывая простые числа 2, 3, 5, ... последовательно, и проверяют, будет ли выполнено сравнение $a^{(n-1)/2} \equiv -1 \bmod n$; если это имеет место, то $p=2$ удовлетворяет (6.4) по (7.24); в противном случае n составное по (1.2). Если трудно найти целое a, $\left(\frac{a}{n}\right)=-1$, то проверяют, является ли n квадратом.

Далее предположим, что $n \equiv 3 \bmod 4$. В этом случае определяют целое u, удовлетворяющее равенству $(u^2+4)/n=-1$, испытанием $u=1, 2, 3, \ldots$ (ср. (11.6) (a)). Далее полагают

$$\xi=(T \bmod T^2-uT-1) \in (\mathbb{Z}/n\mathbb{Z})[T]/(T^2-uT-1),$$

как и было определено в (10.8), и проверяют, выполняется ли равенство $\xi^{n+1}=-1$; если оно имеет место, то $p=2$ удовлетворяет (6.4) по (10.8); в противном случае n составное по замечанию, предшествующему (10.8).

Это завершает описание процедуры. Альтернативно можно использовать (7.25) или (7.26).

(11.6) *Замечания.* (a) Замечания, сделанные в (11.4) (a) о существовании и величине q, также применимы к числу a, которое появляется в описанной выше процедуре для $n \equiv 1 \bmod 4$.

Допустим, что $n \equiv 3 \bmod 4$. Мы доказываем, что существует $u \in \mathbb{Z}$ с $(u^2+4)/n=-1$. Пусть r — простой делитель числа n с *нечетным* $v_r(n)$, и пусть a — наименьшее положительное целое число, для которого $\left(\frac{a}{r}\right)=-1$. В силу минимальности a существуе v, $v^2 \equiv a-1 \bmod r$, и тогда $(v^2+1)/r=-1$. Пусть теперь $u \in \mathbb{Z}$, такое, что $u \equiv 2v \bmod r$, и такое, что u делится на все другие простые числа, которые делят n. Тогда легко проверить, что $(u^2+4)/n=-1$, как и требовалось.

Если верна обобщенная гипотеза Римана, то существует абсолютная эффективно вычислимая постоянная c со следующим свойством: если n — положительное нечетное целое число, не являющееся квадратом, и n не имеет простого делителя $\leqslant c^2(\log n)^4$, то наименьшее положительное целое u, $(u^2+4)/n=-1$, удовлетворяет неравенству $u \leqslant c(\log n)^2$. Это можно доказать, комбинируя [9, следствие 1.3] с [3, лемма 1]. Мы признательны А. М. Одлизко за это наблюдение.

(b) Поиск q в (11.2) (d) и поиск a и u в (11.5) суть единственные места в нашем алгоритме проверки простоты, которые

мешают нам доказать для худшего случая оценку времени работы вида $(\log n)^{c \log \log \log n}$. Из (11.4) (a) и (11.6) (a) следует, что справедливость обобщенной гипотезы Римана влечет за собой такую границу для алгоритма; мы должны тогда выбрать $\mathfrak{m} = n\mathbb{Z}[\zeta_{p^k}]$ в (11.1) (a). Если мы хотим, чтобы результат Померанса и Одлизко, упомянутый в разд. 1, имел место для нашего алгоритма, мы должны использовать алгоритм (10.3) в (11.1) (a) и применить (10.7) для проверки (6.4). Условие $k \geqslant 2$ в (10.7) для $p = 2$ и $n \equiv 3 \bmod 4$ не является серьезным ограничением (ср. (7.28)).

12. ДЕТАЛЬНОЕ ОПИСАНИЕ АЛГОРИТМА

(12.1) Пусть N — некоторое большое целое число. Мы описываем с вычислительной точки зрения алгоритм для определения, является ли целое число n, $1 < n \leqslant N$, простым.

Шаг 1. Подготовка таблиц. Эти таблицы зависят только от N и могут быть составлены раз и навсегда.

(a) Выбрать положительное целое число t, $e(t) > N^{1/2}$ (ср. разд. 4, табл. 1).

(b) Выполнить шаги (b1) и (b2) для каждого нечетного простого $q \mid e(t)$.

(b1) Найти методом проб и ошибок примитивный корень g по модулю q, т. е. целое $g \not\equiv 0 \bmod q$, такое, что $g^{(q-1)/p} \not\equiv 1 \bmod q$ для каждого простого $p \mid q-1$. Составить таблицу для функции f: $\{1, 2, \ldots, q-2\} \to \{1, 2, \ldots, q-2\}$, определенной из сравнения $1 - g^x \equiv g^{f(x)} \bmod q$.

(b2) Выполнить шаги (b2a), (b2b), (b2c), (b2d), (b2e), (b2f) для каждого простого $p \mid q-1$.

(b2a) Положить $k = v_p(q-1)$; это число делителей p в $q-1$.

(b2b) Если $p^k \neq 2$, вычислить

$$J_{p,q} = \sum_{x=1}^{q-2} \zeta_{p^k}^{x+f(x)} \in \mathbb{Z}[\zeta_{p^k}].$$

Здесь элемент $\sum_{0 \leqslant i < (p-1)p^{k-1}} a_i \zeta_{p^k}^i$ из $\mathbb{Z}[\zeta_{p^k}]$ с $a_i \in \mathbb{Z}$ должен быть представлен как вектор $(a_i)_{0 \leqslant i \leqslant (p-1)p^{k-1}}$ (ср. разд. 7). (Заметим, что $J_{p,q} = J(\chi, \chi)$ для $\chi = \chi_{p,q}$; см. 8.1).)

(b2c) Если $p \neq 2$, проделать следующее. Пусть

$$M = \{x \in \mathbb{Z}\colon 1 \leqslant x \leqslant p^k,\ x \not\equiv 0 \bmod p\},$$

$$\theta = \sum_{x \in M} x\sigma_x^{-1} \in \mathbb{Z}[G],$$

$$\alpha(v) = \sum_{x \in M} \left[\frac{vx}{p^k}\right] \sigma_x^{-1} \in \mathbb{Z}[G] \text{ для } v \in M,$$

где $[y]$ — наибольшее целое $\leqslant y$, а σ_x и G такие, как в разд. 7. Вычислить

$$J_{0,p,q}=J^{\theta}_{p,q}, \quad J_{v,p,q}=J^{\alpha(v)}_{p,q}$$

для каждого $v\in M$ как элементы $\mathbb{Z}[\zeta_{p^k}]$ (см. определение действия $\mathbb{Z}[G]$ в разд. 7). Числа $J_{v,p,q}$ для $v\in\{0\}\cup M$ должны быть табулированы.

(b2*d*) Есла $p=2$, $k=1$, положить $J_{0,2,q}=q$, $J_{1,2,q}=1$ и табулировать эти значения.

(b2e) Если $p=2$, $k=2$, сделать следующее. Вычислить

$$J_{0,2,q}=J^2_{2,q}\cdot q\in\mathbb{Z}[\zeta_4]$$

и положить $J_{1,2,q}=1$, $J_{3,2,q}=J^2_{2,q}$. Числа $J_{v,2,q}$ для $v=0, 1, 3$ нужно табулировать.

(b2f) Если $p=2$, $k\geqslant 3$, сделать следующее. Вычислить

$$J^*_{2,q}=J_{2,q}\sum_{x=1}^{q-2}\zeta_{2^k}^{2x+f(x)}, \quad J^{\#}_{2,q}=\left(\sum_{x=1}^{q-2}\zeta_8^{3x+f(x)}\right)^2$$

как элементы $\mathbb{Z}[\zeta_{2^k}]$, где $\zeta_8=\zeta_{2^k}^{2^{k-3}}$. (Заметим, что $J^*_{2,q}=J(\chi,\chi,\chi)$ и $J^{\#}_{2,q}=J(\varphi,\varphi^3)^2$ с $\varphi=\chi^{2^{k-3}}$, как в разд. 9.) Пусть

$$L=\{x\in\mathbb{Z}:\ 1\leqslant x\leqslant 2^k,\ x \text{ нечетно}\},$$

$$M=\{x\in L:\ x\equiv 1 \text{ или } 3 \bmod 8\},$$

$$\theta=\sum_{x\in M}x\sigma_x^{-1}\in\mathbb{Z}[G],$$

$$\alpha(v)=\sum_{x\in M}\left[\frac{vx}{2^k}\right]\sigma_x^{-1}\in\mathbb{Z}[G]$$

для $v\in L$; вычислим

$$J_{0,2,q}=(J^*_{2,q})^{\theta}, \quad J_{v,2,q}=(J^*_{2,q})^{\alpha(v)} \quad \text{для } v\in M,$$

$$J_{v,2,q}=(J^*_{2,q})^{\alpha(v)}J^{\#}_{2,q} \quad \text{для } v\in L-M.$$

Числа $J_{v,2,q}$ для $v\in\{0\}\cup L$ нужно табулировать.

Шаг 2. Предварительные тесты. Пусть теперь задано целое число n, $1<n\leqslant N$, которое нужно проверить на простоту.

(c) В зависимости от информации об n, которая уже имеется, уместно испытать n на наличие малых делителей или подвергнуть n тесту Миллера и Рабина [см. [8]).

(d) Проверить, что НОД$(te(t), n)=1$, используя алгоритм Евклида. Если это не так, то получен простой делитель числа n,

поскольку $te(t)$ полностью разложено на множители, и мы останавливаемся.

(e) Выбрать делитель s числа $e(t)$ с $s > n^{1/2}$ (ср. разд. 4). Заменить t на наименьшее t', для которого s делит $e(t')$. (Заметим, что новое t есть показатель группы $(\mathbb{Z}/s\mathbb{Z})^*$ и поэтому делит старое t.)

Шаг 3. Тесты псевдопростоты с суммами Якоби. Выполнить шаги (f), (g), (h) для каждого простого p, делящего t.

(f) Ввести булеву переменную λ_p говорящую нам, было ли проверено (6.4)). Положить $\lambda_p =$ «истинно», если p нечетное и $n^{p-1} \not\equiv 1 \bmod p^2$, и $\lambda_p =$ «ложно» в противном случае.

(g) Для каждого целого числа $k \geqslant 1$, $p^k | t$, определить целые числа u_k, v_k, такие, что $n = u_k p^k + v_k$ и $0 \leqslant v_k < p^k$.

(h) Выполнить шаги (h1), (h2), (h3) для каждого простого $q | s$, $p | q - 1$.

(h1) Положить $k = v_p(q-1)$ и $u = u_k$, $v = v_k$, как в (g). Вычислить

$$J^u_{0,\,p,\,q} J_{v,\,p,\,q} \bmod n\mathbb{Z}\left[\zeta_p{}^k\right]$$

путем повторных возведений в квадрат и умножений по модулю $n\mathbb{Z}\left[\zeta_p{}^k\right]$; здесь класс вычетов

$$\left(\sum_{0 \leqslant i < (p-1)\,p^{k-1}} a_i \zeta_p{}^{ik} \bmod n\mathbb{Z}\left[\zeta_p{}^k\right]\right)$$

с $a_i \in \mathbb{Z}$ должен быть представлен как вектор $(b_i)_{0 \leqslant i < (p-1)\,p^{k-1}}$, где $b_i \in \{0, 1, \ldots, n-1\}$, $b_i \equiv a_i \bmod n$. Если не существует $h \in \{0, 1, \ldots, p^k - 1\}$, такого, что

$$J^u_{0,\,p,\,q} J_{v,\,p,\,q} \equiv \zeta_p{}^{hk} \bmod n\mathbb{Z}\left[\zeta_p{}^k\right],$$

то n составное и алгоритм останавливается. (Это тест (8.8) с $a = b = 1$, если p нечетное; тест (9.2), если $p^k = 2$; тест (9.4) или (9.6), если $p^k = 4$; тест (9.11) или (9.20), если $p = 2$, $k \geqslant 3$.) Предположим теперь, что h существует.

(h2) Если $h \not\equiv 0 \bmod p$ и либо $p^k = 2$, $n \equiv 1 \bmod 4$, либо p нечетно, положить $\lambda_p =$ «истинно». (Это комбинирует (7.24) и (7.19).)

(h3) Если $h \not\equiv 0 \bmod 2$, $p = 2$, $k \geqslant 2$ и $\lambda_2 =$ «ложно», проделать следующее. Проверить, справедливо ли сравнение $q^{(n-1)/2} \equiv -1 \bmod n$. Если оно не справедливо, то n составное и алгоритм останавливается. Если оно справедливо, то положить $\lambda_2 =$ «истинно». (Это (7.26).)

Шаг 4. Дополнительные тесты. Выполнить шаги (i) и (j) для каждого простого p, делящего t, для которого $\lambda_p =$ «ложно».

(i) Выбрать малое простое число q, не делящее s, такое, что

$$q \equiv 1 \bmod p,$$

$$q \equiv 1 \bmod 4, \text{ если } p = 2 \text{ и } n \equiv 3 \bmod 4,$$

$$n^{(q-1)/p} \not\equiv 1 \bmod q.$$

Если такое простое q не может быть найдено в разумных пределах, проделать следующее. Проверить, является ли n p-й степенью. Если это так, объявить n составным и остановиться. В противном случае остановиться с выдачей сообщения, что алгоритм оказался неспособен доказать, что n простое. Предположим теперь, что q найдено. Остановиться, если $n \equiv 0 \bmod q$.

(j) Положить $k = 2$, если $p = 2$ и $n \equiv 3 \bmod 4$, и $k = 1$ в противном случае. Определить целые числа u_k, v_k, как в (g). Вычислить $J_{v,p,q}$, как в (b1), (b2c), (b2d), (b2e), но только для $v \in \{0, v_k\}$. Проверить, справедливо ли сравнение

$$J_{0,p,q}^{u_k} J_{v_k,p,q} \equiv \zeta_p^{h_k} \bmod n\mathbf{Z}[\zeta_p^k]$$

для некоторого $h \in \mathbf{Z}$, $0 \leqslant h < p^k$, $h \not\equiv 0 \bmod p$. Если это не так, то n составное и алгоритм останавливается. (Чтобы убедиться в справедливости этого, см. (11.4) (b).) В противном случае выполнить шаги (h2) и (h3).

Шаг 5. *Финальные пробные деления.* (Маловероятно, что на этом шаге будет обнаружено, что n составное, ср. замечание в конце разд. 2.)

(k) Положить $r_0 = 1$.

(l) Выполнить шаги (l1), (l2), (l3) для $i = 1, 2, \ldots, t$.

(l1) Определить r_i из $r_i \equiv nr_{i-1} \bmod s$, $0 \leqslant r_i < s$.

(l2) Если $r_i = 1$, объявить, что n простое, и остановиться.

(l3) Если $r_i | n$ и $r_i < n$, объявить, что n составное, и остановиться.

(Заметим, что либо (l2), либо (l3) применяется для некоторого $i \leqslant t$, поскольку $n^t \equiv 1 \bmod s$.) Этим заканчивается описание алгоритма.

(12.2) *Замечания.* (a) Поскольку мы использовали $a = b = 1$ в (8.8) (см. шаг (h1)), правильность теста гарантирована, если только $2^p \not\equiv 2 \bmod p^2$ для всех простых $p | t$ (ср. 8.6)). Это условие удовлетворяется для всех $p < 1093$ (см. (8.9) (c)). На практике мы обычно имеем $p < 20$ (см. разд. 4, табл. 1).

(b) В предыдущее описание не были включены некоторые улучшения. Во-первых, не использовались результаты разд. 10. Во-вторых, не был включен алгоритм (3.1). В-третьих, была отвергнута возможность комбинировать тест с предыдущими тестами, описанными в [26] (см. [16, разд. 8]).

13. РЕАЛИЗАЦИЯ

Алгоритм, описанный в разд. 12, был реализован авторами на вычислительной системе CDC Cyber в вычислительном центре SARA в Амстердаме. В этом разделе мы обсуждаем главные особенности этой реализации; подробности читатель найдет в статье Коэна и Ленстры, которая будет опубликована позже.

Были написаны две программы, одна на Паскале, другая на Фортране. Обе программы используют стандартные подпрограммы многократной точности, которые были написаны Уинтером на собирательном языке Компас и сделаны доступными Математическим центром в Амстердаме.

Вспомогательноо число t было выбрано равным 5040 для программы на Паскале и 55 440 для программы на Фортране. Мы имеем $e(5040) > 1.5 \cdot 10^{52}$ и $e(55\,440) > 4.9 \cdot 10^{106}$, так что программа на Паскале может работать с числами до 104 десятичных цифр, а программа на Фортране — с числами до 213 десятичных цифр.

Эти программы включают следующие улучшения, которые не входят в алгоритм разд. 12. Использовались результаты разд. 10, но только в тех случаях, когда целое число f, определенное в начале этого раздела, равно 1. Мы также строим кольцо F из n^2 элементов, являющееся полем, если n простое. Это кольцо позволило иам комбинировать наш алгоритм с тестом, основанным на известных простых делителях $n^2 - 1$ (см. [16, разд. 8]).

Программа на Фортране не пользуется подготовленными таблицами, как списано на шаге 1 алгоритма в разд. 12, поскольку такие таблицы потребовали бы слишком много пространства памяти. Вместо этого необходимые фрагменты таблиц вычислялись заново для каждого n.

Для каждой степени p^k простого числа, делящей t, были написаны специальные подпрограммы для выполнения умножения в $\mathbb{Z}[\zeta_{p^k}]/n\mathbb{Z}[\zeta_{p^k}]$, или, эквивалентно, для умножения многочленов степени, меньшей чем $m = (p-1)p^{k-1}$, с коэффициентами в $\mathbb{Z}/n\mathbb{Z}$ по модулю p^k-го многочлена деления круга $\sum_{i=0}^{p-1} X^{ip^{k-1}}$. В дополнение к m необходимым приведениям по модулю n прямой способ проделать одно такое умножение занимает m^2 умножений целых чисел. Важно уменьшить это число. Теоретически в силу теоремы Винограда (см. [8]) достаточно $2m - 1$ умножений целых чисел; но метод Винограда совершенно непрактичен, поскольку включает очень большое число сложений и умножений на малые постоянные. Мы использовали специальные формулы для каждого p^k. Например, для $p^k = 16$

мы используем 27 умножений целых чисел вместо 64, чтобы выполнить одно умножение в $\mathbb{Z}[\zeta_{16}]/n\mathbb{Z}[\zeta_{16}]$, и только 18, чтобы возвести один раз в квадрат. Возможно, что по этим направлениям возможны дальнейшие улучшения.

Таблица 3

Время работы программы на Паскале в секундах (см. текст)

Число цифр	Среднее	Стандартное отклонение	Максимум	Минимум
50	6.437	1.687	10.030	4.525
60	8.634	2.554	15.168	5.009
70	12.074	2.289	15.214	7.032
80	16.224	3.897	23.800	8.006
90	25.572	5.870	35.752	15.810
100	32.349	9.103	47.689	17.891

Таблица 4

Время работы программы на Фортране в секундах (см. текст)

Число цифр	Среднее	Стандартное отклонение	Максимум	Минимум
100	50.442	15.203	75.416	26.031
120	97.797	28.274	147.259	51.077
140	156.429	43.122	210.756	77.316
160	246.204	44.144	298.144	111.888
180	359.728	55.833	436.039	259.021
200	495.748	80.025	614.254	258.859

В табл. 3 и 4 приводятся данные о времени работы программ на Паскале и Фортране соответственно. Для каждого числа d в первом столбце мы испытывали 20 простых чисел с d десятичными цифрами. Каждое простое выбиралось путем извлечения случайного числа с d цифрами и использования программы для определения наименьшего простого числа, большего, чем полученное число. Второй столбец дает среднее время работы $\bar{t} = (\sum_{i=1}^{20} t_i)/20$, третий — пробное стандартное отклонение $\sum_{i=1}^{20} (t_i - \bar{t})^2/19)^{1/2}$, четвертый — максимальное время работы, пятый — минимальное время работы. Время дано в секундах. Время, потраченное на составные числа, не подсчитано.

Две программы проверяли одно и то же множество из 20 стоцифровых простых чисел. Таблицы показывают, что для этих чисел программа на Фортране работает медленнее, чем программа на Паскале. Это в основном вызвано тем, что каждая программа работает в заданной точности, которая в два раза больше для программы на Фортране, чем на Паскале. Лишь небольшая часть разницы во времени связана с использованием программой на Паскале подготовленных таблиц.

Мы проводим скорость работы используемых подпрограмм многократной точности. Обозначим через $a_m b_m$ числа, состоящие из m слов, каждое слово содержит 47 битов. Тогда вычисление

$$a_8 b_8, \quad a_{16} b_{16}, \quad (a_{16} \bmod b_8) = a_{16} - [a_{16}/b_8]\, b_8,$$
$$(a_{32} \bmod b_{16}) = a_{32} - [a_{32}/b_{16}]\, b_{16}$$

занимает в среднем меньше, чем $7 \cdot 10^{-5}$, $2.1 \cdot 10^{-4}$, $2 \cdot 10^{-4}$ и $4.7 \cdot 10^{-4}$ секунд соответственно.

Мы выражаем благодарность Д. Т. Уинтеру за написание программ многократной точности и А. К. Ленстре за его огромную помощь в реализации алгоритма и выполнении всех тестов, о которых сообщалось в этом разделе.

ЛИТЕРАТУРА

[1] Adleman L. M., Pomerance C., Rumely R. S. On distinguishing prime numbers from composite numbers. — Ann. Math., 1983, v. 117, p. 173—206.
[2] Brillhart J., Lehmer D. H., Selfridge J. L. New primality criteria and factorization of $2^m \pm 1$. — Math. Comp.. 1975, v. 29, p. 620—647.
[3] Burgess D. A. On the quadratic character of a polynomial. — J. London Math. Soc., 1967, v. 42, p. 73—80.
[4] Hardy G. H., Wright E. M. An Introduction to the Theory of Numbers, 5th ed. — Oxford: Oxford Univ. Press, 1979.
[5] Hasse H. Vorlesungen über Zahlentheorie, 2nd ed. — Berlin: Springer-Verlag, 1964.
[6] Hasse H. Zahlentheorie, 3rd ed. — Berlin: Akademie-Verlag, 1969; англ. перевод: Number Theory. — Berlin: Springer-Verlag, 1980.
[7] Joly J. R. Equations et variétés algébriques sur un corps fini. — Enseign. Math., 1973, v. 19, p. 1—117.
[8] Knuth D. E. The Art of Computer Programming. Vol. 2. Seminumerical Algorithms, 2nd ed. — Reading, Mass.: Addison-Wesley, 1981. [Имеется перевод издания 1969 г.: Кнут Д. Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы. — М.: Мир, 1977.]
[9] Lagarias J. C., Montgomery H. L., Odlizko A. M. A bound for the least prime ideal in the Chebotarev density theorem. — Invent. Math., v. 54, 1979, p. 271—296.
[10] Lang S. Algebra. — Reading, Mass.: Addison-Wesley, 1965. [Имеется перевод: Ленг С. Алгебра. — М.: Мир, 1968.]
[11] Lang S. Algebraic Number Theory. — Reading, Mass.: Addison-Wesley, 1970.
[12] Lang S. Cyclotomic Fields. — New York: Springer-Verlag, 1978.
[13] Lehmer D. H. On Fermat's quotient, base two. — Math. Comp., 1981, v. 36, p. 289—290.

[14] Lehmer D. H. Strong Carmichael numbers. — J. Austral. Math. Soc., Ser. A, 1976, v. 21, p. 508—510.
[15] Lenstra H. W., Jr. Divisors in residue classes. — Math. Comp., 1984, v. 42, p. 331—340.
[16] Lenstra H. W., Jr. Primality Testing Algorithms (after Adleman, Rumely and Williams), Sem. Bourbaki, vol. 33, 1980/1981, Expose 576, p. 243—257. — In: Lecture Notes in Math. vol. 901. — Berlin: Springer-Verlag, 1981.
[17] Lenstra H. W., Jr. Primality testing with Artin symbols. — In: Koblitz N. (ed.), Number Theory Related to Fermat's Last Theorem. — Progress in Mathematics, vol. 26. — Boston: Birkhauser, 1982, p. 341—347.
[18] Martello S., Toth P. The 0-1 knapsack problem, Ch. 9. — In: Christofides N., Mingotti A., Toth P., Sandi S. (eds.) Combinatorial Optimization. — New York: Wiley, 1979.
[19] Miller G. L. Riemann's hypothesis and tests for primality. — J. Comput. System Sci., 1976, v. 13, p. 300—317.
[20] Prachar K. Über die Anzahl der Teiler einer natürlichen Zahl, welche die Form $p-1$ haben. — Monatsh. Math., 1955, v. 59, p. 91—97.
[21] Rabin M. O. Probabilistic algorithms for testing primality. — J. Number Theory, 1980, v. 12, p. 128—138.
[22] Serre,J.-P. Cours d'Arithmétique — Paris: Presses Universitaires de France, Paris, 1970; англ. перевод: A Course in Arithmetic. — New York: Springer-Verlag, 1973. [Имеется перевод: Серр Ж.-П. Курс арифметики. — М.: Мир, 1972.]
[23] Solovay R.. Strassen V. A fast Monte-Carlo test for primality. — SIAM J. Comput., 1977, v. 6, p. 84—85; erratum, ibid., 1978, v. 7, p. 118.
[24] Vélu J. Tests for primality under the Riemann hypothesis. — SIGACT News, 1978, v. 10, p. 58—59.
[25] Washington L. C. Introduction to Cyclotomic Fields. — New York: Springer-Verlag, 1982.
[26] Williams H. C. Primality testing on a computer. — Ars. Combin., 1978, v. 5, p. 127—185.

Делители в классах вычетов [1])

Х. Ленстра, мл.

В этой статье доказывается следующий результат. Пусть r, s и n — целые числа, удовлетворяющие неравенствам $0 \leqslant r < s < n$, $s > n^{1/3}$, НОД$(r, s) = 1$. Тогда существует не более 11 положительных делителей n, сравнимых с r по модулю s. Более того, имеется эффективный алгоритм для определения всех этих делителей. Граница 11 получена с помощью комбинаторной модели, связанной с теорией кодирования. Не известно, является ли 11 наилучшей возможной границей; в любом случае оно не может быть заменено на 5. Также не известно, справедливы ли подобные результаты для значительно меньших значений $\log s/\log n$. Алгоритм, применяемый в данной статье, имеет приложения в вычислительной теории чисел.

В данной статье мы доказываем следующую теорему.

Теорема. *Пусть r, s и n — целые числа, удовлетворяющие условиям*

$$0 \leqslant r < s < n, \quad s > n^{1/3}, \quad \text{НОД}(r, s) = 1.$$

Тогда существует не более 11 *положительных делителей n, сравнимых с r по модулю s, и существует полиномиальный алгоритм для определения всех этих делителей.*

Алгоритм, о котором говорится в теореме, описывается в разд. 1. Он *полиномиален* в том смысле, что число битовых операций, требуемых алгоритму, ограничено полиномиальной функцией от двоичной длины числа n. Точнее, мы увидим, что число битовых операций есть $O((\log n)^3)$. Используя технику быстрого умножения, мы можем улучшить эту границу до $O((\log n)^{2+\varepsilon})$ для любого $\varepsilon > 0$.

Упомянем о двух приложениях алгоритма. В некоторых алгоритмах проверки простоты (см. [3, 7]) число n, которое должно быть проверено, подвергается набору тестов «псевдопростоты». Если n не проходит все тесты, то оно составное. Если n проходит все тесты, то оказывается, что каждый делитель числа n лежит в небольшом и точно известном множестве классов

---

[1]) Lenstra H. W., Jr. Divisors in Residue Classes. — Mathematics of Computation, Jan. 1984, v. 42, No. 165, p. 331—340.

вычетов по модулю вспомогательного числа s. В последнем случае все делители n могут быть легко найдены, если s удовлетворяет условию $s > n^{1/2}$. Наш алгоритм показывает, что то же самое может быть сделано, если s удовлетворяет более слабому условию $s > n^{1/3}$. В частных случаях это наблюдение уже было сделано в [2, теоремы 5 и 17].

Второе применение относится к близкой задаче разложения n на множители. Выбирая в качестве s подходящее целое число, большее $n^{1/3}$, и применяя наш алгоритм ко всем классам вычетов $r \bmod s$, мы получаем алгоритм, который раскладывает n на множители за время $O(n^{(1/3)+\varepsilon})$ для каждого $\varepsilon > 0$. Та же граница была достигнута Леманом [6] и предположительно Пинтером [9] с помощью методов, аналогичных по духу. Существуют лучшие методы разложения как в теории, так и на практике (см. [7]), однако это приложение показывает по крайней мере, что может оказаться сложно распространить алгоритм на существенно меньшие значения s.

Для целей этих двух приложений ограничительное условие НОД$(r, s) = 1$, очевидно, не является существенным ограничением. Однако в теореме это условие не может быть опущено. Чтобы увидеть это, замечаем, что для нечетных n делители n^2, сравнимые с n по модулю $2n$, находятся во взаимно однозначном соответствии с делителями числа n. Их число не ограничено 11 и даже полиномиальной функцией от $\log(n^2)$ согласно [4, теорема 317]; поэтому они не могут быть определены с помощью полиномиального алгоритма.

В разд. 2 мы обсуждаем комбинаторную задачу, которая связана с теорией кодирования. Используя результаты разд. 2, мы завершаем доказательство вышеприведенной теоремы в разд. 3. Более общо, доказывается, что для любого вещественного числа $\alpha > 1/4$ существует число $c(\alpha)$ со следующим свойством: если r, s, n — положительные целые числа, удовлетворяющие условиям НОД$(r, s) = 1$, $s > n^{\alpha}$, то число положительных делителей n, равных $r \bmod s$, есть не более чем $c(\alpha)$. Мне не известно, справедлив ли этот результат для *любого* положительного α.

Число 11 в теореме наилучшее, которое можно получить с помощью нашего метода доказательства, однако не известно, является ли оно наилучшим возможным. Мы знаем лишь, что оно не может быть заменено на 5, как это показано в разд. 3 на примерах.

Мы выражаем благодарность Х. Коэну, П. Эрдёшу, Б. Лагевегу, А. Ленстре, А Одлизко, К. Померансу, Д. Загиру и Х. Зантеме, которые тем или иным образом внесли свой вклад в содержание этой статьи.

1. АЛГОРИТМ

Пусть r, s и n такие, как в теореме. Прежде чем мы опишем алгоритм, упоминаемый в теореме, вкратце очертим основную идею. Мы ищем делители n вида $xs + r$, поэтому должны решить уравнение

(1.1) $$(xs + r)(ys + r') = n$$

в неотрицательных целых числах x, y; здесь r' таково, что $rr' \equiv n \bmod s$. Рассматривая (1.1) по модулю s^2, получаем сравнение для $xr' + yr$ по модулю s. Это сравнение можно использовать для получения последовательности сравнений вида

$$xa_i + yb_i \equiv c_i \bmod s.$$

Пользуясь тем, что $s > n^{1/3}$, доказывают, что для некоторого i число $xa_i + yb_i$ столь мало, что остается лишь несколько возможных значений для $xa_i + yb_i$. Для каждого фиксированного значения i неизвестные x или y можно исключить из (1.1) и полученное квадратное уравнение решить.

(1.2) *Алгоритм.* При заданных r, s и n, таких, как в теореме, этот алгоритм определяет все положительные делители n, сравнимые с r по модулю s.

Во-первых, с помощью алгоритма Евклида вычислить целое число r^*, удовлетворяющее сравнению $r^*r \equiv 1 \bmod s$ (см. [5]); и определить целое число r':

$$r' \equiv r^*n \bmod s, \quad 0 \leqslant r' < s.$$

Во-вторых, для $i = 0, 1, 2, \ldots$ проделать следующее. Вычислить a_i, b_i, c_i по формулам

$$a_0 = s, \quad b_0 = 0, \quad c_0 = 0,$$

$$a_1 \equiv r'r^* \bmod s, \quad 0 < a_1 \leqslant s,$$

$$b_1 = 1,$$

$$c_1 \equiv \frac{n - rr'}{s} r^* \bmod s$$

и при $i \geqslant 2$ по формулам

$$a_i = a_{i-2} - q_i a_{i-1},$$

$$b_i = b_{i-2} - q_i b_{i-1},$$

$$c_i \equiv b_{i-2} - q_i c_{i-1} \bmod s,$$

где q_i — однозначно определенное целое число, для которого

$$0 \leqslant a_i < a_{i-1}, \text{ если } i \textit{ четно},$$

$$0 < a_i \leqslant a_{i-1}, \text{ если } i \textit{ нечетно}.$$

Далее, для каждого целого числа c, удовлетворяющего условиям

(1.3) $$c \equiv c_i \bmod s,$$
$$|c| < s, \text{ если } i \text{ четно},$$
$$2a_ib_i \leqslant c \leqslant \frac{n}{s^2} + a_ib_i, \text{ если } i \text{ нечетно},$$

решить систему уравнений

(1.4) $$\begin{cases} xa_i + yb_i = c, \\ (xs + r)(ys + r') = n \end{cases}$$

(см. (1.5)), и если x и y окажутся неотрицательными целыми числами, то добавить $xs + r$ к списку делителей числа n, равных $r \bmod s$. Если $a_i = 0$, то алгоритм останавливается в этом месте; в противном случае он продолжает работу со следующим значением i.

Этим заканчивается описание алгоритма (1.2). Корректность его будет доказана ниже (см. (1.7)).

(1.5) Нетрудно видеть, что система (1.4) может быть сведена к одному квадратному уравнению от одной переменной. В самом деле, если положить

$$u = a_i(xs + r), \quad v = b_i(ys + r'),$$

то

$$uv = a_ib_in, \quad u + v = cs + a_ir + b_ir',$$

так что u, v — нули многочлена

$$T^2 - (cs + a_ir + b_ir')T + a_ib_in.$$

Заметим, что числа a_i, b_i, появляющиеся в алгоритме, вычисляются с помощью расширенного алгоритма Евклида (см. [5]), примененного к s, a_1. Поэтому условие окончания $a_i = 0$ выполняется при некотором значении i; обозначая эту величину через t, получаем $t = O(\log s)$ по [5]. Поскольку $a_i > 0$ для нечетных i, число t *четно*.

Следующие свойства a_i, b_i легко проверяются по индукции:

$$(a_i, b_i) \in \mathbf{Z}_{>0} \times \mathbf{Z}_{>0} \text{ для } i \text{ нечетного}, \ 0 < i < t,$$
$$(a_i, b_i) \in (\mathbf{Z}_{\geqslant 0} \times \mathbf{Z}_{\leqslant 0}) - \{(0, 0)\} \text{ для } i \text{ четного}, \ 0 \leqslant i \leqslant t,$$
$$b_{i+1}a_i - a_{i+1}b_i = (-1)^i s \text{ для } 0 \leqslant i < t.$$

Прежде чем мы докажем корректность алгоритма, рассмотрим лемму.

(1.6) **Лемма.** *Пусть a_i, b_i, t такие же, как выше, и пусть x, $y \in \mathbf{R}_{\geqslant 0}$, $\gamma \in \mathbf{R}_{>0}$. Тогда существует $i \in \{0, 1, \ldots, t\}$, такое,*

что

$$-\gamma s < xa_i + yb_i < \gamma s, \text{ если } i \text{ четно},$$
$$2\gamma a_i b_i \leqslant xa_i + yb_i \leqslant \gamma^{-1}xy + \gamma a_i b_i, \text{ если } i \text{ нечетно}.$$

Доказательство. Сначала рассмотрим числа $xa_i + yb_i$ для *четных* значений i. Из $b_0 = 0$, $a_t = 0$ следует, что

$$xa_0 + yb_0 \geqslant 0, \quad xa_t + yb_t \leqslant 0.$$

Поэтому найдется четный индекс i, такой, что

$$xa_i + yb_i \geqslant 0, \quad xa_{i+2} + yb_{i+2} \leqslant 0.$$

Если одно из этих чисел по абсолютной величине меньше γs, то все доказано. Допустим поэтому, что первое $\geqslant \gamma s$ и второе $\leqslant -\gamma s$. Тогда

$$(xa_i + yb_i)/\gamma \geqslant s = b_{i+1}a_i - a_{i+1}b_i \geqslant b_{i+1}a_i,$$

так что $x \geqslant \gamma b_{i+1}$, и

$$(xa_{i+2} + yb_{i+2})/\gamma \leqslant -s = b_{i+2}a_{i+1} - a_{i+2}b_{i+1} \leqslant b_{i+2}a_{i+1},$$

так что $y \geqslant \gamma a_{i+1}$. Следовательно, имеем

$$xa_{i+1} + yb_{i+1} \geqslant 2\gamma a_{i+1}b_{i+1},$$

и из $(x - \gamma b_{i+1})(y - \gamma a_{i+1}) \geqslant 0$ следует, что

$$xa_{i+1} + yb_{i+1} \leqslant \gamma^{-1}xy + \gamma a_{i+1}b_{i+1}.$$

Поскольку $i + 1$ нечетно, это завершает доказательство леммы.

(1.7) **Предложение.** *При заданных r, s и n, таких, как в теореме, алгоритм* (1.2) *правильно определяет все положительные делители числа n, сравнимые с r по модулю s. Число битовых операций, необходимых алгоритму, равно $O((\log n)^3)$ и равно $O((\log n)^{2+\varepsilon})$ для любого $\varepsilon > 0$, если используются методы быстрого умножения.*

Доказательство. Сначала мы докажем корректность алгоритма. Пусть $xs + r$ есть положительный делитель n, сравнимый с r по модулю s. Тогда $x \in \mathbb{Z}_{\geqslant 0}$ и $(xs + r)d = n$ для некоторого $d \in \mathbb{Z}_{>0}$. Умножая на r^*, мы видим, что $d \equiv r^*n \equiv r' \bmod s$, поэтому можем записать $d = ys + r'$ с $y \in \mathbb{Z}_{\geqslant 0}$. Рассматривая $(xs + r)(ys + r') = n$ по модулю s^2,

$$xr' + yr \equiv (n - rr')/s \bmod s;$$

заметим, что правая часть есть целое число. Умножая на r^* находим, что

$$xr'r^* + y \equiv \frac{n - rr'}{s} r^* \bmod s.$$

Это в точности случай $r=1$ в последовательности сравнений

(1.8) $\quad xa_i + yb_i \equiv c_i \bmod s \quad (0 \leqslant i \leqslant t).$

Для $i=0$ это сравнение выполняется тривиально, а для $i \geqslant 2$ оно получается с помощью тривиальных индуктивных рассуждений из определения a_i, b_i, c_i.

Применяя лемму (1.6) с $\gamma=1$, находим, что существует $i \in \{0, 1, \ldots, t\}$, такое, что

$$|xa_i + yb_i| < s, \text{ если } i \text{ четно},$$

$$2a_ib_i \leqslant xa_i + yb_i \leqslant xy + a_ib_i, \text{ если } i \text{ нечетно}.$$

Фиксируем такое значение i и положим $c = xa_i + yb_i$. Из (1.8), только что доказанного неравенства и неравенства

$$xy \leqslant (xs+r)(ys+r')/s^2 = ns^2$$

следует тогда, что c удовлетворяет (1.3). Поскольку x, y удовлетворяют (1.4), отсюда следует, что делитель $xs+r$ в самом деле обнаруживается алгоритмом. Это доказывает корректность.

Далее мы оцениваем число битовых операций. Число r^* может быть найдено за $O((\log n)^2)$ битовых операций (см. [5, упр. 4.5.2.30]). Из $n/s^2 < s$ и $a_ib_i > 0$ для нечетных i следует, что для каждого $i \in \{0, 1, \ldots, t\}$ найдется не более двух значений c, удовлетворяющих (1.3). Следовательно, для каждого i алгоритм делает лишь ограниченное число сложений, вычитаний, умножений, делений и извлечений квадратного корня. Эти операции выполняются с целыми числами, двоичная длина которых равна $O(\log n)$; поэтому каждая из них может быть сделана за $O((\log n)^2)$ битовых операций или за $O((\log n)^{1+\varepsilon})$ с помощью техники быстрого умножения (см. [1]). Поскольку число значений для i равно $t+1 = O(\log n)$, это доказывает предложение.

(1.9) **Замечания.** (a) Доказательство показывает, что алгоритм также полиномиален, если $s/n^{1/3}$ ограничено снизу.

(b) Мы применяли лемму (1.6) только с $\gamma=1$. Может оказаться, что иной выбор γ приводит на практике к более быстрому алгоритму.

(c) Если s много больше, чем $n^{1/3}$, то число квадратных уравнений, которые следует решить, может быть сильно сокращено. Например, если $s > n^{1/2}$, то $xy \leqslant n/s^2 < 1$, так что нам нужно лишь рассмотреть случаи $x=0$ и $y=0$. Если $s > n^{2/5}$, можно использовать тот факт, что $a_i^2 + b_i^2 \leqslant (4/3)^{1/2}s$ для некоторого i (см. [5, упр. 3.3.4.5; 9]); для этого значения i число $xa_i + yb_i$ лежит в интервале длины, не превосходящей некото-

рой постоянной, умноженной на s, кроме случая $xy=0$, поэтому лишь ограниченное число квадратных уравнений должно быть решено. Более общо, если $s>n^{\alpha}$ с $\alpha>1/3$, то алгоритм может быть модифицирован таким образом, что число квадратных уравнений, которые должны быть решены, будет ограничено постоянной, зависящей лишь от α. Это наблюдение сделано Х. Зантемой.

2. КОМБИНАТОРНАЯ МОДЕЛЬ

Мы обозначаем через — и $\triangle$ теоретико-множественную разность и симметрическую разность соответственно: $X\triangle Y=(X-Y)\cup(Y-X)$. Мощность множества X обозначается $\#X$.

Весовая функция на конечном множестве V есть функция w, сопоставляющая неотрицательное вещественное число каждому подмножеству множества V таким образом, что $w(X\cup Y)=w(X)+w(Y)$ для любых двух непересекающихся подмножеств X, Y в V.

(2.1) **Предложение.** *Пусть V — конечное множество, w — весовая функция на V, $w(V)>0$ и $\alpha\in\mathbb{R}$, $\alpha>1/4$. Пусть далее $\mathcal{D}$ — система подмножеств множества V, такая, что*

$$\max\{w(D-D'),\ w(D'-D)\}\geqslant\alpha w(V)$$

для всех D, $D'\in\mathcal{D}$, $D\neq D'$. Тогда $\#\mathcal{D}\leqslant c(\alpha)$, где $c(\alpha)$ — постоянная, зависящая только от α.

(2.2) *Замечание.* Утверждение (2.1) не выполняется для $\alpha\leqslant 1/4$. Чтобы увидеть это, возьмем в качестве V векторное пространство над двухэлементиым полем $\mathbb{F}_2$ и обозначим через $\mathcal{D}$ множество гиперплоскостей в V. Положим $w(X)=\#X$ для $X\subset V$. Тогда $w(D-D')={}^1/_4\#V\geqslant\alpha w(V)$ для любых двух D, $D'\in\mathcal{D}$, $D\neq D'$, но $\#\mathcal{D}=\#V$ стремится к бесконечности с ростом размерности векторного пространства.

Доказательство (2.1). Зафиксируем ε, $0<\varepsilon<2\alpha-1/2$ и положим $\eta=4\alpha-1-2\varepsilon$, так что $\eta>0$. Запишем

$$\mathcal{D}_{\beta}=\{D\in\mathcal{D}:\ \beta w(V)\leqslant w(\mathcal{D})<(\beta+\varepsilon)w(V)\}$$

для $\beta\in\mathbb{R}$, $0\leqslant\beta\leqslant 1$. Ниже мы докажем, что

(2.3) $$\#\mathcal{D}_{\beta}\leqslant 1+\eta^{-1}$$

для всех β. Поскольку

$$\mathcal{D}=\bigcup_{i=0}^{[1/\varepsilon]}\mathcal{D}_{i\varepsilon},$$

то

$$\#\mathscr{D} \leqslant ([1/\varepsilon]+1)(1+\eta^{-1}),$$

что и требовалось доказать.

Далее доказываем (2.3). Пусть $D, D' \in \mathscr{D}_\beta$, $D \neq D'$. Тогда разность между $w(D)$ и $w(D')$ не превосходит по модулю $\varepsilon w(V)$. Вычитая $w(D \cap D')$, мы видим, что разность между $w(D-D')$ и $w(D'-D)$ также не превосходит $\varepsilon w(V)$. Кроме того, наибольшее из $w(D-D')$, $w(D'-D)$ не меньше, чем $\alpha w(V)$ по предположению. Следовательно, наименьшее из этих чисел не меньше, чем $(\alpha-\varepsilon)w(V)$, и

$$w(D \triangle D') = w(D-D') + w(D'-D) \geqslant$$
$$\geqslant (2\alpha-\varepsilon)w(V) = {}^1/_2(1+\eta)w(V).$$

Обозначим $\mathscr{D}_\beta = \{D_1, \ldots, D_m\}$, $m = \#\mathscr{D}_\beta$. Из только что доказанного неравенства следует, что

$$\sum_{1\leqslant i<j\leqslant m} w(D_i \triangle D_j) \geqslant \frac{1}{2}\binom{m}{2}(1+\eta)w(V).$$

С другой стороны, имеем

$$\sum_{1\leqslant i<j\leqslant m} w(D_i \triangle D_j) =$$
$$= \sum_{x\in V} \#\{(i, j)\colon 1\leqslant i<j\leqslant m,\ x\in D_i \triangle D_j\}\, w(\{x\}) =$$
$$= \sum_{x\in V} \#\{(i, j)\colon 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant m,\ x\in D_i,\ x\notin D_j\}\, w(\{x\}) =$$
$$= \sum_{x\in V} m_x(m-m_x)\, w(\{x\}),$$

где $m_x = \#\{i\colon 1\leqslant i\leqslant m,\ x\in D_i\}$. Из $m_x(m-m_x)\leqslant {}^1/_4 m^2$ мы видим теперь, что

$$\sum_{1\leqslant i<j\leqslant m} w(D_i \triangle D_j) \leqslant \frac{1}{4}m^2 \sum_{x\in V} w(\{x\}) = \frac{1}{4}m^2 w(V).$$

В сочетании с прежним неравенством это дает

$$\frac{1}{2}\binom{m}{2}(1+\eta)w(V) \leqslant \frac{1}{4}m^2 w(V),$$
$$(m-1)(1+\eta)\leqslant m,\ m\leqslant 1+\eta^{-1},$$

что и требовалось. Это доказывает (2.3) и (2.1).

Замечание. Отметим сходство приведенного выше предложения с границей Плоткина в теории кодирования (см. [8, гл. 2, разд. 2]).

(2.4) **Предложение.** Пусть V, w, $\mathcal{D}$, α удовлетворяют всем условиям предложения (2.1), и предположим далее, что $\alpha > 1/3$. Тогда $\#\mathcal{D} \leqslant 11$.

(2.5) *Замечание.* Это предложение наилучшее возможное в том смысле, что для $\alpha \leqslant 1/3$ должно выполняться неравенство $\#\mathcal{D} \geqslant 12$. Чтобы увидеть это, положим $\#V = 6$ и возьмем в качестве $\mathcal{D}$ систему подмножеств, характеристические функции которых заданы в столбцах следующей матрицы:

$$\begin{matrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{matrix}.$$

В этом примере мы полагаем $w(X) = \#X$ для всех $X \subset V$. Прежде чем доказывать (2.4), рассмотрим две леммы.

(2.6) **Лемма.** *Пусть* $V_1, V_2 \ldots, V_l \subset V$ *и* $t \in \mathbf{Z}$. *Тогда*

$$\frac{1}{2} t(t+1) w\left(\bigcup_{i=1}^{l} V_i\right) + \sum_{1 \leqslant i < j \leqslant l} w(V_i \cap V_j) \geqslant t \sum_{i=1}^{l} w(V_i).$$

Доказательство. Для каждого $y \in \mathbf{Z}$ мы, очевидно, имеем $^1/_2(y-t)(y-(t+1)) \geqslant 0$, что эквивалентно

$$\frac{1}{2} t(t+1) + \frac{1}{2} y(y-1) \geqslant ty.$$

Применим это к

$$y = n_x = \#\{i\colon\ 1 \leqslant i \leqslant l,\ x \in V_i\}$$

для $x \in \bigcup_{i=1}^{l} V_i$. Умножая получившееся неравенство на $w(\{x\})$ и суммируя по $x \in \bigcup_{i=1}^{l} V_i$, получаем в точности требуемое неравенство. Это доказывает (2.6).

(2.7) **Лемма.** *Пусть предположения такие же, как в* (2.1), *и пусть* $V_1, V_2, \ldots, V_l \in \mathcal{D}$ *удовлетворяют неравенствам*

$$w(V_1) \leqslant w(V_2) \leqslant \ldots \leqslant w(V_l),\ V_i \neq V_j \quad (1 \leqslant i < j \leqslant l).$$

Тогда числа $y_i = w(V_i)/w(V)$ *удовлетворяют для каждого* $t \in \mathbf{Z}$ *неравенству*

$$-ty_1 + (-t+1)y_2 + \ldots + (-t+l-1)y_l + \\ + \frac{1}{2} t(t+1) \geqslant \frac{1}{2} l(l-1)\alpha.$$

Доказательство. Это непосредственно следует из предыдущей леммы, если воспользоваться тем, что

$$w\left(\bigcup_{i=1}^{l} V_i\right) \leqslant w(V),$$

$$w(V_i \cap V_j) \leqslant w(V_j) - \alpha w(V), \quad 1 \leqslant i < j \leqslant l;$$

последнее неравенство следует из условий на $\mathscr{D}$ в (2.1). Это доказывает (2.7).

Доказательство (2.4). Предположим, что $\#\mathscr{D} \geqslant 12$, и выберем $D_1, D_2, \ldots, D_{12} \in \mathscr{D}$, такие, что

$$w(D_1) \leqslant w(D_2) \leqslant \ldots \leqslant w(D_{12}), \quad D_i \neq D_j (1 \leqslant i < j \leqslant 12).$$

Обозначим $x_i = w(D_i)/w(V)$. Применяя (2.7) к $\{V_1, V_2\} = \{D_1, D_2\}$, $t=0$ и к $\{V_1, V_2\} = \{D_{11}, D_{12}\}$, $t=1$, находим, что $x_2 \geqslant \alpha$, $x_{11} \leqslant 1-\alpha$. При $\{V_1, \ldots, V_l\} = \{D_2, D_3, D_4, D_5, D_6, D_7\}$, $t=2$ мы получаем

$$-2x_2 - x_3 + x_5 + 2x_6 + 3x_7 + 3 \geqslant 15\alpha,$$

а $\{V_1, \ldots, V_l\} = \{D_6, D_7, D_8, D_9, D_{10}, D_{11}\}$, $t=3$ приводит к

$$-3x_6 - 2x_7 - x_8 + x_{10} + 2x_{11} + 6 \geqslant 15\alpha.$$

Складывая последние два неравенства и пользуясь тем, что $x_3 \geqslant x_2 \geqslant \alpha$, $x_{10} \leqslant x_{11} \leqslant 1-\alpha$, находим, что

$$-3\alpha + x_5 - x_6 + x_7 - x_8 + 3(1-\alpha) + 9 \geqslant 30\alpha.$$

Поскольку $x_5 \leqslant x_6$ и $x_7 \leqslant x_8$, это дает $12 \geqslant 36\alpha$, что противоречит условию. Это доказывает (2.4).

(2.8) Для целого числа $k \geqslant 2$ обозначим через $\alpha(k)$ наибольшее значение α, для которого могут выполняться условия (2.1) с $\#\mathscr{D} = k$. Нетрудно видеть, что $\alpha(k)$ существует и что для заданного k оно может быть вычислено путем решения задачи линейного программирования с $2^k + 1$ переменными.

Из (2.4) и (2.5) мы видим, что $\alpha(12) = 1/3$. В табл. 1 даны значения $\alpha(k)$ для $2 \leqslant k \leqslant 12$. Эта таблица была получена следующим образом. Тот факт, что табулированные значения являются верхними границами для $\alpha(k)$, был получен с помощью методов линейного программирования; мы признательны Б. Лагевегу за оказанную при этом помощь. Во всех случаях, кроме $k=9$, неравенства из (2.7) оказались достаточны для получения этих верхних границ. Тот факт, что табулированные значения являются нижними границами для $\alpha(k)$, был затем доказан Х. Зантемой, который привел примеры, подобные (2.5).

Если $\alpha > \alpha(k)$, то в (2.1) мы можем взять $c(\alpha) = k-1$. Из (2.1) и (2.2) следует, что $\alpha(k)$ стремится к 1/4 при k, стре-

Таблица 1

k	$\alpha(k)$	k	$\alpha(k)$
2	$1 = 1.000000$	8	$4/11 = 0.363636$
3	$1/2 = 0.500000$	9	$13/37 = 0.351351$
4	$1/2 = 0.500000$	10	$9/26 = 0.346154$
5	$2/5 = 0.400000$	11	$31/92 = 0.336957$
6	$2/5 = 0.400000$	12	$1/3 = 0.333333$
7	$3/8 = 0.375000$		

мящемся к бесконечности. Доказательство (2.1) показывает, что мы можем взять $c(\alpha) = O((\alpha - 1/4)^{-2})$ для $1/4 < \alpha \leqslant 1$; поэтому $\alpha(k) = 1/4 + O(k^{-1/2})$, однако мне не известно, такова ли в действительности скорость сходимости.

3. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ

Для положительного целого числа k мы обозначаем

$$V(k) = \{p^t\colon\ p \text{ простое},\ t \in \mathbb{Z},\ t \geqslant 1,\ p^t \text{ делит } k\},$$

например, $V(12) = \{2, 4, 3\}$. Определим весовую функцию w на каждом $V(k)$, полагая $w(\{p^t\}) = \log p$. Простые вычисления показывают что $w(V(k)) = \log k$.

Доказательство теоремы. Поскольку последнее утверждение теоремы было доказано в разд. 1, достаточно доказать первое утверждение.

Мы применяем (2.4) к $V = V(n)$ с тем же w, что и ранее. Имеем $w(V) > 0$ при $n > 1$, что, очевидно, можно допустить. Пусть

$$\mathscr{D} = \{V(d)\colon\ d \text{ делит } n,\ d > 0,\ d \equiv r \bmod s\}.$$

Пусть d, d' — два различных положительных делителя числа n, сравнимых с r по модулю s. Поскольку s делит $d - d'$ и взаимно просто с d, наибольший общий делитель чисел d и d' делит $(d - d')/s$. Следовательно,

$$\text{НОД}(d, d') \leqslant \frac{|d - d'|}{s} < \frac{\max\{d, d'\}}{n^{1/3}},$$

так что

$$\frac{1}{3}\log n < \max\{\log(d/\text{НОД}(d, d')),\ \log(d'/\text{НОД}(d, d'))\}.$$

Поскольку $V(\text{НОД}(d, d')) = V(d) \cap V(d')$, это приводит к

$$^1/_3 w(V) < \max\{w(V(d) - V(d')),\ w(V(d') - V(d))\}.$$

Следовательно, мы можем выбрать $\alpha > 1/3$, так что правая часть $\geqslant \alpha w(V)$ для всех пар d, d'. Тогда все условия (2.4) выполнены, и поэтому $\#\mathcal{D} \leqslant 11$. Это завершает доказательство теоремы.

(3.1) **Предложение.** *Для любого $\alpha \in \mathbb{R}$, $\alpha > 1/4$, существует постоянная $c(\alpha)$ со следующим свойством. Если r, s, n — целые числа, удовлетворяющие условиям $n > 0$, $s > n^{\alpha}$, НОД$(r, s) = 1$, то число положительных делителей n, сравнимых с r по модулю s, не превосходит $c(\alpha)$.*

Доказательство аналогично только что приведенному с заменой (2.4) на (2.1). Это доказывает (3.1).

Если $\alpha \geqslant \alpha(k)$, $\alpha(k)$ такое же, как в (2.8), то мы можем взять $c(\alpha) = k - 1$ в предложении (3.1). Мне не известно, можно ли условие $\alpha > 1/4$ в (3.1) заменить на $\alpha > 0$.

Число 11 в теореме не может быть заменено на 5. На самом деле Коэн доказал, что существует бесконечно много положительных целых чисел n, которые имеют не менее шести положительных делителей в одном и том же взаимно простом классе вычетов по модулю некоторого вспомогательного числа $s > n^{1/3}$. Первые десять значений n выписаны в табл. 2 вместе

Таблица 2

n	s	r	n	s	r
245 784	65	1, 19	1 755 600	131	2, 100
288 288	71	1, 28	1 796 760	137	3, 93
320 320	69	1, 22	2 066 400	143	2, 25
480 480	83	5, 65	2 511 600	149	7, 8
911 064	115	1, 34	2 841 696	175	2, 23

с классами вычетов $r \bmod s$, которые содержат шесть делителей n. Таблица была составлена Ленстрой с помощью компьютера VAX 11-780 в Математическом центре в Амстердаме. Другие примеры с $n < 3 \cdot 10^6$ неизвестны, и не было обнаружено ни одного примера с семью делителями в одном и том же классе вычетов.

ЛИТЕРАТУРА

[1] Alt H. Square rooting is as difficult as multiplication. — Computing, 1979, v. 21, p. 221—232.

[2] Brillhart J., Lehmer D. H., Selfridge J. L. New primality criteria and factorizations of $2^m \pm 1$. — Math. Comp., 1975, v. 29, p. 620—647; p. 112—139. — In: Selected Papers of D. H. Lehmer, vol. 1, Charles Babbage Research Centre, St. Pierre, Manitoba, 1981.

[3] Cohen H., Lenstra H., Jr. Primality testing and Jacobi sums. — Math. Comp., 1984, v. 42, p. 297—330. [Имеется перевод в настоящем сборнике, с. 101—146.]
[4] Hardy G. H., Wright E. M. An Introduction to the Theory of Numbers, 5th ed. — Oxford: Oxford University Press, 1979.
[5] Knuth D. E The Art of Computer Programming. Vol. 2. Seminumerical Algorithms 2nd ed. — Reading Mass., Addison-Wesley, 1981. [Имеется перевод 1-го изд.: Кнут Д. Искусство программирования для ЭВМ. Т. 2.— М.: Мир, 1977.]
[6] Lehman R. S. Factoring large integers. — Math. Comp., 1974, v. 28, p. 637—646.
[7] Lenstra H. W., Jr., Tijdeman R. (eds.) Computational Methods in Number Theory. — Amsterdam: Mathematical Centre Tracts 154/155, 1982.
[8] MacWilliams F. J., Sloane N. J. A. The Theory of Error-Correcting Codes. — Amsterdam: North-Holland, 1978.
[9] Pinter R. Y. Using Hyperbolic Tangents in Integer Factoring. — Thesis, M. I. T., Cambridge, Mass., 1980.

Сильно регулярные графы [1]

К. Юбо [2]

В этой статье мы попытались собрать известные результаты о сильно регулярных графах. В статью включены как теоретико-групповые, так и комбинаторные аспекты обсуждаемой теории. Мы приводим список всех известных ко времени написания статьи сильно регулярных графов, а также обширную библиографию по рассматриваемому предмету.

0. ВВЕДЕНИЕ

Теорию сильно регулярных графов (с. р. графов) начал развивать Боуз [7] в 1963 г. в связи с частичными геометриями и схемами отношений с двумя классами. Годом позже Хигман [34] начал изучать группы подстановок ранга 3 с использованием сильно регулярных графов. В последние годы развивались как комбинаторный, так и теоретико-групповой аспекты теории сильно регулярных графов. Кроме того, интерес к сильно регулярным графам стимулировался открытием новых простых групп. В этой статье мы попытались собрать основные результаты по этой тематике, а также включить ряд новых результатов. Мы также приводим обширную библиографию по с. р. графам.

На протяжении всей статьи мы используем обозначения, введенные Сейделом [65] при изучении равноугольных прямых (см. ван Линт и Сейдел [80]). Эти обозначения очень удобны для обсуждения понятий дополнения и дополнительного графа. В первом разделе мы укажем связь наших обозначений с обозначениями, введенными Боузом и Хигманом в связи с изучением схем отношений с n-классами и централизаторных колец.

В качестве приложения мы приводим таблицу всех известных нам с. р. графов, связанных с классическими группами, спорадическими группами, а также возникающих из различных комбинаторных конструкций.

---

[1]) Hubaut Xavier L. Strongly regular graphs. — Discrete Mathematics, 1975, v. 13, p. 357—381.

[2]) Free University of Brussels, Brussels, Belgium. Частичная финансовая поддержка этому исследованию оказана ONR Contract N00014-67-A-0232-0016 (OSURF-3430A1).

Автор глубоко признателен Д. Рао-Чаудхури за плодотворные обсуждения, а также В. Кантору, Д. Пэрроту и И. Сейделу за полезную информацию.

1. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

Все рассматриваемые здесь графы неориентированы, без петель и кратных ребер.

Пусть $\mathcal{G}$ — такой граф и v — число его вершин. Граф $\mathcal{G}$ называется *регулярным*, если каждая его вершина смежна с одним и тем же числом k вершин. При этом k называется *валентностью* графа $\mathcal{G}$. Граф $\mathcal{G}$ называется *сильным*, если

(i) для любых двух заданных смежных вершин x, y сумма числа вершин, смежных как с x, так и с y, и числа вершин, не смежных ни с x, ни с y, постоянна;

(ii) для любых двух заданных несмежных вершин эта сумма также постоянна.

Граф $\mathcal{G}$ является *сильно регулярным*, если он одновременно сильный и регулярный. Это означает, что

(i) число вершин, смежных с обоими концами ребра, постоянно и равно, скажем, λ;

(ii) число вершин, смежных с двумя несмежными вершинами, постоянно и равно, скажем, μ.

Через $\Delta(p)$ (соответственно $\Gamma(p)$) будем обозначать множество вершин, смежных (соответственно несмежных) с вершиной p.

Пусть $\overline{\mathcal{G}}$ — граф, дополнительный к $\mathcal{G}$. Множество вершин графа $\overline{\mathcal{G}}$ то же, что и у графа $\mathcal{G}$; две вершины в $\overline{\mathcal{G}}$ смежны, если и только если они несмежны в графе $\mathcal{G}$. Если $\mathcal{G}$ регулярен, то $\overline{\mathcal{G}}$ также регулярен и его валентность равна $l = v - k - 1$. Более того, если $\mathcal{G}$ сильный, то $\overline{\mathcal{G}}$ также сильный.

Пусть $\mathcal{H}_1 \cup \mathcal{H}_2$ — разбиение графа $\mathcal{G}$. Граф $\mathcal{G}'$, получаемый посредством *переключения* относительно $\{\mathcal{H}_1, \mathcal{H}_2\}$, — это граф, множество вершин которого то же, что у графа $\mathcal{G}$, причем внутри $\mathcal{H}_1$ и $\mathcal{H}_2$ все ребра те же, что в $\mathcal{G}$; вершина из $\mathcal{H}_1$ смежна с вершиной из $\mathcal{H}_2$, если и только если эти вершины в графе $\mathcal{G}$ несмежны.

С каждым графом мы будем связывать его *матрицу смежности* A. Пусть вершины графа $\mathcal{G}$ занумерованы числами $1, 2, \ldots, v$. Тогда A — матрица размера $v \times v$ и ее элементы определяются следующим образом:

$$a_{ij} = \alpha, \text{ если } i = j,$$

$$a_{ij} = \beta, \text{ если } i \text{ и } j \text{ смежны},$$

$$a_{ij} = \gamma, \text{ если } i \text{ и } j \text{ несмежны}.$$

1/36 Зак. 469

Если $\mathcal{G}$ — сильно регулярный граф, то, как легко показать, матричная алгебра, порожденная матрицами A, I, J (матрица, целиком состоящая из единиц), имеет размерность 3. Прямые вычисления показывают, что

$$A^2 = [2(\alpha-\gamma)+(\lambda-\mu)(\beta-\gamma)]A +$$
$$+ [k(\beta-\gamma)^2+\lambda(\gamma-\alpha)(\beta-\gamma)+\mu(\alpha-\beta)(\beta-\gamma)-(\alpha-\gamma)^2]I +$$
$$+ [k\gamma(2\beta-\gamma)+l\gamma^2-\lambda\gamma(\beta-\gamma)+\mu\beta(\beta-\lambda)+\gamma^2]J;$$
$$AJ = (\alpha+k\beta+l\gamma)J.$$

В частности, если $\alpha=0$, $\beta=-1$, $\gamma=1$, то это $(0,-1,1)$-матрица смежности графа $\mathcal{G}$, удовлетворяющая соотношениям

$$A^2+2(\lambda-\mu+1)A-(4k-2\lambda-2\mu-1)I = \\ = (v-4k+2\lambda+2\mu)J,$$
$$AJ=(l-k)J.$$

Собственные значения матрицы A — числа $\rho_0 = l-k$ и ρ_1, ρ_2, причем последние являются корнями квадратного уравнения

$$x^2+2(\lambda-\mu+1)x-(4k-2\lambda-2\mu-1)=0 \quad (\rho_1>0>\rho_2).$$

Кратности m_1, m_2 собственных значений ρ_1, ρ_2 равны соответственно

$$[-\rho_0-\rho_2(v-1)](\rho_1-\rho_2)^{-1}, \quad [\rho_0+\rho_1(v-1)](\rho_1-\rho_2)^{-1}.$$

Анализируя эти кратности, можно вывести условия, необходимые для существования сильно регулярного графа, которые состоят в том, что либо

(I) $k=l$, $\mu=\lambda+1={}^1/_2k$,

либо

(II) $d=(\lambda-\mu)^2+4(k-\mu)$ является квадратом и $\sqrt{d}$ делит $2k+(\lambda-\mu)(v-1)$. Более того, $2\sqrt{d}$ не делит указанную величину, если v четно, и делит, если v нечетно.

Во втором случае собственные значения ρ_1, ρ_2 являются нечетными целыми числами. В первом же случае $\rho_0=0$, $\rho_1=-\rho_2=\sqrt{v}$ и известно, что необходимым условием существования таких графов является то, что $v=a^2+b^2$, где a и b — целые числа различной четности. Графы этого типа были построены для всех значений $v=p^\alpha$, где p простое, и для некоторых других значений v.

Отметим, что $(0,-1,1)$-матрица смежности A сильного графа удовлетворяет соотношению

$$(A-\rho_1 I)(A-\rho_2 I)=(v-1+\rho_1\rho_2)J.$$

Если $v-1+\rho_1\rho_2 \neq 0$, то, как показал Сейдел [65], такой граф является сильно регулярным.

Переключение по отношению к $\{\mathscr{H}_1, \mathscr{H}_2\}$ преобразует матрицу A в матрицу A' следующим образом:

$$a'_{ij}=a_{ij}, \text{ если } i \text{ и } j \text{ содержатся в } \mathscr{H}_1 \text{ или } \mathscr{H}_2,$$

$$a'_{ij}=-a_{ij}, \text{ если } i \text{ и } j \text{ содержатся в различных } \mathscr{H}_k.$$

Матрица смежности $\bar{A}$ дополнительного графа $\bar{\mathscr{G}}$ графа $\mathscr{G}$ равна $(-A)$, и справедливы следующие соотношения:

$$\bar{v}=v, \quad \bar{k}=l, \quad \bar{l}=k, \quad \bar{\lambda}=l-k+\mu-1, \quad \bar{\mu}=l-k+\lambda+1,$$

$$\rho_0+\bar{\rho}_0=\rho_1+\bar{\rho}_2=\rho_2+\bar{\rho}_1=0.$$

Другие используемые обозначения

(A) Хигман [34] рассматривает (0, 1)-матрицу смежности графа, определяемую тем, что $\alpha=0$, $\beta=1$, $\gamma=0$. Эта матрица удовлетворяет уравнениям

$$A^2-(\lambda-\mu)A-(k-\mu)I=\mu J \quad \text{и} \quad AJ=kJ.$$

Ее собственные числа s и t связаны с ρ_1 и ρ_2 равенствами $\rho_1=-(2s+1)$, $\rho_2=-(2t+1)$.

(B) По терминологии схем отношений с двумя классами (см. [7]) две вершины находятся в первом (соответственно во втором) отношении, если они смежны (соответственно несмежны). Соответствие между обозначениями следующее: $k=n_1$, $l=n_2$, $\lambda=p^1_{11}$, $\mu=p^2_{11}$.

2. ЧАСТИЧНЫЕ ГЕОМЕТРИИ

Частичная геометрия — это множество элементов, называемых точками, и набор его подмножеств, называемых прямыми, такой, что

(i) каждая пара точек лежит не более чем на одной прямой,

(ii) каждая прямая содержит K точек, $K \geqslant 2$,

(iii) каждая точка лежит на R прямых, $R \geqslant 2$,

(iv) для любой заданной неинцидентной пары точка — прямая (p, L) имеется ровно T прямых, проходящих через p, которые содержат точки, инцидентные L, $K \geqslant T \geqslant 1$.

По каждой частичной геометрии может быть построен некоторый сильно регулярный граф $\mathscr{G}$. При этом вершины графа $\mathscr{G}$ — это точки рассматриваемой геометрии; две вершины смежны тогда и только тогда, когда соответствующие точки лежат на одной прямой. Другими словами, $\mathscr{G}$ — точечный граф рассматриваемой геометрии. Параметры графа $\mathscr{G}$ могут быть вы-

числены, исходя из параметров (R, K, T) частичной геометрии. Имеют место равенства

$$v = KT^{-1}[(R-1)(K-1)+T],$$
$$k = R(K-1),$$
$$l = (K-1)(R-1)(K-T)T^{-1},$$
$$\lambda = K-2+(R-1)(T-1),$$
$$\mu = RT.$$

Очевидно, все эти числа целые, поэтому T делит $K(K-1)(R-1)$. Более того, поскольку граф $\mathcal{G}$ сильно регулярный, из необходимых условий существования с. р. графа следует, что $T(R+K-T-1)$ делит $RK(K-1)(R-1)$.

Граф $\mathcal{G}$, обладающий таким набором параметров (v, k, l, λ, μ), что для некоторых целых чисел (R, K, T) выполнены приведенные выше соотношения, называется *псевдогеометрическим*. Такой граф называется *геометрическим*, если существует соответствующая частичная геометрия.

Псевдогеометрические графы не всегда возникают из частичных геометрий. Например, существует граф с параметрами $v=16$, $k=6$, $\lambda=2$, что соответствует набору $R=2$, $K=4$, $T=1$, причем этот граф не изоморфен точечному графу единственной частичной геометрии с параметрами $(2, 4, 1)$.

Теорема Боуза [7] содержит достаточное условие того, что псевдогеометрический граф геометрический: в $\mathcal{G}$ существует множество Σ клик (полных подграфов), такое, что (1) две смежные вершины содержатся в единственной клике из Σ; (2) каждая вершина принадлежит ровно R кликам из Σ; (3) число K, равное мощности каждой клики из Σ, больше чем R. Другой результат Боуза состоит в том, что псевдогеометрический граф $\mathcal{G}$ является геометрическим в случае, когда

$$K > {}^1/_2[R(R-1)+T(R+1)(R^2-2R+2)].$$

Для заданной частичной геометрии с параметрами (R, K, T) двойственная геометрия, т. е. геометрия, у которой точками являются прямые, а прямыми — точки исходной геометрии, также является частичной геометрией с параметрами (K, R, T). Такие частичные геометрии исследовались Боузом [7], Симсом [73], Хигманом [41], а также Аренсом и Секересом [1].

3. t-СХЕМЫ И СИММЕТРИЧЕСКИЕ 2-СХЕМЫ

t-схема $S_\lambda(t, k, v)$ — это множество из v *точек* и набор k-элементных подмножеств множества точек, называемых *блоками*, такой, что любые t различных точек содержатся ровно в λ блоках. При этом число b блоков задается равенством $b = \lambda\binom{v}{t}/\binom{k}{t}$.

Если $t=2$, то может оказаться, что число блоков равно числу точек. В этом случае $\lambda(v-1)=k(k-1)$. Простейшими примерами являются проективные пространства, при этом блоки суть гиперплоскости. Заметим, что в симметрической 2-схеме два блока имеют λ общих точек и для каждой точки имеется k блоков, ее содержащих.

В некоторых частных случаях симметрическую схему удается построить, исходя из сильно регулярного графа.

(A) Если $\lambda=\mu$, то выберем в качестве блоков множества $\Delta(p)$ для всех вершин p графа $\mathcal{G}$. Это приводит к симметрической схеме $S_\lambda(2, k, v)$.

(B) Если $\lambda=\mu-2$, то, взяв в качестве блоков множества $\{p\}\cup\Delta(p)$ для всех вершин p графа $\mathcal{G}$, мы получим симметрическую схему $S_\mu(2, k+1, v)$.

Заметим, что если $\lambda=\mu-2$, то в дополнительном графе $\overline{\mathcal{G}}$ выполнено равенство $\bar{\lambda}=\bar{\mu}$ и симметрическая схема является дополнительной к схеме, получаемой, исходя из дополнительного графа.

В случае (A), т. е. когда $\lambda=\mu$, необходимые условия существования сильно регулярного графа сводятся к тому, что $4(k-\lambda)=d$ является квадратом и $\sqrt{d}$ делит $2k$. Отсюда $k-\lambda=m^2$ и m делит k. Это означает, что m делит λ. Следовательно, для заданного λ существует лишь конечное число сильно регулярных графов, таких, что $\lambda=\mu$.

Такие графы, которые иногда называют (v, k, λ)-графами, изучались в работах [10, 62, 83]. Рудвалис [62] доказал, что существование (v, k, λ)-графа эквивалентно существованию симметрической схемы $S_\lambda(2, k, v)$, допускающей полярность без абсолютных точек. Необходимым (но не достаточным) условием существования таких графов (или схем) является то, что

$$(v,\ k,\ \lambda)=(s\,[(s+a)^2-1]/a,\ s(s+a),\ sa),$$

где a делит $s(s^2-1)$, причем, если a четно, то s и $s(s^2-1)/a$ должны быть нечетными целыми.

Отмеченная связь между (v, k, λ)-графами и некоторыми симметрическими схемами изучалась в работах Холла и др. [30] и Юбо [49].

4. РАВНОУГОЛЬНЫЕ ПРЯМЫЕ

Множество из v прямых (проходящих через одну точку) в r-мерном евклидовом пространстве называется набором равноугольных прямых, если угол между любыми двумя прямыми один и тот же. Интересной является проблема определения максимального числа $v(r)$ таких прямых в r-мерном пространстве.

Сейдел [67] показал, что, исходя из симметричной $(0, -1, 1)$-матрицы A размером $v \times v$, можно построить набор равноугольных прямых в некотором r-мерном пространстве. Если ρ — наименьшее собственное значение (обязательно отрицательное) с кратностью $v - r$, то матрицу $(A - \rho I)/\rho$ можно интерпретировать как матрицу Грама набора из v векторов в r-мерном пространстве, причем угол α между любыми двумя прямыми удовлетворяет равенству $\cos\alpha = 1/\rho$. В случае сильно регулярных и сильных графов кратность наименьшего собственного значения обычно очень большая, и поэтому число v равноугольных прямых велико по сравнению с r. Кроме того, имеется связь между такими наборами прямых и регулярными многоугольниками, благодаря которой для некоторых наборов равноугольных прямых группа автоморфизмов соответствующего графа оказывается очень большой. Более подробно эта тематика изложена в [52].

5. ГРАФЫ РАНГА 3

Пусть G — транзитивная группа подстановок на множестве Ω. Если подгруппа G_p группы G, состоящая из всех подстановок, фиксирующих точку $p \in \Omega$, имеет r орбит, то говорят, что G является группой ранга r. Пусть $r = 3$ и соответствующие 3 орбиты суть $\{p\}$, $\Delta(p)$, $\Gamma(p)$. Очевидно, что $q \in \Delta(p) \Rightarrow p \in \Delta(q)$ тогда и только тогда, когда порядок G четный. В этом случае по группе G удается построить сильно регулярный граф $\mathcal{G}$, множество вершин которого есть Ω и две вершины p и q смежные в $\mathcal{G}$, если $p \in \Delta(q)$.

Хигман [34—42] развил теорию групп ранга 3. Эти группы являются группами автоморфизмов сильно регулярных графов, причем они действуют транзитивно как на множество вершин, так и на множество ребер.

Бесконечные классы сильно регулярных графов возникают из рассмотрения представлений классических групп, в особенности простых. Большинство из них обладают представлениями ранга 3 и являются нормальными подгруппами в группах $\mathrm{Aut}(\mathcal{G})$. В некоторых случаях представления имеют больший ранг, но может оказаться, что и они приводят к сильно регулярным графам.

Результат Зейтца [68] содержит важную информацию о представлениях ранга 3 групп Шевалле. А именно для каждого класса $G(q)$ групп Шевалле существует такое число N, что если $q > N$, то представлением ранга 3 группы $G(q)$ может быть лишь представление на смежных классах по параболической подгруппе. (В действительности результат Зейтца применим к любым рангам.) Такие представления ранга 3 не возникают

для групп $G_2(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$ и для скрученных групп $E_6'(q)$, $F_4'(q)$ и $D_4''(q)$.

Большинство таких представлений было найдено геометрическими методами. Следует упомянуть работы [58, 59] по ортогональным группам, [8, 12, 13] по унитарным группам, [43] по симплектическим и унитарным группам, а также серию статей [19, 23, 85, 86, 87, 88] по классическим группам.

Исключительные представления групп $PO_{2n+1}(3)$ были открыты Рудвалисом [62]. Другие исключительные графы и схемы, связанные с группой $V_{2n} \cdot O_{2n}^{\pm}(2)$, были комбинаторно построены Манном [54], а также Дельсартом и Гёталсом [20] в связи с задачами теории кодирования. Тейлор [76] построил сильные графы, для которых $PSU_n(q^2)$ являются группами автоморфизмов. Относительно спорадических групп, имеющих представления ранга 3, см. статью Титса [78].

6. НЕКОТОРЫЕ РЕЗУЛЬТАТЫ О ГРАФАХ РАНГА 3

6.1. Общие результаты

Фоулзер [24] и Дорнхофф [21] описали примитивные разрешимые группы ранга 3. Соответствующие графы имеют следующие параметры:

(i) $(v, k, \lambda) = (n^2, g(n-1), (g-1)(g-2)+n-2)$, т. е. это графы типа $L_g(n)$ (К.1). Допустимыми являются лишь значения (n, g): $(3^2, 4)$, $(13, 6)$, $(17, 6)$, $(19, 8)$, $(3^3, 4)$, $(29, 6)$, $(31, 8)$ $(47, 24)$ или $(3^2, 4)$, $(7^2, 10)$.

(ii) $(v, k, \lambda) = (64, 27, 10)$.

Кроме того, существуют еще два случая — когда G является подгруппой аффинной группы прямой или когда G действует на векторном пространстве V, таком, что $V = V_1 \oplus V_2$ и $V_1 \cup V_2$ — блок импримитивности группы G.

Каллахер [51] и Либлер [53] доказали, что если группа ранга 3 действует на аффинной плоскости, то это трансляционная плоскость.

Если группа ранга 3 допускает нормальную регулярную подгруппу, то она изоморфна некоторой подгруппе в полной группе автоморфизмов аффинного пространства $AG(n, g)$, содержащей все трансляции.

6.2. Характеризация посредством составляющих

Тсудзуку [79] описал все примитивные расширения ранга 3 симметрической группы $Sym(k)$, действующей естественным образом на k точках. В случае когда $k > 1$, возникают лишь следующие расширения:

(i) $k=2$, $v=5$ и $G \simeq D_5$ — диэдральная группа порядка 10,
(ii) $k=3$, $v=10$, $\mathcal{G}$ — граф Петерсена и $G \simeq \mathrm{Sym}(5)$,
(iii) $k=5$, $v=16$, $\mathcal{G}$ — граф Клебша и $G \simeq 2^4.\mathrm{Sym}(5)$,
(iv) $k=7$, $v=50$, $\mathcal{G}$ — граф Хоффмана — Синглтона и $G \simeq \mathrm{PSU}_3^*(5^2)$.

Ивасаки [50] доказал, что тот же результат справедлив и в случае, когда $G_{0|\Delta} = \mathrm{Alt}(k)$ — знакопеременная группа в естественном представлении. Монтаг [57] доказал несуществование большинства расширений групп $\mathrm{PSL}_2(q)$, $\mathrm{PSU}_3(q^2)$, $\mathrm{R}(q)$, $\mathrm{Sz}(q)$ в их естественных представлениях на k точках, где $k = q+1$, q^3+1, q^3+1, q^3+1, причем $|\Delta| = k$, $|\Gamma| = {}^1/_2(k(k-1))$. Единственными исключениями являются случаи

(i) $\mathrm{PSL}_2(3) \simeq \mathrm{Sym}(3)$: расширением является граф Петерсена;

(ii) $\mathrm{PSL}_2(4) \simeq \mathrm{Alt}(5)$ расширяется до графа Клебша;

(iii) $\mathrm{PSL}_2(9)$ приводит к группе $\mathrm{PSL}_3(4)$, действующей на графе с параметрами $(56, 10, 0)$ (S.1).

Если группы $G_{0|\Delta}$ и $G_{0|\Gamma}$ являются 2-транзитивными на Δ и Γ, то граф изоморфен либо циклу длины 5, либо объединению двух полных графов порядка $n = v/2$. В последнем случае нормальная подгруппа, фиксирующая каждую компоненту, должна действовать 3-транзитивно на K_n.

Баннаи [3] доказал, что если $G_{0|\Delta} \simeq \mathrm{PSL}_n(2^f)$ в естественном представлении, то $n=2$ и либо $f=1$, либо $f=2$. Оба этих случая охвачены результатом Монтага. В другой статье Баннаи [4] изучал случай, когда $G_{0\Delta}$ является 4-транзитивной. Он показал, что $|\Delta| = 5, 7$ и $G_{0|\Delta} \simeq \mathrm{Sym}(5)$, $\mathrm{Sym}(7)$ или $\mathrm{Alt}(7)$.

6.3. Характеризация посредством подстепеней

В некоторых случаях знание подстепеней k и l в совокупности с предположением о том, что рассматривается граф ранга 3, оказывается достаточным для классификации графов. Хигман [39] доказал следующее:

(i) Если $v = m^2$, $k = 2(m-1)$, $m \geqslant 2$, то $G \simeq \mathrm{Sym}(m) \wr \mathrm{Sym}(2)$ и граф $\mathcal{G}$ имеет тип $L_2(m)$.

(ii) Если $v = \binom{m}{2}$, $k = 2(m-2)$, $m \geqslant 5$, то либо G является 4-транзитивной подгруппой в $\mathrm{Sym}(m)$ и $\mathcal{G}$ — граф типа $T(m)$, либо

(a) $G \simeq \mathrm{P\Gamma L}_2(8)$ и $\mathcal{G}$ — граф типа $T(8)$,
(b) $\mu = 6$, $m = 9, 17, 27, 57$,
(c) $\mu = 7$, $m = 51$,
(d) $\mu = 8$, $m = 28, 36, 325, 903, 8128$.

Единственный известный случай — это действие группы $G_2(2)$ на 36 точках (S.9).

(iii) Если $v = Q_n Q_{n-1}/Q_2$, $k = qQ_2$, где $Q_n = (q^n - 1)/(q - 1)$, то либо G — подгруппа в группе $\mathrm{P\Gamma L}_m(q)$, которая при действии на прямых в $P_{m-1}(q)$ транзитивна на 4-симплексах, либо $m = 4$, 5 или $m = 2a + 1$ и $17 \geqslant m \geqslant 7$, где $\mu \neq (q+1)^2$. Аналогичный результат был получен Еномото [22]. Если $v = m^2$ и $k = 3(m-1)$, то $\mu = 6$, за исключением случая $\mu = 4$, $m = 14$ или 352. Кроме того, если предположить, что рассматривается граф ранга 3 при $m > 23$, за исключением двух указанных случаев, то G является группой автоморфизмов некоторого графа типа $L_3(n)$, где $n = 2^f$.

Отметим, что эти результаты получены без предположения о том, что ранг равен трем.

Другой результат Хигмана [35] относится к графам с $\lambda = 0$, $\mu = 1$, т. е. для $v = k^2 + 1$, и состоит в том, что k должно быть равно 2, 3, 7, 57. Такие графы существуют и имеют ранг 3 при $k = 2$, 3, 7. Ашбахер [2] доказал, что в случае $k = 57$ не существует графа ранга 3.

Если $\lambda = 0$ и $\mu \neq 2$, 4, 6, то при фиксированном μ существует лишь конечное число графов [6].

Хигман [41] изучал также псевдогеометрические графы с $T = 1$ и $v < 100$. Кроме того, он доказал несуществование графов ранга 3 с параметрами $(76, 21, 2)$ и $(96, 20, 4)$, а также единственность графа ранга 3 с параметрами $(64, 18, 2)$.

Уэлс [81] доказал, что знание $G_{0|\Delta}$ и $G_{0|\Gamma}$ однозначно определяет граф $\mathscr{G}$, если известны некоторые подстепени.

6.4. Характеризация с. р. графов посредством их собственных значений

Сейдел [66] описал все с. р. графы с наименьшим собственным значением $\rho_2 = -3$. Эти графы следующие:

(i) $L_2(n)$,
(ii) $T(n)$,
(iii) негеометрический граф с $v = 16$, $k = 6$, $\lambda = 2$,
(iv) три графа Чанга [14],
(v) графы Петерсена, Клебша и Шлэфли.

Интересно отметить, что последние три графа образуют башню ранга 3. Симс [73] доказал, используя результат Рая-Чаудхури [59] относительно реберных графов, что граф ранга 3 с наименьшим собственным значением $\rho_2 = -3$ является графом типа (i), (ii) или (iii). Более того, он высказал гипотезу о том, что если имеется бесконечно много графов ранга 3 с наименьшим собственным значением ρ_2, то $\rho_2 = 2q + 1$ $(q = p^\alpha)$, и за

конечным числом исключений такие графы исчерпываются графами типа С.1 и С.11. В другой формулировке эта гипотеза состоит в том, что параметр μ ограничен некоторой функцией от наименьшего собственного значения. Эта гипотеза доказана с использованием результата Хоффмана.

7. БАШНИ РАНГА 3

Пусть $\mathcal{G}$ — граф ранга 3 и $\Delta(p)$, $\Gamma(p)$ — две нетривиальные орбиты группы G_p. Может оказаться, что $G_{p|\Delta}$ также является представлением ранга 3 для некоторой группы. Такая ситуация может повторяться несколько раз и привести к так называемой *башне ранга* 3. Группы, составляющие известные башни, — это в основном спорадические группы и некоторые другие «исключительные» простые группы. Параметры известных башен приведены в табл. 1. Относительно первых четырех башен дальнейшие пояснения можно найти в статье Титса [77]. Заметим, что в последнем случае на первом графе подорбита $\Gamma(p)$ тоже является ортогональной башней.

8. СИЛЬНО РЕГУЛЯРНЫЕ ГРАФЫ, СВЯЗАННЫЕ С ГРУППАМИ ШЕВАЛЛЕ[1])

1. $PSL_n(q)$ $(A_{n-1}(q))$, действующая на прямых пространства $PG(n-1, q)$, $n \geqslant 4$; смежные вершины — пересекающиеся прямые.

2. $P\Omega_{2n+1}(q)$ $(B_n(q))$, действующая на точках квадрики в $PG(2n, q)$; смежные вершины — точки на образующей.

3. $PSp_{2n}(q)$ $(C_n(q))$, действующая на точках квадрики $PG(2n-1, q)$ с симплектической полярностью; смежные вершины — сопряженные точки.

4^+. $P\Omega^+_{2n}(q)(D_n(q))$, действующая на точках гиперболической квадрики пространства $PG(2n-1, q)$; смежные вершины — точки на образующей.

4^-. $P\Omega^-_{2n}(q)({}^1D_n(q^2))$, действующая на точках эллиптической квадрики пространства $PG(2n-1, q)$; смежные вершины — точки на образующей.

5. $PSU_n(q^2)$ $({}^1A_{n-1}(q^2))$, действующая на точках эрмитова многообразия в пространстве $PG(n-1, q^2)$; смежные вершины — точки на образующей.

6. $E_6(q)$, действующая на точках 26-мерного проективного представления; смежные вершины — точки на образующей.

---

[1]) Полная группа автоморфизмов рассматриваемых графов обычно совпадает с группой автоморфизмов соответствующего пространства, за некоторыми исключениями, которые имеют место при малых q и n.

Таблица 1

	v	k	l	λ	μ	G	G_0
Башня Хигмана—Симса	77	60	16	47	45	M_{22}	2^4A_6
	100	77	22	60	56	HS	M_{22}
Башня Маклафлина	162	105	56	72	60	$PSU_4(3)$	$PSL_3(4)$
	275	162	112	105	81	McL	$PSU_4(3)$
Башня Судзуки	36	14	21	4	6	$G_2(2) \simeq PSU_3(3^2)$	$PSL_3(2) \simeq PSL_2(7)$
	100	36	63	14	12	HJ	$G_2(2)$
	416	100	315	36	20	$G_2(4)$	HJ
	1 782	416	1 365	100	96	Suz	$G_2(4)$
Башня Фишера	693	180	512	51	45	$PSU_6(2^2)$	$2^9 \cdot PSU_4(2^2)$
	3 510	693	2 816	180	126	Fi_{22}	$PSU_6(2^2)$
	31 671	3 510	28 160	693	351	Fi_{23}	Fi_{22}
	306 936	31 671	275 263	3510	3240	Fi_{24}	Fi_{23}
Башня Конвея	1 408	840	567	488	520	$PSU_6(2^2)$	$PSU_4(3^2)$
	2 300	1 408	891	840	896	$Co \cdot 2$	$2 \cdot PSU_6(2^2)$
Башня Матье	1 288	792	495	476	504	M_{24}	$2 \cdot M_{12}$
	2 048	1 288	759	792	840	$2^{11} \cdot M_{24}$	M_{24}
Ортогональные башни	2^{2n}	$2^{2n-1} \mp 2^{n-1}$	$2^{2n-1} \pm 2^{n-1} - 1$	$2^{2n-2} \mp 2^{n-1}$	$2^{2n-2} \mp 2^{n-1}$	$2^{2n} \cdot O^{\pm}_{2n}(2)$	$O^{\pm}_{2n}(2)$
	$2^{2n+1} \pm 2^n - 1$	2^{2n}	$2^{2n} \pm 2^n - 2$	$2^{2n-1} \mp 2^{n-1}$	2^{2n-1}	$O^{\pm}_{2n+2}(2)$	$2^{2n} \cdot O_{2n}(2)$

7. $P\Omega_{10}^{+}(q)$, действующая на одном семействе изотропных 4-плоскостей гиперболической квадрики в $PG(9, q)$; смежные вершины — 4-плоскости, пересекающиеся по 2-плоскости.

8. $PSU_5(q^2)$, действующая на прямых эрмитова многообразия в пространстве $PG(4, q^2)$; смежные вершины — пересекающиеся прямые.

Замечание: то же представление группы $PSU_4(q^2)$ на прямых эрмитова многообразия приводит к графу, описанному в п. (4^-) при $n = 3$.

$9^{\pm}$. $P\Omega_{2n}^{\pm}(2)$, действующая на точках квадрики в пространстве $PG(2n-1, 2)$; смежные вершины — точки на касательной.

$10^{\pm}$. $P\Omega_{2n+1}(3)$, действующая на точках внутри (соответственно вне) квадрики в пространстве $PG(2n, 3)$; смежные вершины — точки на прямой, не пересекающей квадрику.

Другие графы, связанные с классическими группами

11. Стабилизатор копрямой в $PG(n, q)$, $n \geqslant 3$, действующий на прямых, не пересекающих эту копрямую; смежные вершины — пересекающиеся прямые.

$12^{\pm}$. $V_{2n}(q) \cdot O_{2n}^{\pm}(q)$, действующая на точках евклидова пространства $(V_{2n}(q))$ с квадратичной формой; смежные вершины — точки на изотропной прямой.

13. Подгруппа $x' = a^2x + b$ аффинной прямой над $GF(q)$, где $q = 1 \pmod 4$, действующая на точках; смежные вершины — точки, координаты которых отличаются на квадрат.

Замечание: п. 11, $12^{\pm}$, 13 являются представлениями ранга 3.

14. $PSU_n(q^2)$ $({}^1A_{n-1}(q^2))$, действующая на точках эрмитова многообразия в пространстве $PG(n-1, q^2)$; смежные вершины — точки на касательной.

15. Группа автоморфизмов пространства $AG(n, q)$, действующая на прямых; смежные вершины — пересекающиеся прямые (представление ранга 4).

16. Группа автоморфизмов $AG(3, q^2)$ с выделенной бэровской подплоскостью на бесконечности; смежные вершины — точки на «изотропной» прямой (представление ранга 3).

17. Группа автоморфизмов $AG(3, 2^r)$ с полной коникой в бесконечности (объединение коники и ее узла), действующая на точках; смежные вершины — точки на «изотропной прямой» (представление ранга 4, за исключением случая $r = 2$, когда ранг равен 3).

18. Та же группа, действующая на изотропных прямых; смежные вершины — пересекающиеся прямые (интранзитивное

представление, за исключением случая $r=2$, когда ранг равен 4).

19. Подгруппа автоморфизмов пространства $AG(2, q)$, сохраняющих m изотропных направлений, действующая на точках; смежные вершины — точки на изотропной прямой.

20. Группа автоморфизмов эрмитовой параболы P в пространстве $AG(2, q^2)$ (q нечетно). Если уравнение для P имеет вид $x\bar{x}+(y+\bar{y})=0$, то две вершины смежны тогда и только тогда, когда для соответствующих точек с координатами (x_1, y_1) и (x_2, y_2) выражение $x_1\bar{x}_2+y_1+\bar{y}_2$ является квадратом (соответственно неквадратом) в $GF(q)$ при $-1\notin GF^{x2}(q)$ (соответственно при $-1\in GF^{x2}(q)$).

S. *Сильно регулярные графы, связанные со спорадическими группами*

1. $PSL_3(4)$, действующая на орбите из 56 полных коник в пространстве $PG(2, 4)$; смежные вершины — непересекающиеся коники (см. [25, 26, 57]). Представление ранга 3 группы $PSL_3(4)$ по подгруппе $Alt(6)$.

2. M_{22}, действующая на 77 блоках системы $S(3, 6, 22)$; смежные вершины — непересекающиеся блоки. Представление ранга 3 группы M_{22} на смежных классах по подгруппе $2^4\cdot Alt(6)$.

3. $PSU_3(5^2)$, действующая на подмножествах самосопряженных треугольников в пространстве $PG(2, 5^2)$ с эрмитовой коникой. Простое описание можно получить следующим образом. Пусть $p=A_7$, $\Delta(p)$ — множество из 7 подгрупп A_6 в группе A_7 (стабилизаторы точек). Пусть $\Gamma(p)$ — множество из 7×6 подгрупп A_5, содержащихся в A_6 и действующих транзитивно на 6 точках. Две точки из $\Gamma(p)$ смежны, если соответствующие подгруппы A_5 пересекаются по подгруппе D_5 (см. [5, 48, 64]). Представление ранга 3 группы $PSU_3(5^2)$ на смежных классах по подгруппе $Alt(7)$.

4. $PSL_3(4)$, действующая на 105 флагах пространства $PG(2, 4)$. Две вершины смежны, если соответствующие флаги имеют различные центры и оси, причем центр одного флага лежит на оси другого (см. [26, 67]). Представление ранга 6.

5. $PSL_3(4)$, действующая на орбите из 120 бэровских подплоскостей в пространстве $PG(2, 4)$; смежные вершины — плоскости, пересекающиеся по единственной точке (см. [26]). Представление ранга 5.

6. M_{23}, действующая на 253 блоках системы $S(4, 7, 23)$; смежные вершины — блоки, пересекающиеся по единственной точке. Представление ранга 3 группы M_{23} на смежных классах по подгруппе $2^4\cdot Alt(7)$.

7. M_{22}, действующая на 176 блоках системы $S(4, 7, 23)$, не проходящих через фиксированную точку; смежные вершины —

блоки, пересекающиеся по единственной точке [26]. Представление ранга 3 группы M_{22} на смежных классах по Alt(7).

8. $PSU_3(5^2)$, действующая на 175 ребрах графа Хоффмана — Синглтона (S.3). Другое описание можно получить, исходя из графа 7, а именно в последнем надо выбрать вершину p, рассмотреть подграф $\Delta(p) \cup \Gamma(p)$ и осуществить переключения относительно $\{\Delta(p), \Gamma(p)\}$. Представление ранга 4 группы $PSU_3(5^2)$ по подгруппе $Alt(6) \cdot 2$.

9. Представление ранга 3 группы $G_2(2)$ на 36 точках [68].

10. Представление ранга 3 группы HS на 100 точках [42, 78, 26].

11. Представление ранга 3 группы HJ на 100 точках [30, 77, 78].

12. Представление ранга 3 группы $PSU_4(3)$ на 162 точках [78].

13. Представление ранга 3 группы McL на 275 точках. Простое описание может быть получено с использованием графа 6. Для заданной точки системы S(4, 7, 23) 253 блока последней распадаются на два класса $\mathscr{H}_1$, $\mathscr{H}_2$, а именно блоки, проходящие через эту точку (77), и оставшиеся блоки (176). Теперь осуществим переключение графа 6 относительно $\{\mathscr{H}_1, \mathscr{H}_2\}$, возьмем дополнение $\overline{\mathscr{H}_1}$ к подграфу $\mathscr{H}_1$ и добавим оставшиеся 22 точки системы S(4, 7, 23) со следующим отношением смежности: точка смежна с каждым блоком из $\mathscr{H}_1$, которому она неинцидентна, и с каждым блоком из $\mathscr{H}_2$, которому она инцидентна (см. [17], а также [55, 78]).

14. Представление ранга 3 группы $G_2(4)$ на 416 точках [78].

15. Представление ранга 3 группы Suz на 1782 точках [78, 79, 81].

16. Представление ранга 3 группы Fi_{22} на 3510 точках [78].

17. Представление ранга 3 группы Fi_{23} на 31 671 точках [78].

18. Представление ранга 3 группы Fi_{24} на 306 936 точках [78].

19. Представление ранга 3 группы $2^{11} \cdot M_{24}$ на 2048 точках. Соответствующий граф связан с кодом Голея (см. [26]).

20. Представление ранга 3 группы M_{24} на смежных классах по подгруппе $M_{12} \cdot 2$; 1288 вершин графа — это 1288 разбиений 24 точек системы S(5, 8, 24) на два подмножества, каждое мощностью 12 (такие подмножества называют додекадами), на которых M_{12} действуют неэквивалентным образом. Две вершины смежны, если две пары додекад пересекаются в (4, 8, 4, 8) точках.

21. Представление ранга 3 группы $CO \cdot 2$ на смежных классах по подгруппе $PSU_6(2) \cdot 2$. Выберем в решетке Лича две точки на расстоянии $4\sqrt{2}$ и две сферы с центрами в этих точках

подходящего радиуса. Группа Co·2 действует на 2300 парах противоположных точек решетки Лича, лежащих на пересечении сфер (см. [17]).

22. Представление ранга 3 группы $PSU_6(2)$ на смежных классах по подгруппе $PSU_4(3)$. Рассмотрим снова решетку Лича и выберем треугольник типа 222. Стабилизатор вершин этого треугольника действует на 408 точках, дополняющих треугольник до тетраэдра типа 222222.

23. Представление ранга 3 группы Рудвалиса на смежных классах по подгруппе $'F_4(2)$ (см. [18]).

9. КОМБИНАТОРНЫЕ СИЛЬНО РЕГУЛЯРНЫЕ ГРАФЫ

Комбинаторная точка зрения также приводит к некоторым интересным классам с. р. графов. Более того, некоторые графы характеризуются лишь своими комбинаторными свойствами. Мы уже упоминали результат Сейдела [66] относительно графов, для которых -3 является наименьшим собственным значением. В его доказательстве использовался более ранний результат Чанга [14] (а также результат Коннора [16]), результат Хоффмана [46], относящийся к треугольным схемам отношений $T(m)$, и результат Шрикханде [69], касающийся L_2-схем отношений $L_2(n)$. В действительности рассматриваемые параметры определяют указанные два класса графов и два исключительных примера. Для $v=28$, $k=12$, $\lambda=6$, кроме $T(8)$, существуют еще три неизоморфных графа [15], получаемых из $T(8)$ путем переключения [65]. Для $v=16$, $k=6$, $\lambda=2$ существует негеометрический граф с теми же параметрами. На этом пути Буссемакер и Сейдел [11] доказали существование более чем 80 неизоморфных графов типа $L_2(6)$ и более чем 23 графов типа $NL_2(6)$. Другие классы с. р. графов были построены различными способами.

Меснер [56], используя результат Рая-Чаудхури [60], построил два класса (в действительности только один) с. р. графов, являющихся графами типа отрицательных латинских квадратов (т. е. имеющих те же параметры, что и $L_{-g}(n)$).

Боуз и Шрикханде [10] построили большое число с. р. графов с $\lambda=\mu$, являющихся графами типа $L_2(2r)$, $NL_2(2r)$, и с параметрами $(v, k, \lambda)=(4r^2-1,\ 2r^2,\ r^2)$. Кроме того, Валлис [83, 84] изучал графы с $\lambda=\mu$ и построил графы других типов, используя аффинные разрешимые схемы. Он также доказал существование по крайней мере двух неизоморфных графов с параметрами $(n^2(n+2), n(n+1), n)$ для $n=p^\alpha$.

Эти графы были впервые построены Холлом [29] при $p=2$ и Аренсом и Секересом [1] в общем случае. Из построения Аренса и Секереса получается еще один класс с. р. графов (К.3).

Если $p \neq 2$, это построение тесно связано с построением графа на эрмитовой параболе в аффинной плоскости.

Другие построения с помощью матриц Адамара можно найти у Холла [28] и у Гёталса и Сейдела [26]. В последней статье построены также некоторые другие интересные графы, связанные с квазисимметричными схемами (схемы, у которых лишь два типа пересечений блоков). В частности, там содержится очень аккуратное исследование схемы S(5, 8, 24) и связанных с ней графов. Отметим, что высказанная там гипотеза о существовании с. р. графа с $v = 1288$ (см. [26]) верна (см. башни ранга 3).

К. *Комбинаторные сильно регулярные графы*

1. Графы латинских квадратов $L_g(n)$. Пусть заданы $g-2$ ортогональных латинских квадратов порядка n. Граф строится на n^2 клетках квадрата. Две вершины смежны, если клетки находятся либо в одной строке, либо в одном столбце, либо они содержат одинаковые символы.

2. Треугольные графы. Они отвечают представлению ранга 3 группы $\mathrm{Sym}(k)$ на парах точек. Две вершины смежны, если пары содержат общую точку (см. также С.1).

3. Точечный граф частичной геометрии типа $(\lambda+2, \lambda, 1)$, $\lambda = p^\alpha$ (см. Аренс и Секерес [1]).

4. Граф прямых той же геометрии.

5. Графы отрицательных латинских квадратов (см. [56, 10]).

6. Граф прямых схемы $S(2, \tilde{k}, \tilde{v})$; смежные вершины — пересекающиеся блоки.

ПРИЛОЖЕНИЕ

	v	k	l	λ	μ	ρ_1	ρ_2
S.1	56	10	45	0	2	7	−5
S.2	77	16	60	0	4	11	−5
S.3	50	7	42	0	1	5	−5
S.4	105	32	72	4	12	19	−5
S.5	120	42	77	8	18	23	−5
S.6	253	112	140	36	60	51	−5
S.7	176	70	105	18	34	35	−5
S.8	175	72	102	20	36	35	−5
S.9	36	14	21	4	6	7	−5
S.10	100	22	77	0	6	15	−5
S.11	100	36	63	14	12	7	−13
S.12	162	56	105	10	24	31	−5
S.13	275	112	162	30	56	55	−5
S.14	416	100	315	36	20	7	−41

	v	k	l	λ	μ	ρ_1	ρ_2
S.15	1 782	416	1 365	100	96	31	−41
S.16	3 510	693	2 816	180	126	17	−127
S.17	31 671	3 510	28 160	693	351	17	−703
S.18	306 936	31 671	275 264	3 510	3 240	161	−703
S.19	2 048	759	1 288	310	264	17	−111
S.20	1 288	495	792	206	180	17	−71
S.21	2 300	891	1 408	378	324	17	−127
S.22	1 408	567	840	246	216	17	−79
S.23	4 060	1 755	2 304	730	780	129	−31

	v	k	l
K.1.	n^2	$g(n-1)$	$(n-g+1)(n-1)$
K.2.	$\binom{n}{2}$	$2(n-2)$	$\binom{n-2}{2}$
K.3.	q^3	$(q-1)(q+2)$	$(q-1)^2(q+1)$
K.4.	$q^2(q+2)$	$q(q+1)$	$(q+1)^2(q-1)$
K.5.	n^2	$g(n+1)$	$(n-g-1)(n+1)$
K.6.	$\frac{\tilde{v}(\tilde{v}-1)}{\tilde{k}(\tilde{k}-1)}$	$\tilde{k}\frac{\tilde{v}-\tilde{k}}{\tilde{k}-1}$	$\frac{(\tilde{v}-\tilde{k})(\tilde{v}-\tilde{k}^2+\tilde{k}-1)}{\tilde{k}(\tilde{k}-1)}$

	λ	μ	$\{\rho_1, \rho_2\}$
K.1.	$(g-1)(g-2)+n-2$	$g(g-1)$	$2g-1,\ 2g-2n-1$
K.2.	$n-2$	4	$2n-7,\ -3$
K.3.	$q-2$	$q+2$	$2q+3,\ 3-2q$
K.4.	q	q	$2q-1,\ -2q-1$
K.5.	$(g+1)(g+2)-n-2$	$g(g+1)$	$-2g+1,\ -2g+2n-1$
K.6.	$(\tilde{k}-1)^2+\frac{\tilde{v}-1}{\tilde{k}-1}-2$	$\tilde{k}^2$	$2\tilde{k}-1,\ 2\tilde{k}-1-2\frac{\tilde{v}-\tilde{k}}{\tilde{k}-1}$

	v	k	l
C.1.	$\frac{(q^{n+1})(q^n-1)}{(q+1)(q-1)^2}$	$\frac{q(q+1)(q^{n-1}-1)}{q-1}$	$\frac{q^4(q^{n-1}-1)(q^{n-2}-1)}{(q+1)(q-1)^2}$

	v	k	l
C.2.3.	$\frac{q^{2n}-1}{q-1}$	$q\,\frac{q^{2n-2}-1}{q-1}$	q^{2n-1}
C.4.$^{\pm}$	$\frac{(q^n \mp 1)(q^{n-1} \pm 1)}{q-1}$	$\frac{q(q^{n-1} \mp 1)(q^{n-2} \pm 1)}{q-1}$	q^{2n-2}
C.5.*	$\frac{(q^{n-1} \mp 1)(q^n \pm 1)}{q^2-1}$	$\frac{q^2(q^{n-3} \mp 1)(q^{n-2} \pm 1)}{q^2-1}$	q^{2n-3}
C.6.	$\frac{(q^{12}-1)(q^9-1)}{(q^4-1)(q-1)}$	$\frac{q(q^8-1)(q^3+1)}{q-1}$	$\frac{q^8(q^5-1)(q^4+1)}{q-1}$
C.7.	$\frac{(q^8-1)(q^3+1)}{q-1}$	$\frac{q(q^5-1)(q^2+1)}{q-1}$	$\frac{q^6(q^5-1)}{q-1}$
C.8.	$(q^5+1)(q^3+1)$	$q^3(q^2+1)$	q^8
C.9.$^{\pm}$	$2^{2n-1} \pm 2^{n-1}$	$2^{2n-2}-1$	$2^{2n-2} \pm 2^{n-1}$
C.10.	$\frac{3^n(3^n \pm 1)}{2}$	$\frac{3^{n-1}(3^n \mp 1)}{2}$	$3^{2n-1} \pm 3^{n-1} \cdot 2 - 1$
C.11.	q^{2n-2}	$(q+1)(q^{n-1}-1)$	$q(q^{n-1}-1)(q^{n-2}-1)$
C.12.$^{\pm}$	q^{2n}	$(q^n \mp 1)(q^{n-1} \pm 1)$	$q^{n-1}(q-1)(q^n \mp 1)$
C.13.	$4\alpha+1=q$	2α	2α
C.14.*	$\frac{q^{n-1}(q^n \pm 1)}{q+1}$	$(q^{n-1} \mp 1)(q^{n-2} \pm 1)$	$\frac{q^{n-2}(q^{n-1} \mp 1) \times (q^2-q-1)}{q+1}$
C.15.	$\frac{q^{n-1}(q^n-1)}{q-1}$	$\frac{q^2(q^{n-1}-1)}{q-1}$	$\frac{q(q^n-1)(q^{n-2}-1)}{q-1} + q - 1$
C.16.	q^6	$(q+1)(q^3-1)$	$q(q^2-1)(q^3-1)$
C.17.	2^{3r}	$2^{2r}+2^r-2$	$(2^{2r}-1)(2^r-1)$
C.18.	$2^{2r}(2^r+1)$	$2^r(2^r+1)$	$(2^{2r}-1)(2^r+1)$
C.19.	q^2	$m(q-1)$	$(q+1-m)(q-1)$
C.20.	q^3	$\frac{(q-1)(q^2+1)}{2}$	$\frac{(q+1)(q^2-1)}{2}$

* Верхний знак отвечает нечетным значениям n, а нижний — четным

	λ	μ	$\{\rho_1, \rho_2\}$
C.1.	$\frac{q^n-1}{q-1}+q^2-2$	$(q+1)^2$	$2q+1,$ $-2\frac{q^{n-1}-1}{q-1}+2q+3$
C.2.3.	$\frac{q^{2n-2}-1}{q-1}-2$	$\frac{q^{2n-2}-1}{q-1}$	$2q^{n-1}+1,\ -2q^{n-1}+1$
C.4.$^{\pm}$	$\frac{q(q^{n-2}\mp 1)(q^{n-2}\pm q)}{q-1}+$ $+q-1$	$\frac{(q^{n-1}\mp 1)(q^{n-2}\pm 1)}{q-1}$	$\pm 2q^{n-2}+1,$ $\mp 2q^{n-1}+1$
C.5.	$\frac{q^3(q^{n-4}\pm 1)(q^{n-4}\mp q)}{q^2-1}+$ $+q^2-1$	$\frac{(q^{n-3}\mp 1)(q^{n-2}\pm 1)}{q^2-1}$	$\pm 2q^{n-2}+1,$ $\mp 2q^{n-3}+1$
C.6.	$\frac{q^2(q^2+1)(q^5-1)}{q-1}+$ $+q-1$	$\frac{(q^4-1)(q^3+1)}{q-1}$	$2q^3+1,$ $-2\frac{q^4(q^5-1)}{q-1}+1$
C.7.	$\frac{q^2(q^3-1)(q+1)}{q-1}+q-1$	$\frac{(q^3-1)(q^2+1)}{q-1}$	$2q^2+1,$ $\frac{-2q^3(q^3-1)}{q-1}+1$
C.8	q^3-1	q^2+1	$2q^2+1,\ -2q^3+1$
C.9.$^{\pm}$	$2^{2n-3}-2$	$2^{2n-3}\mp 2^{n-2}$	$1\pm 2^{n-1},\ -1\mp 2^n$
C.10.	$\frac{3^{n-1}(3^{n-1}\mp 1)}{2}$	$\frac{3^{n-1}(3^{n-1}\mp 1)}{2}$	$3^{n-1}\cdot 2-1,$ $-3^{n-1}\cdot 2-1$
C.11.	$q^{n-1}+q^2-q-2$	$q(q+1)$	$2q+1,\ -2q^{n-1}+2q+1$
C.12.$^{\pm}$	$q(q^{n-1}\mp 1)(q^{n-2}\pm 1)+$ $+q-2$	$q^{n-1}(q^{n-1}\pm 1)$	$\pm 2q^{n-1}+1,$ $\pm 2q^{n-1}\mp 2q^n+1$
C.13.	$\alpha-1$	α	$\sqrt{q},\ -\sqrt{q}$
C.14.*	$q^{2n-5}(q+1)\pm$ $\pm q^{n-2}(q-1)-q$	$q^{n-3}(q+1)(q^{n-2}\pm 1)$	$\pm q^{n-2}+1,$ $\mp 2q^{n-3}(q^2-q-1)+1$
C.15.	$\frac{q^n-1}{q-1}+q^2-2q-1$	q^2	$2q-1,$ $-2\frac{q^n-1}{q-1}+2q+1$
C.16.	q^3+q^2-q-2	$q(q+1)$	$2q+1,\ -2q^3+2q+1$
C.17.	2^r-2	2^r+2	$2^{r-1}+3,\ -2^{r-1}+3$
C.18.	2^r	2^r	$2^{r-1}-1,\ -2^{r-1}-1$
C.19.	$(m-1)(m-2)+q-2$	$m(m-1)$	$2m-1,\ 2m-2q-1$
C.20.	$\frac{(q-1)^3}{4}-1$	$\frac{(q-1)(q^2+1)}{4}$	$q^2,\ -q$

* Верхний знак отвечает нечетным значениям n, а нижний — четным.

ЗАМЕЧАНИЯ ПРИ КОРРЕКТУРЕ

С 1973 г. были получены новые результаты. Мы хотели бы включить большинство из них.

К разд. 2. Частичные геометрии. Дж. Тас (Simon Stevin, 1973, v. 46, p. 95—98) построил частичные геометрии, которые несбалансированы и не являются сетями.

К п. 6.2. Характеризация посредством составляющих. Автор описал расширение групп $\mathrm{Sym}(n)$ и $\mathrm{Alt}(n)$, действующих на $\binom{n}{2}$ неупорядоченных парах элементов множества мощностью n. Исключительные расширения ранга 3 возникают лишь при $n=5$ и $n=8$. В этих двух случаях $(v, k, \lambda)=(16, 10, 5)$ и $(64, 28, 35)$; в остальных случаях получается треугольный граф $\mathrm{T}(n+2)$.

П. Камерон (Proc. London Math. Soc. 1972, v. 25, p. 427—440) показал, что если $G_{0|\Delta}$ является t-транзитивной группой ($t \geqslant 3$), то имеет место одно из следующих соотношений: (i) $|\Gamma| = {}^1/_2(k(k-1))$, (ii) $|\Gamma|=k(k-1)$ или (iii) $v=(\alpha+1)^2(\alpha+4)^2$, $k=(\alpha+1)(\alpha^2+5\alpha+5)$, $\mu=(\alpha+1)(\alpha+2)$ (единственный известный пример в случае (iii) — это граф Хигмана — Симса, S.10).

Ф. Бюкенхаут и К. Юбо описали все расширения в случае, когда $G_{0|\Delta}$ содержит классическую группу $\mathrm{PS}p$, $\mathrm{P}\Omega$ или PSU в естественном представлении ранга 3. Расширения ранга 3 — это (i) $\mathrm{C}.12^{\pm}$, что является расширением графов из $\mathrm{C}.4^{\pm}$ при $q=2$; (ii) $\mathrm{C}.9^{\pm}$, что является расширением C.2 при $q=2$; (iii) $(v, k, \lambda)=(35, 16, 6)$; $(176, 40, 12)$, $(275, 112, 30)$, $(126, 25, 8)$, $(126, 45, 12)$ и $(3510, 693, 180)$, причем группы автоморфизмов изоморфны $\mathrm{Alt}(8)$, $\mathrm{PSU}_5(4)$, $\mathrm{Alt}(10)$, McL, $\mathrm{P}\Omega_6^-(3)$ и Fi_{22} (в печати).

К п. 6.3. Характеризация посредством подстепеней. Если $\mathcal{G}$ — граф ранга 3, где

$$(v,\ k,\ l)=\left(\frac{q^r-1}{q-1},\ q\,\frac{q^{r-2}-1}{q-1},\ q^{r-1}\right),$$

то при некоторых предположениях $\mathcal{G}$ есть граф типа C.3. Этот сильнейший результат был получен В. Кантором (характеризация классических геометрий как графов ранга 3) при $r \geqslant 6$. Другие результаты при дополнительных предположениях можно найти в [34] и статье А. Янушки (характеризация симплектических групп $\mathrm{PS}p(2m, q)$ как групп подстановок ранга 3).

Относительно расширений ранга 3 упомянем результат М. С. Смит (Bull. London Math. Soc., 1974, v. 6, p. 1—3), который состоит в том, что если дан граф $\mathcal{G}$ ранга 3, то при неко-

торых предположениях относительно характеров рассматриваемого представления существуют самое большее 4 расширений ранга 3 $\mathcal{G}'$ графа $\mathcal{G}$. На комбинаторном языке сформулированные условия эквивалентны тому, что $\mathcal{G}'$ и $\mathcal{G}$ имеют общее собственное значение.

К разд. 7. Башни ранга 3. Две бесконечные башни возникают из представлений ортогональных групп над полем GF(3). Эти группы следующие: $P\Omega_4^{\pm}(3) \subset P\Omega_5(3) \subset P\Omega_6^{\mp}(3) \subset P\Omega_7(3)\ldots$ в представлениях, описанных в C.10′, а графы являются дополнительными к C.10± (C.10′ см. ниже).

Унитарные группы над полем GF(4) также приводят к бесконечной башне; соответствующие графы — это дополнительные графы к графам C.14 при $q=2$.

К разд. 8. С. Р. графы. Добавим следующие серии: C.10′±. $P\Omega_{2n}^{\pm}(3)$, действующая на блоках импримитивности точек, лежащих вне квадрики в пространстве $PG(2n-1, 3)$; смежные вершины — точки на прямой, не пересекающей квадрику,

$$v=3^{n-1}\frac{3^n\mp 1}{2},\quad k=3^{n-1}\frac{3^{n-1}\mp 1}{2},\quad l=3^{2n-2}-1,$$

$$\lambda=3^{n-2}\frac{3^{n-1}\pm 1}{2},\quad \mu=3^{n-1}.$$

C.11. $V_{10}(q)\cdot PSL(5, q)$, действующая на кососимметрических тензорах; смежные вершины — тензоры, разность которых является бивектором,

$$v=q^{10},\quad k=(q^5-1)(q^2+1),\quad l=q^2(q^3-1)(q^5-1),$$
$$\lambda=q(q+1)(q^3-2)+q-2,\quad \mu=q^2(q^2+1).$$

П. Камерон (сообщила М. С. Смит). $S.24.2^{11}\cdot M_{24}$, действующая на смежных классах по M_{24}. Вершины множества Δ — это 276 неупорядоченных пар точек системы S(5, 8, 24), вершины из множества Γ — это 1771 специальное разбиение множества точек на 6 четверок. Пара смежна с набором из 6 четверок тогда и только тогда, когда она целиком лежит в одной четверке. Для заданного набора из 6 четверок имеется 240 других наборов, таких, что одна четверка из исходного набора имеет пересечение (3, 1) с двумя четверками из другого набора.

$$v=2048,\quad k=276,\quad l=1771,\quad \lambda=44,\quad \mu=36,$$
$$\rho_1=-41,\quad \rho_2=23.$$

(Дж. Конвей и М. Смит).

Автор хотел бы поблагодарить рецензента за улучшение рукописи.

ЛИТЕРАТУРА

[1] Ahrens R. W., Szekeres G. On a combinatorial generalization of 27 lines associated with a cubic surface. — J. Austral. Math. Soc., 1964, v. 10, p. 485—492.

[2] Ashbacher M. The non existence of rank three permutation group of degree 3250 and subdegrees 57, 3192. — J. Algebra, 1971, v. 19, p. 538—540.

[3] Bannai E. Primitive extensions of rank 3 of the finite projective special linear groups PSL(n, q), $q = 2^f$. — Osaka J. Math., 1972, v. 3, p. 75—94.

[4] Bannai E. On rank 3 graphs with a multiply transitive constituent. — J. Math. Soc. Japan, 1972, v. 24, p. 252—254.

[5] Benson C. T., Losey N. E. On a graph of Hoffman and Singleton. — J. Combin. Theory, 1971, v. 11, p. 67—79.

[6] Biggs N. Finite Groups of Automorphisms. — London Math. Soc. Lecture Note Series. — Cambridge, 1971.

[7] Bose R. C. Strongly regular graphs, partial geometries and partially balanced designs. — Pacific J. Math., 1963, v. 13, p. 389—419.

[8] Bose R. C., Chakravarti I. M. Hermitian varieties in a finite space PG(N, g^2). — Can. J. Math., 1966, v. 18, p. 1161—1182.

[9] Bose R. C., Shimamoto T. Classification and analysis of partially balanced incomplete block designs with two associate classes. — J. Amer. Statist. Assoc., 1952, v. 47, p. 151—184.

[10] Bose R. C., Shrikhande S. S. Graphs in which each pair of vertices is adjacent to the same number d of other vertices. — Studia Sci Math. Hungar., 1970, v. 5, p. 181—195.

[11] Busenmaker F. C., Seidel J. J. Symmetric Hadamard matrices of order 36. — Techn. Univ. Eindhoven, 1970.

[12] Chakravarti I. M. Strongly regular graphs (two class association schemes) and block design from Hermitian varieties in a finite projective space PG$(3, q^2)$. — Proc. 2nd Chapel Hill Conf. on Combinatorial Mathematics and its Applications. — Univ. of N. Carolina, Chapel Hill, N. C., 1970, p. 58—66.

[13] Chakravarti I. M. Some properties and applications of Hermitian varieties in a finite projective space PG(N, q^2) in the construction of strongly regular graphs (two-class association schemes) and blocks-designs. — J. Combin. Theory, 1971, v. 11, p. 268—283.

[14] Chang L. C. The uniqueness and nonuniqueness of triangular association chemes. — Sci. Record, 1949, v. 3, p. 604—613.

[15] Chang L. C. Association schemes of partially balanced block designs with parameters $v = 28$, $n_1 = 12$, $n_2 = 15$ and $p^2_{11} = 4$, — Sci. Record, 1950, v, 4, p. 12—18.

[16] Connor W. S. The uniqueness of the triangular association scheme. — Ann. Math. Statist., 1958, v. 29, p. 262—266.

[17] Conway J. H. A group of order 8, 315, 553, 613, 086. 720, 000, — Bull. London Math. Soc., 1969, v. 1, p. 79—88.

[18] Conway. H., Wales D. The construction of the Rudvalis simple group J. order 145, 926, 144, 000. — J. Algebra. 1973, v. 27, p. 538—548.

[19] Dai Zong-Duo, Feng Xu-Ning. Studies in finite geometries and the construction of incomplete block designs IV. Some «Anzahl» theorems in orthogonal geometry over finite fields of characteristic $\neq 2$. — Acta Math. Sinica, 1965, v. 15, p. 545—558.

[20] Delsarte P., Goethals J M. Tri-weight codes and generalized Hadamard matrices. — Information and Control, 1969, v. 15, p. 196—206.

[21] Dornhoff L. The rank of primitive solvable permutation gropus. — Math. Z., 1969, v 109, p. 205—210.

[22] Enomoto H. Strongly regular graphs and finite permutation groups of

rank 3. — J. Math. Kyoto Univ., 1971, v. 11(3), p. 381—397.
[23] Feng Xu-Ning, Dai Zong-Duo. Studies in finite geometries and the construction of incomplete block designs V. Some «Anzahl» theorems in orthogonal geometries over finite fields of characteristic 2. — Acta Math. Sinica, 1965, v. 15, p. 664—682.
[24] Foulser D. A. Solvable primitive permutation groups of low rank. — Trans. Amer. Math. Soc., 1969, v. 143, p. 1—54.
[25] Gewirtz A. The uniqueness of $G(2, 2, 10, 56)$. — Trans. New York Acad. Sci., 1969, v. 31,p . 656—675.
[26] Goethals J. M., Seidel J. J. Quasi-symmetric block designs. — Proc. Calgary Int. Conf. Calgary. Alta, 1969, p. 111—116.
[27] Goethals J. M., Seidel J. J. Strongly regular graphs derived from combinatorial designs. — Can. J. Math., 1970, v. 22, p. 597—614.
[28] Hall M. Automorphisms of Hadamard matrices. — SIAM J. Appl. Math., 1969, v. 17(6), p 1094—1101.
[29] Hall M., Jr. Affine Generalized Quadrilaterals. — Studies in Pure Math. — New York: Academic Press, 1971, p. 113—116.
[30] Hall M., Lane R., Wales D. Designs derived from permutation groups. — J. Combin. Theory, 1970, v. 8, p. 12—22.
[31] Hall M., Wales D. The simple group of order 604,800. — J. Algebra, 1968, v. 9, p. 417—450.
[32] Hestenes M. D. Rank 3 graphs. — Proc. Conf. West Mich. Univ., Kalamazoo, Mich.. 1968. — Berlin. Springer, 1969, p. 191—192.
[33] Hestenes M. D., Higman D. G. Rank 3 groups and strongly regular graphs. — SIAM-Ans Proc. Computers in Algebra and Number Theory, 1971, v. IV, p. 141—159. [Имеется перевод: Кибернет. сб., 1986, вып. 23, с. 131—152.]
[34] Higman D. G. Finite permutation groups of rank 3. — Math. Z., 1964, v. 86 p. 145—156.
[35] Higman D. G. Primitive rank 3 groups with a prime subdegree. — Math. Z., 1966, v. 91, p. 70—86.
[36] Higman D. G. Intersection matrices for finite permutation groups. — J. Algebra, 1967, v. 6, p. 22—42.
[37] Higman D G. On finite affine planes of rank 3. — Math. Z., 1968, v. 104, p. 147—149.
[38] Higman D. G. A survey of some questions and results about rank 3 permutation groups. — Actes, Congres Int. Math. Rome, 1970, v. 1, p. 361—365.
[39] Higman D. G. Characterization of families of rank 3 permutation groups by the subdegrees I, II. — Arch. Math., 1970, v. 21, p. 151—156; 353—361.
[40] Higman D. G. Coherent configurations. — Rend. Sem. Mat. Univ. Padova, 1970, v. 44, p. 1—26.
[41] Higman D. G. Partial geometries, generalized quadrangles and strongly regular graphs. — Att. del Conv. di Geom. Comb. e sue Applic., Perugia, 1971, p. 263—294.
[42] Higman D. G. Solvability of a class of rank 3 permutation groups. — Nagoya Math. J., 1971, v. 41, p. 89—96.
[43] Higman D. G., MacLaughlin J. E. Rank 3 subgraphs of finite symplectic and unitary groups. — J. Reine Angew. Math., 1965, v. 218, p. 174—189.
[44] Higman D. G., Sims S. A simple group of order 44,352,000. — Math. Z. 1968, v. 105, p. 110—113.
[45] Higman G. On the simple group of D. G. Higman and C. C. Sims. — Illinois J. Math., 1969, v. 13, p. 74—80.
[46] Hoffman A. J. On the uniqueness of the triangular association scheme. — Ann. Math. Statist., 1960, v. 31, p. 492—497.
[47] Hoffman A. J., Ray-Chaudhuri D. K. On the line graph of a finite affine plane, — Can. J. Math., 1965, v. 17, p. 687—694.

[48] Hoffman A. J., Singleton R. R. On Moore graphs with diameter 2 and 3. — IBM J. Res. Develop., 1960, v. 4, p. 497—504.
[49] Hubaut X. L. Designs et graphes de Schläfli. — Acid. Roy. Belg. Bull. Cl. Sci., 1972, v. 58, p. 622—624.
[50] Iwasaki S. A note on primitive extension of rank 3 of alternating groups.— J. Cac. Sci. Hokkaido Univ, Ser. 1, 1970, v. 21, p. 125—128.
[51] Kallaher M. J. On finite affine planes of rank 3. — J. Algebra, 1969, v. 3, p. 544—553.
[52] Lemmens P. W. H., Seidel J. J. Equiangular Lines. — J. Algebra, 1973, v. 24, p. 494—512.
[53] Lieber R. A. Finite affine planes of rank 3 are translation planes. — Math. Z., 1970, v. 116, p. 89—93.
[54] Mann H. B. Addition Theorems. — New York: Interscience, 1965.
[55] MacLaughlin J. A simple group of order 898,128,000. — In: Theory of Finite Groups. — New York: Benjamin, 1969, p. 109—111.
[56] Mesner D. M. A new family of partially balanced incomplete block designs with some Latin square design properties. — Ann. Math. Statist., 1967, v. 38, p. 571—581.
[57] Montague S. On rank 3 groups with a multiply transitive constituent. — J. Algebra, 1970, v. 14, p. 506—522.
[58] Primrose E. J. F. Quadratics in finite geometries. — Proc. Cambridge Philos. Soc., 1951, v. 47, p. 294—304.
[59] Ray-Chaudhuri D. K. Characterization of line graphs. — J. Combin. Theory, 1967,v. 3, p. 201—214.
[60] Ray-Chaudhuri D. K. On the application of the geometry of quadratics to the construction of partially balanced incomplete block design and error correcting codes. — Inst. Stat. Mimeo. Ser. no. 230, Univ. of N. Carolina, 1959.
[61] Ray-Chaudhuri D. K. Some results on quadratics in finite geometry. — Can. J. Math., 1962, v. 14, p. 120—130.
[62] Rudvalis A. (v, k, λ)-graphs and polarities of (v, k, λ) designs. — Math. Z., 1971, v. 120, p. 224—230.
[63] Shult E. The graph extension theorem. — Proc. Amer. Math. Soc., 1972, v. 33, p. 278—284.
[64] Shult E. Supplement to «The graph extension theorem.». — Univ. of Florida, Gainesville, Fla. (mimeographied notes), 1972.
[65] Seidel J. J. Strongly regular graphs of L_2-type and of triangular type. — Indag. Math., 1967, v. 29, p. 188—196.
[66] Seidel J. J. Strongly regular graphs with (—1, 1, 0) adjacency matrix having eigenvalue 3 — Linear Algebra and Appl., 1968, v. 1, p. 281—298.
[67] Seidel J. J. Strongly regular graphs. — Proc. 3rd Waterloo Conf. on Combinatorics. — New York: Academic Press. 1969, p. 185—198.
[68] Seitz G. Small rank permutation representations of finite Chevalley groups. — J. Algebra, 1974, v. 28, p. 508—517.
[69] Shrikhande S. S. The uniqueness of the L_2 association scheme. — Ann. Math. Statist., 1959, v. 30, p. 781—798.
[70] Shrikhande S. S., Bath V. N. Non isomorphic solution of pseudo (3, 5, 2) and pseudo (3, 6.3) graphs. — Ann. New York Acad. Sci., 1970, v. 175, p. 331—350.
[71] Sims C. C. Graphs and finite permutation groups. — Math. Z., 1967, v. 95, p. 76—86.
[72] Sims C. C. On the isomorphism of two groups of order 44,352,000, — In: Theory of Finite Groups. — New York: Benjamin, 1969.
[73] Sims C. C. On graphs with rank 3 automorphism groups (не опубликовано).
[74] Smith M. On a class of rank three permutation groups. — J. Algebra,1975, v. 33, p. 22—42.

[75] Suzuki M. A simple group of order 448, 345, 497, 600. — In: Theory of Finite Groups. — New York: Benjamin, 1969, p. 113—119.
[76] Taylor D. E. Some topics in the theory of finite groups. — Ph. D. Thesis, Oxford, 1971.
[77] Tits J. Le groupe de Janko d'ordre 604, 800. — In: Theory of Finite Groups. — New York: Benjamin, 1969, p. 91—96.
[78] Tits J. Groupes finis sporadiques. — Sem. Bourbaki No. 375, 1970.
[79] Tsuzuku T. On primitive extensions of rank 3 of symmetric groups. — Nagoya Math. J., 1966, v. 27, p. 171—178.
[80] van Lint J. H., Seidel J. J. Equilateral point sets in elliptic geometry. — Indag. Math., 1966, v. 28, p. 335—348.
[81] Wales D. Uniqueness of the graph of a rank 3 group. — Proc. J. Math., 1969, v. 30, p. 271—276.
[82] Wallis W. D. Some non isomorphic graphs. — J. Comb. Th.. 1970, v. 8, p. 448—449.
[83] Wallis W. D. A non-existence theorem for (v, k, λ)-graphs. — J. Aust. Math. Soc., 1970, v. 11, p. 381—383.
[84] Wallis W. D. Construction of strongly regular graphs using affine designs. — Null. Austr. Math. Soc., 1971, v. 4, p. 41—49.
[85] Wan Zhe-Xian. Studies in finite geometries and the construction of incomplete block designs, I, II. Some «Anzahl» theorems in symplectic geometry over finite fields. — Acta. Math. Sin., 1965, v. 15, p. 354—361; 362—371.
[86] Wan Zhe-Xian. Yang Ben-Fu. Studies in finite geometries and the construction of incomplete block designs, III. Some «Anzahl» theorems in unitary geometry over finite fields and their applications. — Acta. Math. Sin., 1965, v. 15, p. 533—544.
[87] Yang Ben-Fu. Studies in finite geometries and the construction of incomplete block designs, VII. An association scheme with many associate classes constructed from maximal completely isotropic subspaces in symplectic geometry over finite fields.—Acta. Math. Sin., 1965, v. 15, p. 812—825.
[88] Yang Ben-Fu. Studies in finite geometry and the construction of incomplete block designs, VIII. An association scheme with many associate classes constructed from maximal completely isotropic subspaces in unitary geometry over finite fields. — Acta. Math. Sin., 1965, v. 15, p. 825—841.

Сильно регулярные графы и частичные геометрии[1)]

А. Е. Браувер, Й. Х. ван Линт

Приводится обзор недавних результатов, касающихся построения, единственности и несуществования сильно регулярных графов и частичных геометрий. В основном мы ограничиваемся изложением результатов, не нашедших отражения в хорошо известных ранее вышедших обзорах.

1. ВВЕДЕНИЕ

С тех пор как Боузом [4] были введены сильно регулярные графы и частичные геометрии, появилось несколько обзоров по теории таких графов и их построениям. По теории сильно регулярных графов самый последний обзор — это обзор Сейдела [63]. Относительно построений обычно ссылаются на обзор Юбо [45]. Бóльшая часть теории содержится также в статье Камерона [10] и книге Камерона и ван Линта [14]. Обзор по частичным геометриям, отражающий состояние дел на 1976 г., был написан Тасом [70]. Основная цель предлагаемой статьи состоит в кратком описании того, что было сделано после выхода этих обзоров.

Мы предполагаем, что читатель знаком с теорией сильно регулярных графов и более ранними обзорами, однако в целях достижения полноты приведем в этом введении несколько определений и теорем. Подробности читатель может найти в литературе.

Пусть X — конечное множество. *Схема отношений* с d классами есть пара $(X, \{R_0, R_1, \ldots, R_d\})$, такая, что

(i) $\{R_0, R_1, \ldots, R_d\}$ — разбиение множества $X \times X$,
(ii) $R_0 = \{(x, x) \mid x \in X\}$,
(iii) $R_i = R_i^T$ $(i = 0, 1, \ldots, d)$,

(iv) существуют числа p_{ij}^k (называемые *числами пересечений* схемы), такие, что для любой пары $(x, y) \in R_k$ справедливо

[1)] Brouwer A. E., van Lint J. H. Strongly regular graphs and partial geometries. — In: Enumerating and Design. Ed. by D. M. Jackson and S. A. Vanstone. — Academic Press, 1984, p. 85—122.

равенство $p_{ij}^k = |\{z \mid (x, z) \in R_i \text{ и } (z, y) \in R_j\}|$. Назовем $n_i := p_{ii}^0$ *валентностью* R_i и положим $v := |X| = \sum n_i$.

Сильно регулярный граф — это схема отношений с двумя классами. Точки из X суть вершины графа, а $\{x, y\}$ — его ребро, если $(x, y) \in R_1$. Мы будем использовать обозначение

$$\operatorname{srg}(v, k, \lambda, \mu), \quad \text{где} \quad v = |X|, \quad k = n_1, \quad \lambda = p_{11}^1, \quad \mu = p_{11}^2.$$

Граф, дополнительный к $\operatorname{srg}(v, k, \lambda, \mu)$, — это

$$\operatorname{srg}(v, l := v - k - 1, v - 2k + \mu - 2, v - 2k + \lambda).$$

(0, 1)-матрица смежности srg определяется следующим образом: $A(x, y) := 1$, если $\{x, y\}$ — ребро, и $A(x, y) := 0$ в противном случае. По определению имеем

$$AJ = kJ, \quad A^2 + (\mu - \lambda) A + (\mu - k) I = \mu J.$$

Большинство необходимых условий существования сильно регулярных графов было найдено при изучении собственных значений матрицы A и свойств трехмерной алгебры **A** линейных комбинаций матриц I, J и A (*алгебра Боуза — Меснера* рассматриваемого srg).

Пусть $E_j (0 \leqslant j \leqslant 2)$ — базис алгебры **A**, состоящий из минимальных идемпотентов. Рассматриваемая алгебра замкнута относительно покомпонентного умножения (обозначаемого через $\circ$). Определим числа q_{ij}^k следующим образом:

$$E_i \circ E_j = v^{-1} \sum_{k=0}^{2} q_{ij}^k E_k.$$

Отметим, что Дельсарт [26] ввел понятие *двойственности* для схем отношений (а следовательно, и для srg). Достаточным условием существования двойственного srg является наличие регулярной абелевой группы автоморфизмов. (Если srg имеет v вершин, валентности k и l и кратности f и g, то двойственный граф, если он существует, имеет v вершин, валентности f и g и кратности k и l.) Некоторые из упомянутых ниже сильно регулярных графов были найдены с использованием двойственности.

Необходимые условия

Выпишем некоторые необходимые условия существования сильно регулярного графа $\operatorname{srg}(v, k, \lambda, \mu)$. Мы исключаем из рассмотрения тривиальные графы (несвязные графы и их дополнения), т. е. мы предполагаем, что $0 < \mu < k < v - 1$. Из рассмотрения параметров дополнительного графа мы видим, что для существования srg необходимо выполнение неравенства

$v-2k+\mu-2\geqslant 0$. Это условие исключает, например, параметры $(v, k, \lambda, \mu)=(273, 256, 240, 240)$.

Условие целочисленности

Матрица A обладает собственным значением k с кратностью 1 и еще двумя собственными значениями r, $s (r>s)$, удовлетворяющими уравнению $x^2+(\mu-\lambda)x+(\mu-k)=0$. Кратность этих собственных значений равна

$$f=\frac{-k(s+1)(k-s)}{(k+rs)(r-s)} \quad \text{и} \quad g=\frac{k(r+1)(k-r)}{(k+rs)(r-s)},$$

и ясно, что они должны быть целыми. В действительности если $f\neq g$, то r и s должны быть целыми. Другую ситуацию (т. е. когда $f=g$) называют *половинным случаем*.

Частичным обращением сформулированного выше условия на собственные значения является следующая полезная теорема.

Теорема. *Регулярный связный граф является сильно регулярным в случае, если его матрица смежности имеет три собственных значения.*

Мы будем говорить, что набор параметров (v, k, λ, μ) *реализуем*, если для него выполнены сформулированные выше условия.

2. ЧАСТИЧНЫЕ ГЕОМЕТРИИ

Частичная геометрия $\mathrm{pg}(K, R, T)$ — это частичное линейное пространство $(X, \mathbf{L})$ с постоянным размером прямой, равным K (т. е. $|L|=K$ для $L\in\mathbf{L}$), причем каждая точка пространства лежит на R прямых и для заданных прямой L и точки $x\notin L$ имеется ровно T прямых, проходящих через x, которые пересекают прямую L. (Tac [70] использует обозначения $s+1=K$, $t+1=R$, $\alpha=T$.) Если $x\in L$, $y\in L$, то мы пишем $x\sim y$ и говорим, что эти точки коллинеарны. *Точечный граф* частичной геометрии имеет точки в качестве вершин, и пара $\{x, y\}$ является ребром, если $x\sim y$. Точечный граф геометрии $\mathrm{pg}(K, R, T)$ является сильно регулярным графом (быть может тривиальным) с параметрами

$$v=K\left(1+\frac{(K-1)(R-1)}{T}\right), \quad k=R(K-1),$$

$$\lambda=(K-2)+(R-1)(T-1), \quad \mu=RT, \quad r=K-1-T, \quad s=-R.$$

Отсюда следует, что из необходимых условий существования srg следуют необходимые условия существования pg.

Если srg обладает такими параметрами, что он мог бы быть точечным графом некоторой pg, то такой srg называется *псевдогеометрическим*; если он действительно является точечным графом некоторой pg, то говорят, что граф *геометрический*. Мы увидим, что псевдогеометрический srg не обязательно является геометрическим. Боуз [4] доказал следующую теорему.

Теорема. *Пусть* srg *псевдогеометрический и соответствует геометрии* pg(K, R, T). *Если при этом*

$$2K > R(R-1) + T(R+1)(R^2 - 2R + 2),$$

то граф геометрический. (В действительности отсюда следует, что либо $T = R$, либо $T = R - 1$.)

Частичные геометрии можно разделить на четыре класса:

1. Pg с $T = K$ (двойственно $T = R$) является 2-$(v, K, 1)$-*схемой* (*двойственной к ней схемой*).
2. Pg с $T = R - 1$ (двойственно $T = K - 1$) является *сетью* (*трансверсальной схемой*).
3. Pg с $T = 1$ называется *обобщенным четырехугольником*.
4. Если $1 < T < \min\{K - 1, R - 1\}$, то pg называется *собственной*.

Нас интересуют лишь обобщенные четырехугольники (обозначаемые через pg$(K, R, 1) = \mathrm{GQ}(K - 1, R - 1)$) и собственные частичные геометрии.

Обобщенные четырехугольники $\mathrm{GQ}(s, t)$ известны для параметров (s, t), равных соответственно $(q, 1)$, (q, q), (q, q^2), (q^2, q^3), $(q - 1, q + 1)$, и для двойственных наборов (q — степень некоторого простого числа). Собственные pg, описанные Тасом [70], имеют параметры

$$K = 2^h - 2^m + 1, \quad R = 2^h - 2^{h-m} + 1,$$

$$T = (2^m - 1)(2^{h-m} - 1), \quad 0 < m < h,$$

соответственно

$$K = 2^h, \quad R = 2^{h+m} - 2^h + 2^m, \quad T = 2^m - 1.$$

Несколько новых построений описано в разд. 11.

В приведенной ниже таблице выписаны параметры возможных частичных геометрий с $v < 100$ (за исключением схем, сетей и двойственных к ним); из пары двойственных наборов параметров мы приводим тот, для которого $K \leqslant R$.

v	k	λ	μ	K	R	T	
15	6	1	3	3	3	1	GQ(2, 2), граф $T(6)$*
27	10	1	5	3	5	1	GQ(2, 4), граф Шлэфли
28	15	6	10	4	5	2	pg не существует, см. разд. 11A
40	12	2	4	4	4	1	GQ(3, 3)
45	28	15	21	5	7	3	pg известна, см. разд. 11B
64	18	2	6	4	6	1	GQ(3, 5)
66	45	28	36	6	9	4	pg не существует, см. разд. 11B
70	42	23	28	7	7	4	pg неизвестна, но известно несколько графов
75	32	10	16	5	8	2	Граф неизвестен, см. разд. 11H
76	21	2	7	4	7	1	GQ(3, 6) не существует, см. разд. 11C
81	30	9	12	6	6	2	Спорадическая, см разд. 11D
85	20	3	5	5	5	1	GQ(4, 4)
91	66	45	55	7	11	5	pg неизвестна, граф $T(14)$*, см. разд. 11B
95	40	12	20	5	10	2	Граф неизвестен
96	35	10	14	6	7	2	Граф неизвестен
96	50	22	30	6	10	3	Граф неизвестен

3. РЕЗУЛЬТАТЫ ОТНОСИТЕЛЬНО НЕСУЩЕСТВОВАНИЯ

Следующие шесть необходимых условий существования исключают несколько возможных наборов параметров. В каждом случае мы приводим набор, который исключается этим условием, но не исключается никаким другим из приведенных условий. Это указывает на независимость всех шести условий.

A. Половинный случай (конференц-матрицы)

Если $f=g$, то мы имеем $v=4\mu+1$, $k=2\mu$, $\lambda=\mu-1$. Если существует такой srg, то имеется конференц-матрица C порядка $v+1$ (см. разд. 7B). Известно (см. [1, 51]), что такая матрица C существует лишь в случае, если v — сумма двух квадратов. Это условие исключает, например, набор $(v, k, \lambda, \mu)=(21, 10, 4, 5)$.

B. Условия Крейна

Нетрудно показать, что все числа q_{ij}^k должны быть неотрицательными (хотя не обязательно целыми). Путем непосредственного вычисления этих чисел мы получаем четыре так на-

зываемых условия Крейна [50, 60, 39, 26]). Два из этих условий всегда выполнены, а два нетривиальных ограничения следующие:

$$\text{Крейн 1: } q_{11}^1 = \frac{f^2}{v}\left(1 + \frac{r^3}{k^2} + \frac{(-1-r)^3}{l^2}\right) \geqslant 0,$$

$$\text{Крейн 2: } q_{22}^2 = \frac{g^2}{v}\left(1 + \frac{s^3}{k^2} + \frac{(-1-s)^2}{l^2}\right) \geqslant 0.$$

Эти условия могут быть записаны в следующем виде:

$$(r+1)(k+r+2rs) \leqslant (k+r)(s+1)^2,$$

$$(s+1)(k+s+2rs) \leqslant (k+s)(r+1)^2.$$

Они исключают, например, $(v, k, \lambda, \mu) = (184, 48, 2, 16)$.

C. Абсолютная граница

Подходящая линейная комбинация матриц I, A и J является матрицей Грама скалярных произведений набора векторов с двумя типами попарных расстояний, лежащих на сфере в $\mathbb{R}^f$. Поскольку такое множество может содержать самое большее $^1/_2 f(f+3)$ векторов (см. [49, 27, 63]), мы получаем $v \leqslant$ $\leqslant {}^1/_2 f(f+3)$ и аналогично $v \leqslant {}^1/_2 g(g+3)$. Это исключает, например, $(v, k, \lambda, \mu) = (50, 21, 4, 12)$.

Эту границу усилил следующим образом Ноймайер [58]: $v \leqslant {}^1/_2 f(f+1)$ при $q_{11}^1 \neq 0$. (Графы, для которых $q_{11}^1 = 0$ или $q_{22}^2 = 0$, называются графами Смит.) Эта граница исключает, например, $(v, k, \lambda, \mu) = (841, 200, 87, 35)$.

D. Граница, возникающая из рассмотрения лап

Боуз [4] первым изучал связь между сильно регулярными графами и частичными геометриями. При этом он вывел неравенство, которое мы упоминали в разд. 2. Эта идея была развита Ноймайером [57], а затем после улучшения, сделанного Браувером, приняла следующий вид:

$$\text{Если} \quad \mu \neq s^2, \quad \mu \neq s(s+1), \quad \text{то} \quad 2(r+1) \leqslant s(s+1)(\mu+1).$$

Идея состоит в том, чтобы показать, что если r достаточно велико, то srg — точечный граф некоторой частичной геометрии, а затем применить абсолютную границу и условия Крейна к графу прямых этой частичной геометрии. Условие исключает, например, $(v, k, \lambda, \mu) = (2058, 242, 91, 20)$.

E. Случай $\mu = 1$

Как было замечено Боузом и Доулингом [5], если $\mu = 1$, то множество соседей каждой точки является объединением $(\lambda + 1)$-клик. Следовательно, $(\lambda + 1) \mid k$. Это исключает, например, набор $(v, k, \lambda, \mu) = (726, 29, 4, 1)$. Общее число $(\lambda + 2)$-клик равно $vk/(\lambda + 1)(\lambda + 2)$, что должно быть целым. Это исключает, например, $(v, k, \lambda, \mu) = (209, 16, 3, 1)$.

F. Случай $\mu = 2$

Браувер и Ноймайер [8] заметили, что при $\mu = 2$ соседи каждой точки обладают структурой частичного линейного пространства с обхватом по меньшей мере 5. Отсюда следует, что если $k < {}^1/_2\lambda(\lambda + 3)$, то $(\lambda + 1) \mid k$. Это исключает, например, $(v, k, \lambda, \mu) = (736, 42, 8, 2)$. Удается получить некоторую дополнительную информацию, которая также исключает набор $(v, k, \lambda, \mu) = (1944, 67, 10, 2)$. Кроме приведенных выше шести необходимых условий мы упомянем еще несколько результатов.

G. Ограничение на μ

Комбинируя различные ограничения, Ноймайер [57] доказал, что $\mu \leqslant s^3(2s + 3)$, причем равенство достигается тогда и только тогда, когда $v = {}^1/_2 f(f + 3)$. Это очень удобное ограничение, но, поскольку оно следует из упомянутых выше ограничений, с его помощью нельзя получить новых результатов о несуществовании.

H. Спорадические результаты несуществования

Для двух указанных ниже графов несуществование было доказано с помощью некоторых специальных рассуждений. Первый из них имеет параметры $(v, k, \lambda, \mu) = (49, 16, 3, 6)$ (см. [9]), и в этом случае частично использовались результаты вычисления на ЭВМ. Второй набор — это $(v, k, \lambda, \mu) = (57, 14, 1, 4)$ (см. [73]). Доказательство основано на подсчете определенных подграфов. Более конкретно, показано, что как предположение о существовании 15-коклик в графе, так и обратное предположение приводят к противоречию. Эти два набора параметров были минимальными, для которых вопрос о существовании графа не мог быть решен с помощью других условий. В настоящее время первым открытым случаем является набор параметров $(v, k, \lambda, \mu) = (65, 32, 15, 16)$, отвечающий конференц-матрице порядка 66.

4. ОГРАНИЧЕНИЕ НА ПОДМНОЖЕСТВА

Хотя нас в первую очередь интересуют построения, нам представится возможность воспользоваться результатами более теоретического характера. Прежде всего мы имеем так называемые границы Хоффмана на размер клик и коклик в графе.

Теорема 1. *Пусть C — клика в сильно регулярном графе с параметрами $(v, k, \lambda, \mu, r, s)$. Тогда*

$$|C| \leqslant 1 + k/(-s),$$

причем равенство достигается тогда и только тогда, когда каждая вершина вне C смежна ровно с $\mu/(-s)$ вершинами из C.

Следствие. Предполагаем, что рассматривается псевдогеометрический граф с параметрами (K, R, T). Если мы найдем клики размера $K(=1+k/(-s))$, такие, что каждое ребро лежит ровно в одной такой клике, то граф геометрический (и $T=\mu/(-s)$).

Теорема 2. *Пусть C — коклика в сильно регулярном графе с параметрами $(v, k, \lambda, \mu, r, s)$. Тогда*

$$|C| \leqslant v(-s)/(k-s),$$

причем равенство достигается тогда и только тогда, когда каждая вершина вне C смежна ровно с $-s$ вершинами C.

В некоторых случаях граница Цветковича оказывается более точной.

Теорема 3. *Размер каждой коклики C в произвольном графе G не может превышать числа неотрицательных (неположительных) собственных значений G.*

Теорема 4 [36]. *Предположим, что для коклики C в сильно регулярном графе G достигаются обе приведенные выше границы, т. е.*

$$|C| = g = v(-s)/(k-s).$$

Тогда подграф в G, порожденный дополнением к C, сильно регулярный.

Вторая группа результатов относится к случаям достижения равенства в условии абсолютной границы и в условии Крейна. Приведем лишь одну теорему.

Теорема 5. *Пусть G — сильно регулярный граф, для которого $q^1_{11}=0$ или $q^2_{22}=0$. Тогда для каждой вершины x подграф соседей $\Gamma(x)$ $(=\{y \mid y \sim x\})$ и подграф несоседей $\Delta(x)$ $(=\{y \mid y \neq x,\ y \not\sim x\})$ являются сильно регулярными графами.*

5. РЕЗУЛЬТАТЫ, КАСАЮЩИЕСЯ ЕДИНСТВЕННОСТИ [1])

A. Треугольные графы

Треугольными графами $T(n)$ называют графы, вершины которых составляют пары элементов из множества $\{1, 2, \ldots, n\}$; две вершины смежны, если они имеют общий элемент. Эти графы имеют следующие параметры: $v=\binom{n}{2}$, $k=2(n-2)$, $\lambda=n-2$, $\mu=4$. Графы с такими параметрами единственны, если $n \neq 8$. При $n=8$ кроме $T(8)$ существуют еще ровно 3 графа с теми же параметрами — так называемые графы Чанга. Все четыре графа переключательно эквивалентны (см. [16, 17, 22, 42, 63]).

B. Решетчатые графы

Решетчатый граф $L(n)$ имеет в качестве вершин точки $(x, y) \in \{1, 2, \ldots, n\}^2$, две вершины соединены ребром, если совпадают первая или вторая координаты. Такие графы имеют параметры $v=n^2$, $k=2(n-1)$, $\lambda=n-2$, $\mu=2$. Если $n \neq 4$, то графы с такими параметрами единственны. Для $n=4$ кроме $L(4)$ существует еще один граф — так называемый граф Шрикханде. Эти два графа переключательно эквивалентны (см. [65]).

C. Графы с малым числом вершин

Все графы с числом вершин $v<25$ однозначно определяются своими параметрами, за исключением набора параметров $(16, 6, 2, 2)$, упомянутых выше. Кроме треугольных и решетчатых графов (и их дополнений) это множество включает графы Пэли порядка 5, 9, 13 и 17, а также граф Клебша с параметрами $(v, k, \lambda, \mu)=(16, 5, 0, 2)$.

---

[1]) Здесь и ниже единственность графа означает, что он однозначно характеризуется своими параметрами. — *Прим. перев.*

D. Спорадические графы

Для следующих наборов параметров известно, что существует единственный граф.

k	λ	μ	r	s	f	g	Имя	Единственность доказали
5	0	2	1	—3	10	5	Граф Клебша	Сейдел [61] Клэтуорси [18]
10	1	5	1	—5	20	6	Граф Шлэфли (GQ(2, 4))	Сейдел [61]
7	0	1	2	—3	28	21	Граф Хоффмана — Синглтона	Хоффман и Синглтон [43]
10	0	2	2	—4	35	20	Граф Симса — Гевиртца	Гевиртц [31, 32]
16	0	4	2	—6	55	21	Граф несоседей в HS (S(3, 6, 22))	Браувер [6]
22	0	6	2	—8	77	22	Граф Хигмана — Симса (HS)	Гевиртц [32]
30	2	10	2	—10	90	21	Граф соседей McL (GQ (3, 9))	Камерон, Гёталс и Сейдел [11]
56	10	24	2	—16	140	21	Граф несоседей McL	Камерон, Гёталс и Сейдел [11]
112	30	56	2	—28	252	22	Граф Маклафлина McL	Гёталс и Сейдел [34]

E. Геометрические графы

Камерон, Гёталс и Сейдел [11] показали, что псевдогеометрический граф, соответствующий $GQ(q, q^2)$, всегда геометрический. Это позволяет обосновывать единственность графа в случае, когда известно, что обобщенный четырехугольник единственный.

F. Регулярные два-графы

Два-граф есть набор Ω троек из множества X, такой, что каждое 4-подмножество из X содержит четное число троек из Ω. Относительно тесной связи между srg и два-графами, а также теории переключения см. статью Сейдела [62]. Регулярные два-графы на 16, 28 и 276 вершинах единственны [69, 34], и все они обладают транзитивной группой автоморфизмов. Изолируя точку путем переключения, а затем удаляя ее, мы получаем, что графы Шлэфли и Маклафлина единственны. Это также показывает, что все графы с параметрами $(v, k, \lambda, \mu) = (16, 6, 2, 2)$, $(28, 12, 6, 4)$, $(276, 135, 78, 54)$ переключательно эквивалентны. Для $v = 16$ см. разд. 5B, для $v = 28$ см. разд. 5A, для $v = 276$ известен единственный граф.

6. СИЛЬНО РЕГУЛЯРНЫЕ ГРАФЫ, НАЙДЕННЫЕ ПОСРЕДСТВОМ СКЛЕЙКИ КЛАССОВ В СХЕМАХ ОТНОШЕНИЙ [1])

А. Схема Джонсона

В схеме Джонсона $\binom{n}{3}$ скажем, что две тройки смежны, если они имеют ровно одну общую точку. Если $n=7$ или $n=10$, отношение смежности определяет srg. (При $n=7$ это граф прямых пространства $PG(3, 2)$, а для $n=10$ граф имеет параметры $v=120$, $k=63$, $\lambda=30$, $\mu=36$.)

В схеме Джонсона $\binom{n}{4}$ скажем, что две четверки смежны, если они имеют либо три общие точки, либо ни одной общей точки. При $n=9$ и $n=11$ это определяет srg. Параметры графов следующие: $v=126$, $k=25$, $\lambda=8$, $\mu=4$ и $v=330$, $k=63$, $\lambda=24$, $\mu=9$ соответственно. В схеме Джонсона $\binom{12}{4}$ назовем две четверки смежными, если они имеют либо две общие точки, либо ни одной общей точки. Это приводит к srg(495, 238, 109, 119). Эти графы были найдены Мэтоном [55a] [2]).)

---

[1]) Схемы отношений (в частности, сильно регулярные графы), возникающие путем склейки классов в тех или иных схемах отношений, систематически изучались в работах советских математиков. См. обзоры: Клин М. Х., Фараджев И. А. Метод V-колец в теории групп подстановок и его комбинаторные применения. — В кн.: Исследования по прикладной теории графов. — ВЦ СО АН СССР, Новосибирск, 1986, с. 59—97; Иванов А. А., Клин М. Х., Фараджев И. А. Соответствие Галуа между группами подстановок и клеточными кольцами (схемами отношений). — В кн.: Баннаи Э., Ито Т. Алгебраическая комбинаторика. Схема отношений. — М.: Мир, 1987, с. 331—367. — *Прим. перев.*

[2]) Схемы отношений, получаемые склеиванием классов в схемах Джонсона, систематически исследованы М. Х. Клином в его диссертации: Клин М. Х. Исследование алгебр инвариантных отношений некоторых классов групп подстановок. — Канд. дисс., Николаев, НКИ, 1974; в статье: Клин М. Х. Рассмотрение на ЭВМ «Мир-1» исключительных случаев в задаче о максимальности индуцированных симметрических групп. — В сб.: Вычисления в алгебре и комбинаторике. — Киев: ИК АН УССР, 1978, с. 54—72. Им найдены все графы, описанные в этом подразделе, а также граф с параметрами $(v, k, \lambda, \mu) = (1716, 833, 400, 408)$, получаемый из схемы Джонсона $\binom{13}{6}$ путем соединения шестерок, имеющих 0, 1 или 3 общие точки. Там же приводится доказательство того, что графы со 120 и 330 вершинами, получаемые из схем Джонсона $\binom{10}{3}$ и $\binom{11}{4}$, не являются графами ранга 3. Выдвигается гипотеза, что других сильно регулярных графов путем склеивания классов в схемах Джонсона получить нельзя. Эта гипотеза подтверждается вычислениями, проведенными В. А. Устименко-Бакумовским, который с этой точки зрения изучил схемы Джонсона $\binom{n}{m}$ для $n \leqslant 60$, $m \leqslant 20$ (см. Устименко-Бакумовский В. А. Алгоритмы построения блок-схем и сильно регулярных графов с заданной группой автоморфизмов. — В сб.: Вычисления в алгебре и комбинаторике. — Киев: ИК АН УССР, 1978, с. 137—148). — *Прим. перев.*

В. Схемы Хэмминга

В схеме Хэмминга 4^n назовем два вектора смежными, если расстояние между ними четно. Это приводит к srg с параметрами $v=2^{2n}$, $k=2^{2n-1}+\varepsilon 2^{n-1}$, $\lambda=\mu=2^{2n-2}+\varepsilon 2^{n-1}$, где $\varepsilon=(-1)^{n-1}$. Если n четно, этот граф имеет те же параметры, что граф прямых ортогонального массива (или трансверсальной схемы) OA$(2^n, 2^{n-1})$, однако при $n>2$ эти графы неизоморфны. В любом случае они имеют параметры графов в серии Юбо C_{12}.

В схеме Хэмминга 3^n скажем, что два различных вектора находятся в i-м отношении, если расстояние между ними сравнимо с i по модулю 3 ($i=1, 2, 3$). Это приводит к схеме отношений с 3-классами. Если n четно, то склейка любых двух из этих классов приводит к srg. Параметры следующие: пусть $n=2m$, тогда $v=3^{2m}$.

(a) Вершины смежны в точности тогда, когда расстояние сравнимо с нулем по модулю 3 (но не равно нулю):

$$k=3^{2m-1}+(-1)^m\cdot 2\cdot 3^{m-1}-1;$$
$$\lambda=3^{2m-2}+(-1)^m\cdot 2\cdot 3^{m-1}-2;$$
$$\mu=3^{2m-2}+(-1)^m\cdot 3^{m-1}.$$

(b) Вершины смежны в точности тогда, когда расстояние сравнимо с 1 по модулю 3 (соответственно вершины смежны в точности тогда, когда расстояние сравнимо с 2 по модулю 3):

$$k=3^{2m-1}-(-1)^m\cdot 3^{m-1};$$
$$\lambda=3^{2m-2};$$
$$\mu=4\cdot 3^{2m-2}+(-1)^m\cdot 3^{m-1}-2$$

(см. [46]).

Доказательство этого факта, более простое, чем приведенное в [46], может быть получено с использованием того, что собственные значения схемы Хэмминга вычисляются через многочлены Кравчука. Из хорошо известных соотношений для этих многочленов следует, что указанная склейка приводит к ситуации, когда имеются лишь три различных собственных значения, и поэтому может быть применена теорема из разд. 1. (Вес вектора, взятый по модулю 3, равен значению квадратичной формы $Q(x)=\sum x_i^2$. Отсюда сразу видно, что два графа в случае (b) изоморфны и что в случае (a) граф изоморфен графу из серии C_{12} в каталоге Юбо [1]).)

[1]) Серия srg, получаемых склеванием классов в схеме Хэмминга 4^n, получена М. Х. Клином в статье: Клин М. Х. Об одном методе построения примитивных графов. — Николаев: Тр. НКИ, 1974, № 87, с. 3—8.

Полное исследование схем отношений (и, в частности, сильно регулярных

C. Циклотомическая схема

Пусть $q = p^{(e-1)t}$, тогда p — простое число, t — четное число, e — простое число, большее 2, причем p примитивно по модулю e. Скажем, что два элемента x и y из поля $\mathbb{F}_q$ находятся в j-м отношении $(0 < j \leqslant e)$, если $x - y = \alpha^{ei+j}$ для некоторого i, где α — фиксированный примитивный элемент поля $\mathbb{F}_q$. Тогда каждое отношение в этой схеме отношений является сильно регулярным графом (более того, графом ранга 3) типа отрицательных латинских квадратов, а объединение u классов является srg с параметрами

$$v = q, \quad k = \frac{q-1}{e} u,$$
$$\lambda = (u^2 q - 3ue + u^2 - (e-u)(e-2u) q^{1/2})/e^2,$$
$$\mu = (u^2 q - ue + u^2 + u(e-2u) q^{1/2})/e^2,$$
$$r = (-1 + q^{1/2}) u/e, \quad s = r - q^{1/2},$$
$$f = (q-1)(e-u)/e, \quad g = k$$

(см. [52]).

Более общо, можно выбрать число q, являющееся степенью некоторого простого числа, делитель e числа $q - 1$ и сказать, что два элемента x и y из $\mathbb{F}_q$ находятся в j-м отношении $(0 < j \leqslant e)$, если $x - y = \alpha^{ei+j}$ для некоторого i. В некоторых случаях объединение классов приводит к srg. Это имеет место в следующих примерах:

$$q = 81, \quad e = 8, \quad v = 81, \quad k = 30, \quad \lambda = 9, \quad \mu = 12 \quad [52, 56],$$

графов), получаемых склеиванием классов в схемах Хэмминга 3^n и 4^n, проведено В. А. Устименко-Бакумовским в статье, указанной в сноске на стр. 186, а также в статьях: Устименко-Бакумовский В. А. Сильно регулярные графы, инвариантные относительно групп $[\mathfrak{S}_n]^{\mathfrak{S}_m}$ при $n \geqslant 3$. — В сб.: Вычисления в алгебре и комбинаторике. — Киев: ИК АН УССР, 1978, с. 101—113 и Устименко-Бакумовский В. А. О группах автоморфизмов сильно регулярных графов, инвариантных относительно экспоненцирования симметрических групп. — В сб.: Вычисления в алгебре, теории чисел и комбинаторике. — Киев: ИК АН УССР, 1980, с. 59—72. Им получены все серии сильно регулярных графов, представленные в этом разделе, и доказано, что нельзя получить никаких схем путем склеивания классов в схеме Хэмминга n^m при $n \geqslant 5$.

В диссертации В. А. Зайченко (Алгоритмический подход к синтезу комбинаторных объектов и вычислениям в группах подстановок на основе метода инвариантных отношений. — Канд. дисс. М., МФТИ, 1981) найдены все схемы, получаемые склеиванием классов в схемах Хэмминга 2^m при $m \leqslant 16$. На основе этих результатов В. А. Зайченко и В. А. Устименко описали пять бесконечных серий таких схем. Наконец, М. Е. Музычук дал полное описание всех схем (в том числе srg), получаемых склеиванием классов в схемах Хэмминга 2^m (Музычук М. Е. Подсхемы схемы Хэмминга. — В сб.: Исследования по алгебраической теории комбинаторных объектов. — М.: ВНИИСИ, 1985, с. 49—65.). — *Прим. перев.*

$q = 243$, $e = 11$, $v = 243$, $k = 22$, $\lambda = 1$, $\mu = 2$ [3],

$v = 243$, $k = 110$, $\lambda = 37$, $\mu = 60$ [2] (граф — двойственный к предыдущему),

$q = 256$, $e = 15$, $v = 256$, $k = 68$, $\lambda = 12$, $\mu = 20$ (Браувер, неопубликовано).

D. Другие примеры

Пусть q — степень двойки. Группа $PSL(2, q)$ действует как группа ранга $^1/_2q$ на множестве из $^1/_2q(q-1)$ прямых вне гиперовала в $PG(2, q)$. Соответствующая схема отношений имеет валентности $n_0 = 1$, $n_i = q + 1 (1 \leqslant i \leqslant {}^1/_2q - 1)$. Под действием большей группы $P\Sigma L(2, q)$ некоторые из классов склеиваются, и Холлман [44] заметил, что при $q = 16$ получается схема отношений с 3-классами и с валентностями 1, 17, 34, 68, причем склейка отношений R_1 и R_2 приводит к srg с параметрами $v = 120$, $k = 51$, $\lambda = 18$, $\mu = 24$. (Очень похоже, что этот граф изоморфен члену, отвечающему $q = 4$ в серии, построенной Метцом и рассмотренной в разд. 7A [1].)

Группа $PGL(2, 8)$ действует 2-транзитивно на 28 точках унитали Ри с параметрами $S(2, 4, 28)$. При этом $PSL(2, 8)$ действует как группа ранга 4 и определяет схему отношений с параметрами $v = 28$, $n_1 = n_2 = n_3 = 9$,

$$p^1_{ij} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 2 & 4 & 2 \\ 0 & 4 & 2 & 3 \\ 0 & 2 & 3 & 4 \end{pmatrix}, \quad p^i_{jk} = p^{i+1}_{j+1,\, k+1} \text{ для } \{i, j, k\} \subset \{1, 2, 3\}.$$

Здесь сложение по модулю 3. Униталь — это набор 4-подмножеств с собственной раскраской, т. е. в каждый цвет окрашены два ребра, не имеющие общих вершин. Вторая схема отношений с теми же параметрами может быть получена из предыдущей путем переключения относительно блока в унитали; ее группа автоморфизмов — элементарная абелева группа порядка 8. Это единственные схемы с такими параметрами [44]. Собственные

[1]) Эти графы действительно изоморфны. Дело в том, что группа $PSp(4, 4)$, действующая как группа ранга три на графе из серии Метца ($q = 4$), содержит два класса сопряженности подгрупп $PSL(2, 16)$. Представитель одного класса — стабилизатор вершины, а представитель второго действует транзитивно на множестве прямых вне гиперовала в $PG(2, 16)$ (см., например, Fischer J., McKay J. The nonabelian simple groups G, $|G| < 10^6$ — maximal subgroups. — Math. Comput., 1978, v. 32, p. 1293—1302). Поэтому граф Метца можно получить склейкой некоторых классов в схеме отношений, связанной с упомянутым представлением группы $PSL(2, 16)$. Как выясняется, такая склейка единственна. — *Прим. перев.*

значения у этой схемы следующие:

$$P=\begin{pmatrix} 1 & 9 & 9 & 9 \\ 1 & \lambda_1 & \lambda_2 & \lambda_3 \\ 1 & \lambda_3 & \lambda_1 & \lambda_2 \\ 1 & \lambda_2 & \lambda_3 & \lambda_1 \end{pmatrix},$$

где λ_i — корни уравнения $\lambda^3+\lambda^2-9\lambda-1=0$ [53].

Рассмотрим теперь прямое произведение этих двух схем. Получим схему отношений с 15-классами. При этом отношения задаются правилом

$$R_{ij}=\{(xx',\ yy')\,|\,(x,\ y)\in R_i \text{ и } (x',\ y')\in R_j\}$$

и имеют в качестве собственных значений числа μ_i, μ_j, где μ_i (соответственно μ_j) пробегают множество собственных значений отношения R_i (соответственно R_j). Можно проверить, что $R_{11}\cup R_{22}\cup R_{33}$ имеет собственные значения

$$3n^2=243,\quad (\lambda_1+\lambda_2+\lambda_3)=-9,\quad \lambda_1^2+\lambda_2^2+\lambda_3^2=19 \text{ и}$$
$$\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_2\lambda_3=-9,$$

т. е. мы нашли сильно регулярный граф.

Аналогично $R_{11}\cup R_{22}\cup R_{33}\cup R_{10}\cup R_{20}\cup R_{30}$ обладает собственными значениями 270, 18 и -10, а $R_{11}\cup R_{22}\cup R_{33}\cup R_{10}\cup R_{20}\cup R_{30}\cup R_{01}\cup R_{02}\cup R_{03}$ имеет сообственные значения 297, 17 и -11.

Таким образом, мы нашли сильно регулярные графы со следующими параметрами:

v	k	λ	μ	r	s	f	g
784	243	82	72	19	-9	243	540
784	270	98	90	18	-10	270	513
784	297	116	110	17	-11	297	486

Это построение провел Мэтон (частное сообщение), и оно применимо к более общему классу псевдоциклических схем отношений с 3-классами. Получаемые графы имеют параметры графов латинских квадратов; причем параметры новые лишь в случае, когда v не является степенью простого числа.

Положим $p^1_{1j}=(1\ t-r-s-1\ s\ r)$ и $n_j=t$. Тогда каждая псевдоциклическая схема отношений SPC(r, s, t) на $v=3t+1$ точках порождает три сильно регулярных графа на v^2 точках с параметрами $k=3t^2+3it$, $r=2t+1-i$, $s=-t-i$ $(i=0,\ 1,\ 2)$. Холлманн построил SPC$(50, 58, 165)$ на 496 точках

(см. [44]), поэтому мы получаем новые графы на 246 016 вершинах [1]).

Симметрическая группа S_9 действует как группа ранга 5 на 280 разбиениях девятиэлементного множества на три тройки (валентности 1, 27, 36, 54 и 162). Граф (X, R_4) является сильно регулярным с параметрами (280, 162, 96, 90) [55b] [2]).

7. СИЛЬНО РЕГУЛЯРНЫЕ ГРАФЫ, НАЙДЕННЫЕ ИСХОДЯ ИЗ КЛАССИЧЕСКИХ ГРУПП И ГЕОМЕТРИЙ

А. Конструкция Метца

Пусть Q — невырожденная эллиптическая квадрика в $PG(5, q)$. Пусть p — точка, а Π — гиперплоскость, такие, что p не лежит ни на Q, ни на Π. Пусть $V := \{x \in \Pi \mid px$ пересекает Q в двух точках$\}$, $\mathbf{L} := \{l \mid l$ — прямая в Π, такая, что плоскость $\langle p, l\rangle$ пересекается с Q по двум пересекающимся прямым$\}$, $\mathbf{I} := \{(x, l) \mid x \in l\}$. Тогда $(V, \mathbf{L}, I)$ — получастичная геометрия с параметрами $s + 1 = q$, $t + 1 = q^2 + 1$, $\alpha = 2$, $\mu = 2q(q-1)$. (Определение получастичной геометрии см. в [25].) Точечный граф этой геометрии является сильно регулярным с параметрами

$$v = \frac{1}{2} q^2 (q^2 - 1), \quad k = (q-1)(q^2+1), \quad \lambda = (q-1)(q+2),$$

$$\mu = 2q(q-1), \quad r = q - 1, \quad s = -(q-1)^2,$$

$$f = \frac{1}{2}(q-2)(q+1)(q^2+1), \quad g = \frac{1}{2} q (q^2 + 1).$$

Приведенное выше описание принадлежит, по-видимому, Хиршфелду и Тасу; Метц предложил следующее описание (от-

---

[1]) В работе Фараджева И. А. (Клеточные подкольца симметрического квадрата клеточного кольца ранга 3. — В сб.: Исследования по алгебраической теории комбинаторных объектов. — М.: ВНИИСИ, 1985, с. 76—95) решается сходная задача, а именно дается полное описание параметров схем (в частности, сильно регулярных графов), получаемых склеиванием классов в симметрическом декартовом квадрате схемы отношений с 2-классами. — *Прим. перев.*

[2]) В работе Иванова А. А., Клина М. Х., Фараджева И. А. (Примитивные представления неабелевых простых групп порядка меньше 10^6. Ч. 2 (Препринт). — М.: ВНИИСИ, 1984) приведены результаты систематического исследования схем, получаемых склеиванием классов в схемах отношений, возникающих из примитивных представлений неабелевых простых групп порядка меньше 10^6. Там, в частности, построено шесть новых сильно регулярных графов с параметрами (v, k, λ, μ), равными (144, 39, 6, 12), (231, 30, 9, 3), (280, 36, 8, 4), (280, 117, 44,52), (280, 135, 70, 60), (506, 208. 72, 80), которые связаны с группами $PSL(3,3)$, M_{22}, J_2, A_9, J_2, $Sz(8)$. При этом второй граф независимо построен Камероном (см. разд. 10А), а четвертый граф — дополнительный к упомянутому выше графу, построенному Мэтоном и Розой. — *Прим. перев.*

носительно обсуждения изоморфизма между этими описаниями см. статью [24]). Пусть Q — невырожденная квадрика в $PG(4, q)$. Пусть V — множество гиперплоскостей, пересекающих Q по эллиптической квадрике. Если $x, y \in V$, то положим $x \sim y$, если соответствующие эллиптические квадрики касаются друг друга. (При этом прямые можно определить как пучки попарно касающихся квадрик.) Это представление группы $\Omega(5, q)$ является представлением ранга 3 при $q = 4, 8$.

В. Вариация, предложенная Браувером и Вильбринком

Пусть Q — невырожденная квадрика в $PG(4, q)$, и пусть V — множество гиперплоскостей, пересекающихся с Q по гиперболической квадрике. Если $x, y \in V$, то положим $x \sim y$, если соответствующие гиперболические квадрики касаются друг друга (т. е. если $x \cap y \cap Q$ состоит из двух пересекающихся прямых). Это определяет сильно регулярный граф с параметрами

$$v = \frac{1}{2} q^2 (q^2 + 1), \quad k = (q + 1)(q^2 - 1),$$

$$\lambda = (q - 1)(3q + 2), \quad \mu = 2q(q + 1),$$

$$r = q^2 - 2q - 1, \quad s = -q - 1, \quad f = \frac{1}{2} q(q + 1)^2,$$

$$g = \frac{1}{2}(q - 2)(q + 1)(q^2 + 1).$$

Снова имеются прямые (пучки попарно касающихся квадрик) и $s + 1 = q$, $t + 1 = (q + 1)^2$. Здесь мы получаем не получастичную геометрию, а структуру, в которой для заданных точки p и прямой l, таких, что $p \notin l$, имеются 0, 2 или q точек на l, соединенных с p. Для нечетных q дополнительный граф является псевдогеометрическим и отвечает $pg(^1/_2(q^2 + 1), q(q - 2), {}^1/_2(q - 1)^2 - 1)$. В этом графе действительно удается найти клики размера $^1/_2(q^2 + 1)$. Пусть E — эллиптическая прямая (т. е. $E \cap Q = \varnothing$). Положим $C_E := \{x \in V \mid E^\perp \subset x$ или $E \subset x\}$. Тогда C_E — клика размера $^1/_2(q^2 + 1)$. Число таких эллиптических прямых E равно $^1/_2 q^3 (q - 1)(q^2 + 1)$, и для $q > 3$ каждая C_E определяет E однозначно, так что мы получаем для частичной геометрии слишком много клик, и оказывается, что невозможно выбрать подходящее подсемейство. Однако при $q = 3$ каждая C_E принадлежит 10 различным прямым E, и мы находим 27 наборов C_E, что приводит к частичной геометрии $pg(5, 3, 1)$. Это, конечно же, хорошо известный обобщенный четырехугольник $GQ(4, 2)$, что иллюстрирует спорадический изоморфизм $PSU(4, 2) \simeq \Omega(5, 3)$.

C. Обобщение предыдущих двух конструкций

Вильбринк заметил, что описанные выше два построения в действительности работают во всех размерностях. Итак, пусть Q — невырожденная квадрика в $\mathrm{PG}(2m, q)$. Пусть V — множество гиперплоскостей, пересекающих Q по гиперболической (эллиптической) квадрике. Пусть $\varepsilon = +1(-1)$. Пусть $x, y \in V$, тогда $x \sim y$, если соответствующие квадрики касаются друг друга (т. е. если пересечение $Q \cap x \cap y$ вырождено). Этим определяется сильно регулярный граф с параметрами

$$v = \frac{1}{2} q^m (q^m + \varepsilon), \quad k = (q^m - \varepsilon)(q^{m-1} + \varepsilon),$$

$$\lambda = 2(q^{2m-2} - 1) + \varepsilon q^{m-1}(q - 1),$$

$$\mu = 2q^{m-1}(q^{m-1} + \varepsilon),$$

$$r,\ s = -\varepsilon q^{m-1} - 1 \quad \text{и} \quad \varepsilon q^{m-1}(q - 2) - 1.$$

D. Другое построение Вильбринка

Пусть Q — невырожденная квадрика в $\mathrm{PG}(2m, 5)$. Пусть V — множество неизотропных точек x, таких, что $x^{\perp}$ пересекает Q по *гиперболической* (*эллиптической*) квадрике. Пусть $\varepsilon = \pm 1$, и пусть $x, y \in V$, тогда $x \sim y$, если $x \perp y$. Этим определяется сильно регулярный граф с параметрами

$$v = \frac{1}{2} 5^m (5^m + \varepsilon), \quad k = \frac{1}{2} 5^{m-1} (5^m - \varepsilon),$$

$$\lambda = \frac{1}{2} 5^{m-1} (5^{m-1} + \varepsilon), \quad \mu = \frac{1}{2} 5^{m-1} (5^{m-1} - \varepsilon),$$

$$r,\ s = 2\varepsilon 5^{m-1}, \quad -\varepsilon 5^{m-1}.$$

E. Конструкция Тейлора

Пусть H — эрмитова форма на проективной плоскости $\mathrm{PG}(2, q^2)$, где q — степень нечетного простого числа, и $U = \{x \mid H(x, x) = 0\}$ — соответствующая униталь. Тогда $|U| = q^3 + 1$. Мы можем определить на U два-граф, выбрав те тройки $\{x, y, z\}$, для которых $H(x, y) H(y, z) H(z, x)$ является в $\mathrm{GF}(q^2)$ квадратом, если $q \equiv 3 \pmod 4$, и неквадратом, если $q \equiv 1 \pmod 4$. Изолировав точку ∞ посредством переключения, а затем удалив ее, мы получим сильно регулярный граф с параметрами

$$v = q^3, \quad k = 2\mu = \frac{1}{2}(q - 1)(q^2 + 1), \quad \lambda = \frac{1}{4}(q - 1)^2 - 1,$$

$$r = \frac{1}{2}(q - 1), \quad s = -\frac{1}{2}(q^2 + 1),$$

$$f = (q - 1)(q^2 + 1), \quad g = q(q - 1).$$

(Это серия C_{20} в каталоге Юбо.) Отметим, что коллинеарные тройки унитали содержатся в два-графе, поэтому после переключения для каждой прямой l, проходящей через ∞, множество $l \setminus \{\infty\}$ становится кликой. Следовательно, наш граф допускает разбиение на клики размера q (при этом достигается граница Хоффмана), такие, что каждая вершина вне клики смежна в точности с $^1/_2(q-1)$ вершинами из этой клики. Следовательно, если мы возьмем объединение любых $^1/_2(q^2+1)$ таких клик, то получим регулярный подграф степени $^1/_4(q-1)(q^2+3)$. Тогда добавление новой точки Ω и переключение приводят к сильно регулярному графу с параметрами

$$v = q^3 + 1, \quad k = \frac{1}{2} q (q^2 + 1),$$

$$\lambda = \frac{1}{4}(q-1)(q^2+3), \quad \mu = \frac{1}{4}(q+1)(q^2+1),$$

$$r = \frac{1}{2}(q-1), \quad s = -\frac{1}{2}(q^2+1), \quad f = (q-1)(q^2+1),$$

$$g = q^2 - q + 1.$$

Мыслимо существование другого srg в переключательном классе рассматриваемого регулярного два-графа. Он бы имел параметры

$$k = \frac{1}{2} q^2 (q-1), \quad \lambda = \frac{1}{4}(q^2+1)(q-3), \quad \mu = \frac{1}{4}(q-1)(q^2-1).$$

Для $q = 3$ такого графа не существует (для него нарушается условие абсолютной границы). При $q = 5$ такой граф был построен Гёталсом (см. разд. 10B, посвященный графу Хоффмана — Синглтона). Для бóльших q такие графы неизвестны. Отметим, что при $q = 3^{2n+1}$ дважды транзитивное представление на $q^3 + 1$ точках имеют группы Ри. Это представление приводит к регулярному два-графу с теми же параметрами, что и два-граф, связанный с группой $P\Gamma U(3, q^2)$ и обсуждавшийся выше. Этот два-граф вновь приводит к srg на q^3 вершинах (а быть может, и на $q^3 + 1$ вершинах).

F. Конструкция Кантора

Пусть V — векторное пространство над $GF(q)$, снабженное симплектической, ортогональной или унитарной геометрией. *Накрытие* пространства V — это семейство Σ максимальных вполне изотропных или сингулярных пространств, которые образуют разбиение множества P вполне изотропных или сингулярных точек.

Построим граф, выбрав за вершины множество Ω всех гиперплоскостей, составленных из элементов множества Σ; две различные вершины X, Y соединим ребром, если $X \cap Y^{\perp} \neq 0$. Этот граф сильно регулярен и имеет те же параметры, что и граф, вершины которого составляют точки из P, а ребра — пары перпендикулярных точек. Это построение и его вариации приводят к большому количеству неизоморфных сильно регулярных графов [46].

8. КОМБИНАТОРНЫЕ КОНСТРУКЦИИ

А. Конструкция Хэмерса

Пусть $q = 2^n$, и пусть K — гиперовал в $PG(2, q)$ (рассматриваемый как гиперплоскость в бесконечности пространства $AG(3, q)$). Пусть V — множество прямых в $AG(3, q)$, для которых точка на K является точкой на бесконечности. Для x, $y \in V$ положим $x \sim y$, если x и y пересекаются (как аффинные точки). Это определяет сильно регулярный граф с параметрами

$$v = q^2(q+2), \quad k = q(q+1), \quad \lambda = \mu = q,$$

$$r = q, \quad s = -q, \quad f = \left(\frac{1}{2}q + 1\right)(q^2 - 1), \quad g = \frac{1}{2}q(q+1)^2.$$

(Это семейство C_{18} в каталоге Юбо.) В действительности если построить геометрию, в которой роль прямых играют пучки прямых исходного пространства, то это будет геометрия $GQ(q+1, q-1)$. Теперь $q+2$ классов параллельных прямых разобьем произвольным образом на $^1/_2q + 1$ пар: $k = \bigcup_{i=1}^{q/2+1} \{u_i, v_i\}$. Переопределим смежность таким образом, что для каждого i две прямые в направлении u_i (соответственно v_i) смежны тогда и только тогда, когда плоскость, ими порожденная, проходит через точку v_i (соответственно u_i). Смежность между остальными вершинами мы сохраним. Это приводит к новому сильно регулярному графу с параметрами

$$v = q^2(q+2), \quad k = q^2 + q - 1, \quad \lambda = q - 2, \quad \mu = q,$$

$$r = q - 1, \quad s = -(q+1), \quad f = \frac{1}{2}(q+2)(q^2 + q - 1),$$

$$g = \frac{1}{2}q(q^2 + q - 1).$$

В. Конструкция Мэтона

Симметрическая конференц-матрица порядка n — это матрица C с нулевой диагональю и элементами ± 1 вне диагонали, причем $C = C^T$ и $CC^T = (n-1)I$. Необходимым условием существования такой матрицы является выполнение сравнения

$n \equiv 2 \pmod 4$. Сильно регулярный граф, параметры которого отвечают половинному случаю ($v-1=2k=4\mu$), существует тогда и только тогда, когда существует симметрическая конфереиц-матрица порядка $v+1$. (Если дана такая матрица, то следует нормализовать ее таким образом, что первая строка и первый столбец содержат только 0 и $+1$, а затем удалить эти строку и столбец. Если обозначить полученную матрицу через B, то $A := {}^1/_2(B+J-I)$ будет матрицей смежности некоторого srg, причем этот процесс можно осуществить в обратном порядке.) Известно существование симметрической конференц-матрицы порядка n в следующих случаях (см. дополнение C [72]):

(i) $n=q+1$, где q — степень простого числа и $q \equiv 1 \pmod 4$;

(ii) $n=(h-1)^2+1$, где h — порядок кососимметричной матрицы Адамара;

(iii) $n=(m-1)^a+1$, где m — порядок некоторой симметрической конференц-матрицы, a — произвольное неотрицательное целое число.

Мэтон предложил новую рекурсивную конструкцию для симметрических конференц-матриц, доказав, что если $q=4t-1$ — степень простого числа и существует симметрическая конференц-матрица порядка $q+3$, то существует симметрическая конференц-матрица порядка $q^2(q+2)+1$ (см. [54] или [64]). На этом пути, в частности, получается srg(45, 22, 10, 11).

C. Конструкция Гёталса и Сейдела

Пусть N — матрица инцидентности некоторой системы Штейнера $S(2, K, V)$ размера V на B. Пусть H — матрица Адамара порядка $R+1$. Нормализуем матрицу H таким образом, чтобы первый столбец содержал только единицы, и отбросим этот столбец. Обозначим через $\mathbf{L}$ полученную матрицу размера $R+1$ на R (при этом $J\mathbf{L}=0$). Пусть P — матрица размера $(R+1)V$ на B, полученная из N заменой каждой строки на $R+1$ строк по следующему правилу: все R единиц в каждой строке заменяются на R столбцов матрицы $\mathbf{L}$, а нули — на нулевые столбцы. Пусть $PP^T = RI + A$. Тогда

$$(A+RI)(A-(V+K-1)I)=0, \quad AJ=-RJ$$

(см. [61]). Отсюда следует, что ${}^1/_2(J-I-A)$ — матрица смежности некоторого srg с параметрами

$$v=(R+1)V, \quad k=\frac{1}{2}(v-1+R), \quad \lambda=\frac{1}{4}(R-1)(V+K+2),$$

$$\mu=\frac{1}{4}(R+1)(V+K), \quad r=\frac{1}{2}(R-1), \quad s=-\frac{1}{2}(V+K),$$

$$f=v-1-g, \quad g=B=RV/K.$$

(Это параметры псевдогеометрического графа, отвечающего $\mathrm{pg}(R+1, {}^1/_2(V+K), {}^1/_2(R+1))$, однако $\mathrm{pg}(4,5,2)$ не существует, поэтому такие графы не могут быть всегда геометрическими.)

D. Регулярные симметрические матрицы Адамара с постоянной диагональю

Предположим, что H — регулярная симметрическая матрица Адамара порядка n с постоянной диагональю, т. е.

$$HH^T = nI, \quad H = H^T, \quad HJ = aJ, \quad h_{ij} \in \{\pm 1\}, \quad h_{ii} = \varepsilon$$
$$(1 \leqslant i,\ j \leqslant n).$$

(Тогда ясно, что $n = a^2$.) При этом ${}^1/_2(J - I - H + \varepsilon I)$ — матрица смежности некоторого srg с параметрами

$$v = n, \quad k = \frac{1}{2}(n - 1 - a + \varepsilon), \quad \lambda = \frac{1}{4}(n - 2a) - (1 - \varepsilon),$$
$$\mu = \frac{1}{4}(n - 2a).$$

Очевидно, заменяя в случае необходимости H на $-H$, мы можем считать, что $a > 0$. Кроме того, если $n > 1$, то $4 \mid n$, и поэтому можно записать $a = 2t$. Это приводит к следующим параметрам:

Если $\varepsilon = +1$, то $v = 4t^2$, $k = 2t^2 - t$, $\lambda = \mu = t^2 - t$,
$r, s = \pm t$, $f = 2t^2 - t$, $g = 2t^2 + t - 1$.

(Это параметры графа псевдолатинского квадрата $L_t(2t)$.)

Если $\varepsilon = -1$, то $v = 4t^2$, $k = 2t^2 - t - 1$, $\lambda = t^2 - t - 2$,
$\mu = t^2 - t$, $r = t - 1$, $s = -t - 1$,
$f = 2t^2 + t$, $g = 2t^2 - t - 1$.

(Это параметры графа отрицательного латинского квадрата $\mathrm{NL}_t(2t)$.) Верно и обратное, а именно граф с этими параметрами приводит к симметрической матрице Адамара с постоянной диагональю. Ввиду сказанного выше нас интересует множество пар (n, ε), для которых существует такая матрица (с положительной суммой элементов в строке). Назовем такое множество RSHCD. Тогда имеется следующая рекуррентная конструкция:

$$(m, \delta),\ (n, \varepsilon) \in \mathrm{RSHCD} \to (mn, \delta\varepsilon) \in \mathrm{RSHCD}.$$

Кроме того, известны следующие прямые построения:

(i) $(4, \pm 1)$, $(36, \pm 1) \in \mathrm{RSHCD}$.

(ii) Если существует матрица Адамара порядка m, то $(m^2, 1) \in$ $\in$ RSHCD.

(iii) Если и $a-1$, и $a+1$ — нечетные простые числа, то $(a^2, 1) \in$ RSHCD.

(iv) Если $a+1$ — степень простого числа и существует симметрическая конференц-матрица порядка a, то $(a^2, 1) \in$ RSHCD.

(v) Если существует набор из $t-2$ попарно ортогональных латинских квадратов порядка $2t$ (т. е. трансверсальная схема $T[t; 2t]$), то $(4t^2, 1) \in$ RSHCD.

(vi) Предположим, что имеется система Штейнера $S(2, K, V)$, где $V = K(2K-1)$. Если мы рассмотрим граф на множестве блоков и добавим изолированную точку, то получим граф, который содержится в переключательном классе некоторого регулярного два-графа. Соответствующая матрица Адамара является симметрической с постоянной диагональю, однако не регулярна (как утверждается в [72, стр. 454]). Если, кроме того, рассматриваемая система Штейнера инвариантна относительно некоторой регулярной абелевой группы автоморфизмов (эта группа имеет на множестве блоков орбиты длин V и $2K-1$), то, проводя переключение относительно орбиты на множестве блоков размера V, мы получаем srg с параметрами

$$v = 4K^2, \quad k = V = K(2K-1), \quad \lambda = \mu = K(K-1).$$

Отсюда следует, что $(4K^2, 1) \in$ RSHCD. Система Штейнера $S(2, K, K(2K-1))$ известна для $K = 3, 5, 6, 7$ или 2^t, однако только для $K = 2, 3, 5, 7$ известно, что такие системы обладают регулярными абелевыми группами автоморфизмов. Таким образом, $(196, 1) \in$ RSHCD. (В случае, когда схема разрешима, в качестве требуемого множества для переключения можно выбрать K параллельных классов. Разрешимые схемы известны лишь для $K = 3, 2^t$.)

Большинство конструкций, описанных в этом разделе, принадлежит Гёталсу и Сейделу [33]; более подробно см. [72, разд. 5.3].

9. ПРЕДСТАВЛЕНИЯ РАНГА 3 ДЛЯ КОНЕЧНЫХ ГРУПП

Представления ранга 3 конечных классических групп описаны Кантором и Либлером [48]. Их основной результат формируется следующим образом (мы цитируем):

Теорема 1. *Пусть M — одна из групп $\mathrm{Sp}(2m-2, q)$, $\Omega^{\pm}(2m, q)$, $\Omega(2m-1, q)$ или $\mathrm{SU}(m, q)$ для $m \geqslant 3$ и q — степень простого числа. Пусть $M \trianglelefteq G$, где $G/Z(M) \leqslant \mathrm{Aut}(M/Z(M))$. Предположим, что G действует как примитивная группа подстановок ранга 3 на множестве X смежных классов по подгруппе*

K в G. Тогда с точностью до сопряженности в группе $\mathrm{Aut}(M/Z(M))$ *выполнено (по крайней мере) одно из следующих положений:*

(i) *X — некоторая орбита группы M на множестве сингулярных (или изотропных) точек.*

(ii) *X — некоторая орбита группы M на множестве максимальных вполне сингулярных (или изотропных) подпространств и* $M = \mathrm{Sp}(4, q)$, $\mathrm{SU}(4, q)$, $\mathrm{SU}(5, q)$, $\Omega^-(6, q)$, $\Omega^+(8, q)$ *или* $\Omega^+(10, q)$.

(iii) *X — некоторая орбита группы M на множестве несингулярных точек и* $M = \mathrm{SU}(m, 2)$, $\Omega^\pm(2m, 2)$, $\Omega^\pm(2m, 3)$ *или* $\Omega(2m-1, 3)$.

(iv) *X — либо орбита группы* $M = \Omega(2m-1, 4)$, *либо* $\Omega(2m-1, 8)$ *(где в последнем случае* $G = \Gamma O(2m-1, 8)$*) на множестве несингулярных гиперплоскостей.*

(v) $M = \mathrm{SU}(3, 3)$, $K \cap M = \mathrm{PSL}(3, 2)$.

(vi) $M = \mathrm{SU}(3, 5)$, $K \cap M = 3.A_7$.

(vii) $M = \mathrm{SU}(4, 3)$, $K \cap M = 4.\mathrm{PSL}(3, 4)$.

(viii) $M = \mathrm{Sp}(6, 2)$, $K = G_2(2)$.

(ix) $M = \Omega(7, 3)$, $K \cap M = G_2(3)$.

(x) $M = \mathrm{SU}(6, 2)$, $K \cap M = 3.\mathrm{PSU}(4, 3).2$.

Теорема 2. *Пусть* $M = \mathrm{PSL}(n, q) \leqslant G \leqslant \mathrm{Aut}\, M$. *Предположим, что G действует как примитивная группа подстановок ранга 3 на множестве X смежных классов некоторой подгруппы K в G. Тогда с точностью до сопряженности в* $\mathrm{Aut}\, M$ *выполнено (по крайней мере) одно из следующих положений:*

(i) *X — множество прямых для M, $n \geqslant 4$.*

(ii) $M = \mathrm{PSL}(2, 4) \simeq \mathrm{PSL}(2, 5)$, $|X| = \binom{5}{2}$,

$M = \mathrm{PSL}(2, 9) \simeq A_6$, $|X| = \binom{6}{2}$,

$G = \mathrm{PSL}(4, 2) \simeq A_8$, $|X| = \binom{8}{2}$, *или*

$G = \mathrm{P\Gamma L}(2, 8)$, $|X| = \binom{9}{2}$.

(iii) $M = \mathrm{PSL}(3, 4)$, $M \cap K = A_6$.

(iv) $M = \mathrm{PSL}(4, 3)$, $M \cap K = \mathrm{PSp}(4, 3)$.

Мы предупреждаем читателя, что изоморфизмы между различными группами и автоморфизмы групп позволяют смотреть на некоторые из случаев с различных точек зрения. В особенности изоморфизмы $\mathrm{PSp}(4, q) \simeq \Omega(5, q)$, $\mathrm{PSU}(4, q) \simeq \mathrm{P}\Omega^-(6, q)$, $\mathrm{PSL}(4, q) \simeq \mathrm{P}\Omega^+(6, q)$ и $\mathrm{PSU}(4, 2) \simeq \mathrm{PSp}(4, 3)$ приводят к многочисленным представлениям в случае теоремы 1(i). Аналогично тройственный автоморфизм группы $\mathrm{P}\Omega^+(8, q)$ можно применить в случае 1(iii), а в случае 2(i) можно применить полярность.

Не все из этих подстановочных представлений упомянуты в обзоре Юбо, однако представляется, что новых графов не возникло. (О параметрах графов в случае 1(iv) для произвольного q см. разд. 7С — конструкция Вильбринка.)

Ф. Зара [75] любезно предоставил нам параметры двух представлений ранга 3 групп Фишера, которые не упомянуты в каталоге Юбо:

v	k	l	λ	μ	$\bar{\lambda}$	$\bar{\mu}$	G	G_0
14 080	10 920	3 159	8 408	8 680	918	648	Fi_{22}	$O^+(7,3)$
137 632	109 200	28 431	86 600	86 800	6 030	5 832	Fi_{23}	$(O^+(8,3))' \cdot S_3$

(Здесь $O^+(n,3)$ — подгруппа ортогональной группы, порожденная отражениями $x \to x + (x, a)a$, где $(a, a) = 1$.) [1])

10. НЕКОТОРЫЕ СПОРАДИЧЕСКИЕ ГРАФЫ

А. Семейство Хигмана — Симса

Почти все спорадические графы построены тем или иным способом, исходя из системы Штейнера $S(5, 6, 12)$ или $S(5, 8, 24)$ либо исходя из бинарного или тернарного кода Го-

[1]) В самое последнее время по модулю классификации конечных простых групп получено полное описание групп (и графов) ранга 3. А именно хорошо известно, что если G — примитивная группа ранга 3 и степени n, то верно одно из следующих положений:

(i) $T \times T \lhd G \leqslant T_0 \wr Z_2$, где T_0 — 2-транзитивная группа степени n_0, минимальный делитель T группы T_0 является простой группой и $n = n_0^2$;

(ii) G — аффинная группа, т. е. G обладает регулярной элементарной абелевой нормальной подгруппой и n — степень простого числа;

(iii) минимальный нормальный делитель L группы G является простой группой.

Описание групп в случае (i) можно получить, исходя из классификации 2-транзитивных групп подстановок; их список приведен, например, в статье: Cameron P. J. Finite permutation groups and finite simple groups. — Bull. London Math. Soc., 1981, v. 13, p. 1—22.

Полное описание групп ранга 3 из п. (ii) получено в работе: Liebeck M. W. The affine permutation groups of rank three. — Preprint, Univ. Cambridge, 1984.

В случае (iii), если L — знакопеременная группа, то описание получено в статье: Bannai E. Maximal subgroups of low rank of finite symmetric and alternative groups. — J. Fac. Sci. Univ. Tokyo, 1972, v. 18, p. 475—486; представление ранга 3 для классических групп получено в цитируемой выше статье Кантора и Либлера; наконец, случай, когда L — исключительная группа типа Ли или спорадическая группа, полностью разобран в работе: Liebeck M. W., Saxl J. The finite primitive permutation groups of rank three. — Preprint, Univ. Cambridge. 1986. — *Прим. перев.*

лея. (Другими словами, все графы, описанные в этом разделе, можно так или иначе найти в решетке Лича.) Начнем с графов, получаемых из системы Штейнера $S(3, 6, 22)$.

(i) $(v, k, \lambda, \mu) = (77, 16, 0, 4)$.

В качестве вершин следует взять блоки (единственной) системы $S(3, 6, 22)$ и соединить две вершины ребром в случае, когда блоки не пересекаются. Это приводит к сильно регулярному графу с указанными выше параметрами. (Этот граф единственный [6].)

(ii) $(v, k, \lambda, \mu) = (56, 10, 0, 2)$ — граф Гевиртца.

Предыдущий граф содержит коклику размера 21 (т. е. на ней достигаются и граница Хоффмана, и граница Цветковича), а именно все блоки, содержащие фиксированную точку. Удаление этой коклики приводит к сильно регулярному графу с приведенными выше параметрами. Впервые этот граф был найден Симсом (неопубликовано), а его единственность была доказана Гевиртцем [31]. Добавление единичной матрицы к матрице смежности этого графа приводит к $2-(56, 11, 2)$-схеме (биплоскости). Эта конструкция работает всегда, когда $\mu = \lambda + 2$; при $\mu = \lambda$ сам граф уже является симметричной блок-схемой. Вскоре мы встретимся с примером, когда граф строится, исходя из блок-схемы (допускающей полярность).

(iii) $(v, k, \lambda, \mu) = (100, 22, 0, 6)$ — граф Хигмана — Симса.

Возьмем символ ∞, 22 точки и 77 блоков системы $S(3, 6, 22)$. Соединим ∞ с 22 точками, точку с блоками, ее содержащими, и два блока, если они не пересекаются. Это приводит к графу с указанными выше параметрами. Его единственность доказана Гевиртцем [32]. Простая группа Хигмана — Симса является подгруппой индекса два в группе автоморфизмов описанного графа.

(iv) $(v, k, \lambda, \mu) = (231, 30, 9, 3)$ — граф Камерона.

Возьмем в качестве вершин $\binom{22}{2} = 231$ неупорядоченную пару точек системы $S(3, 6, 22)$. Соединим две вершины ребром, если соответствующие пары не пересекаются, а их объединение содержится в некотором блоке. Это приводит к графу с указанными параметрами (см. [11]). Можно ввести прямые как тройки попарно пересекающихся пар, таких, что их объединение является блоком рассматриваемой схемы. Полученная таким образом геометрия является, по терминологии Хигмана, гамма-пространством, т. е. если x — точка вне прямой L, то x соединена с 0, 1 или со всеми точками из L (как это было замечено

в [8a] и [10a]).

(v) $(v, k, \lambda, \mu) = (176, 49, 12, 14)$.

(Может быть, этот граф не относится к настоящему разделу — например, для него 2 не является собственным значением.) Пусть x_0 и x_1 — две фиксированные точки из множества точек системы $S(5, 8, 24)$. Построим симметрическую схему, точками которой являются блоки, содержащие x_0, но не содержащие x_1, а в качестве блоков — блоки, содержащие x_1, но не содержащие x_0. Точка B инцидентна блоку B' тогда и только тогда, когда $|B \cap B'| \in \{0, 4\}$. Прямая проверка показывает, что в результате получается $2-(176, 50, 14)$-схема. Эта схема была впервые построена Хигманом [40]; приведенная конструкция принадлежит Маргарет Смит [67]. Эта схема имеет в точности две полярности, одна с 176 и одна с 80 фиксированными точками [66, 7]. Используя полярность первого типа, можно записать матрицу инцидентности A как симметрическую матрицу с постоянной диагональю. Тогда $A - I$ является матрицей смежности требуемого сильно регулярного графа. Для этого графа S_8 является группой автоморфизмов. Вопрос единственности не решен. Детальное обсуждение геометрии Хигмана и ее связь с графом Хоффмана — Синглтона см. в статье [5a].

B. Семейство Хоффмана — Синглтона

Мур показал, что граф валентности k и обхвата $2d+1$ может иметь самое большее $1 + k + k(k-1) + \ldots + k(k-1)^{d-1}$ вершин. (Аналогичную границу можно получить и в случае четного обхвата.) Графы, для которых достигается эта граница, называются графами Мура. При $d = 2$ мы получаем $v \leqslant k^2 + 1$, и непосредственно видно, что если достигается равенство, то граф является сильно регулярным (с $\lambda = 0$ и $\mu = 1$). Набор параметров $(k^2 + 1, k, 0, 1)$ допустим только для $k = 2, 3, 7$ и 57, и мы получаем для $k = 2$ пятиугольник, для $k = 3$ — граф Петерсена $T(5)^*$, для $k = 7$ — граф Хоффмана — Синглтона, обсуждаемый ниже, а случай $k = 57$ пока остается открытым.

(i) $(v, k, \lambda, \mu) = (50, 7, 0, 1)$ — граф Хоффмана — Синглтона.

Пусть $X = \{\infty\} \cup \mathbf{P} \cup \mathbf{B}$ — множество вершин графа Хигмана — Симса, описанного выше. Пусть B_0 — блок, не содержащий точку Ω в системе $S(4, 7, 23)$ с множеством точек $\mathbf{P} \cup \{\Omega\}$, причем исходная схема $(\mathbf{P}, \mathbf{B})$ является производной схемой по точке Ω. Тогда B_0 индуцирует следующее разбиение множества

вершин графа Хигмана — Симса:

$$X = (\{\infty\} \cup B_0 \cup \{B \in \mathbf{B} \mid |B \cap B_0| = 1\}) \cup (\mathbf{P} \setminus B_0 \cup \cup \{B \in \mathbf{B} \mid |B \cap B_0| = 3\}).$$

Можно проверить, что

(a) Подграф, индуцированный каждым подмножеством из разбиения X, изоморфен графу Хоффмана — Синглтона.

(b) Любое разбиение графа Хигмана — Симса на два графа Хоффмана — Синглтона может быть получено таким образом. (Граф Хоффмана — Синглтона был впервые построен Хоффманом и Синглтоном [43]; они же доказали его единственность. То, что граф Хигмана — Симса содержит две копии графа Хоффмана — Синглтона, по-видимому, впервые было замечено Симсом [66].)

Обратно, можно следующим образом определить граф Хигмана — Симса в терминах графа Хоффмана — Синглтона. Граф Хоффмана — Синглтона содержит 100 коклик размера 15. Две такие коклики пересекаются по 0, 3, 5, 8 или 15 точкам. Это определяет схему отношений с 4-классами (отношения: R_0 — диагональ, R_1, R_2, R_3, R_4 — пересечение мощности 8, 5, 3, 0 соответственно) со следующими параметрами: $v = 100$, $n_0 = 1$, $n_1 = 15$, $n_2 = 42$, $n_3 = 35$, $n_4 = 7$,

$$(p_{0j}^{(i)}) = I_5,$$

$$(p_{1j}^{i}) = \begin{pmatrix} 0 & 15 & 0 & 0 & 0 \\ 1 & 0 & 14 & 0 & 0 \\ 0 & 5 & 0 & 10 & 0 \\ 0 & 0 & 12 & 0 & 3 \\ 0 & 0 & 0 & 15 & 0 \end{pmatrix}, \quad (p_{2j}^{i}) = \begin{pmatrix} 0 & 0 & 42 & 0 & 0 \\ 0 & 14 & 0 & 28 & 0 \\ 1 & 0 & 35 & 0 & 6 \\ 0 & 12 & 0 & 30 & 0 \\ 0 & 0 & 36 & 0 & 6 \end{pmatrix},$$

$$(p_{3j}^{i}) = \begin{pmatrix} 0 & 0 & 0 & 35 & 0 \\ 0 & 0 & 8 & 20 & 7 \\ 0 & 10 & 0 & 25 & 0 \\ 1 & 0 & 30 & 0 & 4 \\ 0 & 15 & 0 & 20 & 0 \end{pmatrix}, \quad (p_{4j}^{i}) = \begin{pmatrix} 0 & 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 7 & 0 \\ 0 & 0 & 6 & 0 & 1 \\ 0 & 3 & 0 & 4 & 0 \\ 1 & 0 & 6 & 0 & 0 \end{pmatrix},$$

$$P = \begin{pmatrix} 1 & 15 & 42 & 35 & 7 \\ 1 & -15 & 42 & -35 & 7 \\ 1 & 0 & -3 & 0 & 2 \\ 1 & 5 & 2 & -5 & -3 \\ 1 & -5 & 2 & 5 & -3 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 1 & 56 & 21 & 21 \\ 1 & -1 & 0 & 7 & -7 \\ 1 & 1 & -4 & 1 & 1 \\ 1 & -1 & 0 & -3 & 3 \\ 1 & 1 & 16 & -9 & -9 \end{pmatrix}$$

Эта схема импримитивна: граф (X, R_4) есть объединение двух непересекающихся графов Хоффмана — Синглтона. Граф (X, R_1) является регулярным тонким почти октагоном и одно-

значно определяется своими параметрами. Поскольку $(X, R_1 \cup R_4)$ имеет только три собственных значения, этот граф является сильно регулярным и мы вновь приходим к графу Хигмана — Симса. Можно построить систему из трех «сцепленных» графов Хоффмана — Синглтона на 150 вершинах, взяв вершины и каждое из двух множеств по 50 коклик; соединим вершины очевидным способом. Тогда каждое из трех множеств по 100 точек в этом графе индуцирует граф Хигмана — Симса.

Для дальнейших целей упомянем две другие конструкции графа Хоффмана — Синглтона.

(ii) Первая конструкция принадлежит Робертсону [59]. Пусть P_α $(\alpha \in \mathbb{F}_5)$ — пять пятиугольников, а Q_β $(\beta \in \mathbb{F}_5)$ — пять пятиконечных звезд. Занумеруем точки в P_α и Q_β элементами поля $\mathbb{F}_5$ таким образом, что точки в P_α смежны тогда и только тогда, когда их разность равна 1, а в Q_β — тогда и только тогда, когда эта разность равна 2. Проведем ребро между точкой i из P_α и точкой j из Q_β в случае, если $j = i + \alpha\beta$. Это приводит к графу Хоффмана — Синглтона.

Следствие. Множество точек графа Хоффмана — Синглтона можно расщепить на две половины таким образом, что подграф, индуцированный на каждой половине, есть объединение пяти пятиугольников. Объединение двух пятиугольников из разных половин индуцирует ровно одно такое расщепление, поэтому имеется 126 таких расщеплений. Каждое такое расщепление определяет 25 подграфов Петерсена, и любые два расщепления однозначно определяют единственный общий подграф Петерсена. Это приводит к $2-(126, 6, 1)$-схеме, для которой точки — это подграфы Петерсена, а блоки — всевозможные расщепления. Оказывается, что эта схема является классической униталью в пространстве $PG(2, 5^2)$, что позволяет отождествлять группу автоморфизмов графа Хоффмана — Синглтона с группой $P\Sigma U(3, 5^2)$ [2]. Половины двух расщеплений пересекаются по 10 или 15 вершинам. Зафиксируем вершину x и построим граф, вершины которого составляют расщепления, и два расщепления соединены ребром, если те их половины, которые содержат x, пересекаются по 10 вершинам исходного графа. Полученный граф является srg с параметрами $(v, k, \lambda, \mu) = (126, 50, 13, 24)$. Другая конструкция этого графа приведена в п. (vii).

(iii) Вторая конструкция использует хорошо известный факт, что прямые $PG(3, 2)$ можно отождествлять с тройками из фиксированного семиэлементного множества таким образом, что пересекающимся прямым отвечают тройки, имеющие ровно один общий элемент.

Пусть C — множество точек, а D — множество прямых в PG(3, 2). Тогда $|C|=15$ и $|D|=35$. Соединим ребрами прямую с точками, лежащими на ней, и две прямые, если соответствующие тройки не пересекаются. Это приводит к графу Хоффмана — Синглтона.

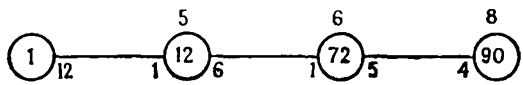
(iv) $(v, k, \lambda, \mu)=(175, 72, 20, 36)$ и новая частичная геометрия.

На 175 ребрах графа Хоффмана — Синглтона (сокращенно Ho — Si) имеется схема отношений с тремя классами (отношения: R_0 — диагональ, R_1 — пересечение, R_2 — вместе лежат в пятиугольнике, R_3 — остальные), причем группа Aut(Ho — Si) действует на этом множестве ребер как группа ранга 4. Параметры следующие:

$$(p^i_{0j})=I_4,\quad (p^i_{1j})=\begin{pmatrix} 0 & 12 & 0 & 0 \\ 1 & 5 & 6 & 0 \\ 0 & 1 & 6 & 5 \\ 0 & 0 & 4 & 8 \end{pmatrix},$$

$$(p^i_{2j})=\begin{bmatrix} 0 & 0 & 72 & 0 \\ 0 & 6 & 36 & 30 \\ 1 & 6 & 20 & 45 \\ 0 & 4 & 36 & 32 \end{bmatrix},\quad (p^i_{3j})=\begin{bmatrix} 0 & 0 & 0 & 90 \\ 0 & 0 & 30 & 60 \\ 0 & 5 & 45 & 40 \\ 1 & 8 & 32 & 49 \end{bmatrix}.$$

Граф, отвечающий отношению R_1, является дистанционно-транзитивным диаметра 3 с диаграммой



и собственными значениями 12^1, 7^{28}, 2^{21}, $(-2)^{125}$; это есть реберный граф графа Хоффмана — Синглтона. (В действительности таковым является любой дистанционный регулярный граф с параметрами i (12, 6, 5; 1, 1, 4). Это следует из того, что, поскольку $\mu=1$, каждое ребро содержится в единственной 7-клике; всего имеется 50 таких 7-клик, и непосредственно проверяется, что граф на этих 7-кликах изоморфен графу Ho — Si.)

Граф, отвечающий отношению R_2, является сильно регулярным с параметрами $(v, k, \lambda, \mu)=(175, 72, 20, 36)$ и собственными значениями 72^1, 2^{153}, $(-18)^{21}$.

Хэмерс [36] заметил, что этот граф обладает структурой частичной геометрии pg(5, 18, 2). Нам надо найти 630 прямых размера 5, т. е. 630 клик мощности 5. Однако 5-клика — это набор из 5 ребер в графе Ho — Si, которые попарно лежат в

одном пятиугольнике. Такие 5 ребер индуцируют в Ho — Si подграф Петерсена. Граф Ho — Si содержит 525 подграфов Петерсена, в то же время граф Петерсена содержит 6 паросочетаний, т. е. граф Ho — Si содержит 3150 5-клик, и мы должны выбрать из них пятую часть таким образом, чтобы каждый пятиугольник определял единственный специальный граф Петерсена. Чтобы сделать это, обозначим через C 15-коклику в Ho — Si и рассмотрим множество вершин графа Ho — Si как объединение $C \cup D$. Заметим следующее:

(1) Каждая из 35 вершин, содержащихся в D, имеет три соседа в C, и мы можем рассматривать C и D как точки и прямые проективного пространства $PG(3, 2)$, как это описано выше.

(2) Из 1260 пятиугольников имеется 630, которые содержат одну вершину из C, и 630, которые содержат две такие вершины. Положим $\mathbf{P}_i = \{$пятиугольники, содержащие i вершин из множества $C\}$ $(i = 1, 2)$.

(3) Стабилизатор множества C в группе $\mathrm{Aut}(\mathrm{Ho} - \mathrm{Si})$ изоморфен A_7 и действует транзитивно на каждом множестве из 630 пятиугольников.

(4) Имеется взаимно однозначное отображение Π из $\mathbf{P}_2$ в $\mathbf{P}_1$, инвариантное относительно действия указанной выше группы, такое, что $P_2 \cup \Pi P_2$ индуцирует граф Петерсена P, такой, что три вершины из $P \cap C$ имеют единственного соседа. (Действительно, если $P_2 \cap C = \{x, y\}$, то прямая $L = xyz$ является вершиной из P_2, поэтому P_2 вместе с ребром Lz определяет подграф Петерсена P. Теперь $P \cap C = \{x, y, z\} \subset \Gamma(L)$.)

(5) Имеется 105 таких специальных графов Петерсена, причем каждый может быть представлен в виде $P_1 \cup P_2$ шестью способами. Каждый из графов Петерсена содержит 6 паросочетаний, и, таким образом, мы находим требуемые 630 прямых.

Построенная таким образом частичная геометрия допускает A_7 в качестве группы автоморфизмов.

(v) $(v, k, \lambda, \mu) = (630, 85, 20, 10)$.

Из доказанного выше существования $pg(5, 18, 2)$ в силу двойственности следует существование $pg(18, 5, 2)$. Точечный граф последний и обладает указанными параметрами.

(vi) $(v, k, \lambda, \mu) = (176, 70, 18, 24)$ и $(v, k, \lambda, \mu) = (176, 90, 38, 54)$.

Для графа, построенного в п. (iv), выполнено равенство $k = 2\mu$, поэтому добавление к нему изолированной вершины приводит к некоторому регулярному два-графу на 176 вершинах. В переключательном классе этого два-графа содержатся сильно ре-

гулярные графы с приведенными наборами параметров. Для того чтобы построить эти графы, мы должны указать подходящие множества, по которым производится переключение. В нашем случае — это регулярные подграфы в графе на 175 вершинах, имеющие 70 (соответственно 90) вершин и валентность 18 (соответственно 38). В первом случае выбор такого подграфа производят естественным образом: в представлении графа Но — Si в виде $C \cup D$, которое использовалось выше, на множестве D имеется 70 ребер, а R_2 в этом множестве из 70 ребер имеет валентность 18. Во втором случае Хэмерс указал следующую возможность. Рассмотрим множество из 18 попарно пересекающихся 5-клик. Поскольку на этих кликах достигается граница Хоффмана, каждая вершина вне клики смежна ровно с двумя вершинами внутри клики. Отсюда это объединение клик имеет валентность $4+17\cdot 2=38$. Такие непересекающиеся 5-клики действительно существуют, поскольку из представления графа Но — Si, предложенного Робертсоном, непосредственно следует существование 25 попарно непересекающихся 5-клик.

(vii) $(v, k, \lambda, \mu)=(126, 50, 13, 24)$.

Если мы удалим из графа Но — Si вершину x и всех ее соседей, то получим граф, имеющий 42 вершины и 126 ребер. Гёталс заметил, что если в графе на 175 вершинах, описанном в п. (iv), рассмотреть подграф, индуцированный этими 126 ребрами, то получится сильно регулярный граф с приведенными выше параметрами. Непосредственная проверка этого является весьма утомительной — легче показать, что такой граф имеет лишь три собственных значения. В завершение мы приведем несколько полезных теорем из работы [35].

Теорема. *Пусть*

$$A=\begin{pmatrix} A_{11} & A_{12} \\ A_{12}^{*} & A_{22} \end{pmatrix}$$

— эрмитова матрица порядка n. Предположим, что A имеет ровно два собственных значения, так что

$$\lambda_1(A)=\ldots=\lambda_f(A)>\lambda_{f+1}(A)=\ldots=\lambda_n(A)$$

для некоторого f, $1\leqslant f<n$. Пусть n_1 и n_2 — порядки матриц A_{11} и A_{22} соответственно. Тогда

$$\lambda_i(A_{22})=$$

$$=\begin{cases} \lambda_1(A)+\lambda_n(A)-\lambda_{f-i+1}(A_{11}) & \text{для } \max\{1, f+1-n_1\}\leqslant \\ & \leqslant i\leqslant \min\{f, n_2\}, \\ \lambda_1(A) & \text{для } 1\leqslant i\leqslant f+1-n_2, \\ \lambda_n(A) & \text{для } f<i\leqslant n_2. \end{cases}$$

Эту теорему можно применить к $(-1, +1, 0)$-матрицам смежности сильных графов, содержащихся в переключательном классе некоторого регулярного два-графа (т. е. к матрицам, удовлетворяющим равенству $(A - \rho_1 I)(A - \rho_2 I) = 0$).

Следствие. Предположим, что некоторый сильный граф, содержащийся в переключательном классе регулярного два-графа с v вершинами, собственными значениями ρ_1, ρ_2 $(\rho_1 > \rho_2)$ и кратностями μ_1, μ_2, имеет подграф с $u \geqslant \mu_1$ вершинами и собственными значениями $\lambda_1, \ldots, \lambda_u$, где $\lambda_1 = \rho_1$, $\lambda_2 = \ldots = \lambda_{\mu_1}$. Тогда подграф, индуцированный оставшимися $v - u$ вершинами, является сильным графом с двумя собственными значениями: $\rho_1 + \rho_2 - \lambda_2$ с кратностью $\mu_1 - 1$ и ρ_2 с кратностью $v - u - \mu_1 + 1$.

Приложение. Добавим изолированную вершину к графу на 175 вершинах и произведем переключение относительно семи ребер, проходящих через x. Тогда получим граф, содержащий Ho — Si в качестве подграфа. Собственные значения $(-1, +1, 0)$-матрицы смежности для этого два-графа равны $\rho_1 = 35$ и $\rho_2 = -5$ (с кратностями $\mu_1 = 22$ и $\mu_2 = 154$), а для графа Ho — Si $\rho_0 = 35$, $\rho_1 = 5$ и $\rho_2 = -5$ с кратностями 1, 21 и 28, поэтому из сформулированного выше следствия вытекает существование сильно регулярного графа на 126 вершинах. Замечая, что этот граф регулярен валентности 50, мы заключаем, что это и есть требуемый граф.

C. Семейство Маклафлина

(i) $(v, k, \lambda, \mu) = (275, 112, 30, 56)$ — граф Маклафлина.

Рассмотрим 23 точки и 253 блока (единственной) системы Штейнера $(X, \mathbf{B})$ с параметрами $S(4, 7, 23)$. Определим граф на этих 276 вершинах таким образом, что X является коклиной, точка соединена с блоками, содержащими ее, а два блока соединены, если они пересекаются по одной точке. Полученный таким образом граф содержится в переключательном классе некоторого регулярного два-графа на 276 точках. (Матричное рассмотрение этого два-графа см. в статье Сейдела [62]; интерпретация в терминах равноугольных прямых в решетке Лича приведена в статье Тейлора [69].) Группа автоморфизмов этого два-графа есть группа Конвея. 3. Изолировав вершину посредством переключения, а затем удалив ее, мы получим граф ранга 3 на 275 вершинах, для которого группой автоморфизмов является простая группа Маклафлина. Описанный граф и два-граф единственные [34].

Из приведенного описания видно, что построенный выше граф на 276 вершинах содержит в качестве подграфа граф Хигмана — Симса (переключенный относительно одной вершины).

Собственные значения $(-1, +1, 0)$-матрицы смежности два-графа равны $\rho_1 = 55$ и $\rho_2 = -5$ с кратностями $\mu_1 = 23$ и $\mu_2 = 253$, а графа Хигмана — Симса $\rho_0 = 55$, $\rho_1 = 15$, $\rho_2 = -5$ с кратностями 1, 22, 77 (соответственно), поэтому (в силу следствия из п. В (vii) мы нашли сильно регулярный граф на 176 вершинах, для которого вершинами являются блоки остаточной схемы $S(4, 7, 23) \setminus S(3, 6, 22)$, а ребрами — пары блоков, пересекающиеся по одной точке. Параметры такого графа суть $(v, k, \lambda, \mu) = (176, 70, 18, 24)$ те же, что и у графа, найденного выше, в п. В (vi).

Теперь уже непосредственно видно, что группой автоморфизмов этого графа является простая группа Хигмана — Симса. Граф Маклафлина экстремален в следующих смыслах: для него $g = 22$ и поэтому достигается равенство в условии абсолютной границы; для него $q_{22}^2 = 0$, т. е. достигается равенство в условии Крейна; для его дополнения $s = -3$ и $\mu = 81$, следовательно, достигается равенство в μ-условии.

(ii) $(v, k, \lambda, \mu) = (162, 56, 10, 21)$ и $(v, k, \lambda, \mu) = (112, 30, 2, 10)$. Камерон, Гёталс и Сейдел [11] доказали, что из равенства $q_{22}^2 = 0$ следует, что и подграф соседей, и подграф несоседей вершины являются сильно регулярными графами. Применив это утверждение к предыдущему графу, мы и получим графы с указанными выше параметрами.

Приведем прямое описание этих графов. Подплоскости Фано в проективной плоскости $PG(2, 4)$ под действием группы $PSL(3, 4)$ разбиваются на три орбиты. Возьмем в качестве вершин точки, прямые и одну из этих орбит на плоскостях Фано. Тогда $v = 21 + 21 + 120 = 162$. Пусть точки и прямые будут двумя 2-кокликами; соединим точку с прямой, если они инцидентны, точку с плоскостью Фано, если они пересекаются по трем точкам, наконец, две плоскости Фано, если они пересекаются по одной точке. Это приводит к единственному srg $(162, 56, 10, 24)$.

Пусть x_0 и x_1 — две фиксированные точки из множества точек системы $S(4, 7, 23)$. Возьмем в качестве вершин все блоки этой системы, которые содержат ровно одну из указанных точек. Соединим два блока, если они содержат одну и ту же фиксированную точку, и это единственная их общая точка. Это приводит к единственному srg$(112, 30, 2, 10)$, являющемуся точечным графом обобщенного четырехугольника $GQ(3, 9)$. Из приведенной конструкции видно, что множество вершин этого графа можно расщепить на две половины таким образом, что граф, индуцированный иа каждой из половин, изоморфен графу Гевиртца. Так же, как это было сделано для графа Хоффмана —

Синглтона, можно построить систему из трех сцепленных графов Гевиртца на 168 вершинах. Для этого следует рассмотреть три точки x_0, x_1 и x_2 в системе $S(5, 8, 24)$, взять в качестве вершин те из блоков, которые содержат ровно две из указанных точек, и соединить блоки B и B' тогда и только тогда, когда

$$|B \cap B'| + 2|B \cap B' \cap \{x_0, x_1, x_2\}| = 6.$$

Тогда любые два графа Гевиртца будут индуцировать точечный граф $GQ(3, 9)$, а весь граф — это точечный граф частичного линейного пространства, у которого размер прямой равен 6.

(iii) $(v, k, \lambda, \mu) = (276, 140, 58, 84)$.

Гёталс и Сейдел [34] показали (явно указав множество для переключения), что в переключательном классе описанного выше два-графа на 276 вершинах содержится сильно регулярный граф с приведенными выше параметрами. Вопрос о его единственности не решен.

(iv) $(v, k, \lambda, \mu) = (243, 110, 37, 60)$ — граф Дельсарта.

В процессе доказательства единственности регулярного два-графа на 276 вершинах Гёталс и Сейдел обнаружили в его переключательном классе граф, содержащий индуцированный подграф, изоморфный $11K_3$ (объединение 11 непересекающихся треугольников), такой, что каждая из оставшихся вершин смежна ровно с одной вершиной в каждом треугольнике. Из теоремы, сформулированной в п. B(vii), мы заключаем что для графа на оставшихся 243 вершинах собственные значения $(-1, +1, 0)$-матрицы смежности суть 49^{22}, 22^{1}, $(-5)^{220}$, поэтому это и есть требуемый граф. Он впервые был построен Дельсартом, исходя из тернарного кода Голея (см. ниже).

D. Код Голея и шапка Хилла

(i) $(v, k, \lambda, \mu) = (243, 22, 1, 2)$ — граф Берлекэмпа — ван Линта — Сейдела.

В [3] предложены три конструкции этого графа (по одному на каждого из авторов). Наиболее проста следующая конструкция: возьмем в качестве вершин $3^5 = 243$ смежных класса по совершенному тернарному коду Голея и соединим две вершины ребром, если соответствующие классы содержат представители, отличающиеся на вектор веса 1. Этот граф обладает двойственным в смысле Дельсарта (поскольку он обладает регулярной абелевой группой автоморфизмов). Этот двойственный граф имеет параметры $(v, k, \lambda, \mu) = (243, 110, 37, 60)$. Как мы видели раньше, он является подграфом в регулярном два-графе на 276 точках.

(ii) $(v, k, \lambda, \mu) = (2048, 276, 44, 36)$ и $(v, k, \lambda, \mu) = (2048, 759, 310, 264)$.

Возьмем $2^{11} = 2048$ смежных классов четной длины расширенного бинарного кода Голея в качестве вершин и соединим два смежных класса ребром, если они содержат представителей, отличающихся на вектор веса 2. Это приводит к srg(2048, 276, 44, 36). (Эквивалентное, но более сложное описание можно найти в обзоре Юбо [45]. Этот граф впервые построили Дж. Конвей и М. Смит. Рассматривая все 2^{12} смежных классов и соединяя два класса ребром, если между ними расстояние один, мы получим регулярный тонкий почти восьмиугольник на 4096 вершинах, в котором описанный выше сильно регулярный граф является графом путей длиной 2 на каждой из двудольных половин.) Двойственный к нему граф в смысле Дельсарта является srg(2048, 759, 310, 264). Последний был впервые построен Гёталсом и Сейделом, которые описали его следующим образом. Рассмотрим $2^{11} = 2048$ смежных классов по подпространству, состоящему из двух тождественных векторов 0 и 1 в расширенном бинарном коде Голея, и соединим два смежных класса ребром в случае, когда расстояние Хэмминга между ними равно 8.

(iii) $(v, k, \lambda, \mu) = (1288, 792, 476, 504)$.

Граф, дополнительный ко второму из графов в п. (ii), является srg(2048, 1288, 792, 840). Его граф соседей и есть граф с требуемыми параметрами.

(iv) $(v, k, \lambda, \mu) = (729, 112, 1, 20)$ — граф Гэймса.

В пространстве PG(5, 3) имеется единственная 56-шапка (т. е. такой набор из 56 точек, что каждая прямая пересекается с этим набором самое большее по двум точкам), см. [41]. Гэймс заметил, что если рассмотреть в качестве вершин точки пространства AG(6, 3) и соединить две вершины ребром в случае, если прямая, проходящая через эти точки, пересекает гиперплоскость, лежащую на бесконечности, в точке, которая содержится в упомянутой шляпе, то получится srg(729, 112, 1, 20) (см. [9a, 30]).

11. НЕДАВНИЕ РЕЗУЛЬТАТЫ ПО ЧАСТИЧНЫМ ГЕОМЕТРИЯМ

A. Pg(4, 5, 2) не существует

В [19] де Клерк классифицировал псевдогеометрические графы, соответствующие геометриям с условием $T = K - 2$. Интересным результатом является несуществование pg(4, 5, 2). В п. 5A мы видели, что существуют ровно четыре неизоморфных srg(28, 15, 6, 10) — дополнение к треугольному графу и гра-

фы Чанга. Для каждого из них можно предположить, что сильно регулярный граф является геометрическим; это приводит к противоречию. Для треугольного графа доказательство выглядит следующим образом.

Пусть вершинами являются неупорядоченные пары (x, y) из множества $\{1, 2, \ldots, 8\}$. Прямыми являются разбиения множества $\{1, 2, \ldots, 8\}$. Без ограничения общности мы можем считать в качестве прямой разбиение (12)(34)(56)(78), и в действительности, не ограничивая общности, мы можем выбрать все прямые, проходящие через точку (12). В этом остаются две возможности для прямых, проходящих через (13) и (24), и оказывается, что невозможно выбрать оставшиеся прямые, проходящие через (13). В остальных случаях доказательства проводятся аналогично.

В. Частичные геометрии, возникающие из $T(n)$*

Если n четно, то

$$\mathrm{srg}\left(\binom{n}{2}, \binom{n-2}{2}, \binom{n-4}{2}\binom{n-3}{2}\right)$$

псевдогеометрический и соответствует $\mathrm{pg}(^1/_2n,\ n-3,\ ^1/_2n-2)$. Как мы видели выше, при $n=8$ вопрос о существовании этих геометрий удается решить вручную. При $n=10$ мы получаем $\mathrm{pg}(5, 7, 3)$, которая известна. Ее можно построить следующим образом. Рассмотрим гиперовал Σ в пространстве $\mathrm{PG}(2, 8)$. Возьмем 45 секантов в Σ как новые точки, а точки вне Σ — как новые прямые. Эти новые точки и прямые образуют указанную частичную геометрию. Если занумеровать точки в Σ от 1 до 10, то пять секантов, проходящих через точку вне Σ, порождают разбиение множества $\{1, 2, \ldots, 10\}$, которое и отвечает нашему первоначальному представлению.

Как было показано Мэтоном [55], не существует других $\mathrm{pg}(5, 7, 3)$ (см. также [29a]). В настоящее время Лэм ведет исчерпывающий поиск с помощью ЭВМ следующей частичной геометрии, т. е. $\mathrm{pg}(6, 9, 4)$. Если эта частичная геометрия не существует, то возможная проективная плоскость порядка 10 не содержит гиперовалов и, следовательно, не имеет расширений.

Дополнение при корректуре. После 183 дней вычислений на ЭВМ исчерпывающий поиск был закончен и частичная геометрия не найдена [50a]. Таким образом, в предположении правильности использованной программы не существует ни $\mathrm{pg}(6, 9, 4)$, ни $\mathrm{S}(3, 12, 112)$.

C. pg(4, 7, 1) не существует

Не известно, существует ли srg(76, 21, 2, 7), однако Диксмер и Зара [28, 29] показали, что pg(4, 7, 1) не может существовать. Мы приведем незначительную модификацию их доказательства. Предположим, что такая частичная геометрия существует.

(i) Пусть $x \not\sim y$. Положим $\mathrm{tr}(x, y) := \{z \mid z \sim x,\ z \sim y\}$, $\Delta(x, y) := \{z \mid z \not\sim x,\ z \not\sim y\}$. Тогда $|\mathrm{tr}(x, y)| = 7$, $|\Delta(x, y)| = 39$.

(ii) Для $i = 0, 1, \ldots, 7$ обозначим через K_i подмножество в $\Delta(x, y)$, состоящее из точек, которые коллинеарны с i точками в $\mathrm{tr}(x, y)$, и пусть $n_i := |K_i|$.

(iii) Элементарный подсчет показывает, что $\sum n_i = 39$, $\sum i n_i = 105$, $\sum \binom{i}{2} n_i = 105$.

(iv) Пусть p и q — коллинеарные точки в Δ, такие, что прямая L, проходящая через p и q, не пересекается с $\mathrm{tr}(x, y)$. Тогда для двух других точек a и b, лежащих на L, имеет место $x \sim a$, $y \sim b$, и прямые, проходящие через x и a, соответственно через y и b, пересекают $\mathrm{tr}(x, y)$ в различных точках. Поэтому если $p \in K_i$, то $q \in K_{5-i}$. Отсюда мы находим, что $(7 - i) n_i = (2 + i) n_{5-i}$ и, следовательно, $n_6 = 0$. Из п. (iii) мы при этом получаем $n_0 = n_5 = n_7 = 0$, $n_1 = 4$, $n_2 = 12$, $n_3 = 15$, $n_4 = 8$.

(v) Пусть $p \in K_1$, и пусть $p \sim z \in \mathrm{tr}(x, y)$. Из (iv) следует, что оставшиеся точки на прямой pz содержатся в K_4. Имеется шесть прямых, проходящих через p и не пересекающихся с $\mathrm{tr}(x, y)$, а в силу п. (iv) на каждой из них лежит точка, содержащаяся в K_4. Поскольку $n_4 = 8$, мы видим, что каждая точка из K_1 смежна со всеми точками из K_4. Это противоречит тому, что $\mu = 7$.

D. Спорадическая геометрия pg(6, 6, 2)

В [52] ван Линт и Шрейвер описали частичную геометрию с параметрами $K = R = 6$, $T = 2$, которая является одной из двух спорадических частичных геометрий. Соответствующий сильно регулярный граф принадлежит семейству графов, описанных в п. 5C. Самое раннее его описание следующее: 81 вершина — это кодовые слова (5, 4)-линейного кода C над $\mathbb{F}_3$, где (1, 1, 1, 1, 1) — вектор проверки на четность. Две вершины соединяются ребром, если расстояние между ними $\equiv 2 \pmod 3$. Шесть кодовых слов (0, 0, 0, 0, 0), (1, 2, 2, 2, 2), ..., (2, 2, 2, 2, 1) образуют клику, которую мы выбираем в качестве прямой S. Оставшиеся прямые получаются с помощью сдвигов $S + \underline{c}$, где $\underline{c} \in C$. Недавно Камерон и ван Линт [15] показали, что группа автоморфизмов этой геометрии изоморфна полупрямому произ-

ведению группы трансляций и группы S_6. Их доказательство использует следующее элегантное описание.

Пусть $\bar{C}$ — код из постоянных векторов длиной 6. Сумма координат любого вектора в смежном классе по $\bar{C}$ постоянна, и мы назовем ее типом этого кода. Пусть $\mathbf{A}_i$ — множество смежных классов типа i. Определим двудольный граф Γ, соединив смежный класс $\bar{C}+\underline{v}$ со смежным классом $\bar{C}+\underline{v}+\underline{w}$ для всех векторов $\underline{w}$ длины 1. Тогда каждый вектор в $\mathbf{A}_i$ имеет шесть соседей в $\mathbf{A}_{i+1}$ и шесть в $\mathbf{A}_{i+2}$. Если рассмотреть любое множество $\mathbf{A}_i$ в качестве множества точек, а $\mathbf{A}_{i+1}$ как множество прямых и определить инцидентность посредством смежности, то получаем pg(6, 6, 2). В действительности мы имеем три сцепленные копии этой геометрии.

Интересно отметить, что Γ является подграфом в srg(243, 22, 1, 2), построенном Берлекэмпом и др. (п. 10D(i)).

E. Новая бесконечная серия pg $(2^{2n-1}, 2^{2n-1}+1, 2^{2n-2})$

Коэн [21] дал первое описание pg(8, 9, 4). Эта геометрия была (а может быть, и будет) спорадической. (*Дополнение при корректуре.* Недавно Тончев [71a] доказал изоморфизм между этой частичной геометрией и двойственной к частичной геометрией, описанной ниже.) Затем Хэмерс и ван Линт [37] предложили следующее более простое описание pg(9, 8, 4).

Возьмем в качестве вершины слова весом 4 или 8 в $(\mathbb{F}_2)^9$ и соединим две такие вершины ребром, если расстояние между ними сравнимо с двумя по модулю 4. Среди клик размера 9 имеются множества, отвечающие строкам матриц $(J-I)_9$,

$$\begin{pmatrix} 0 & \underline{1} & \underline{1} \\ \underline{1}^t & (J-I)_4 & 0 \\ \underline{1}^t & 0 & (J-I)_4 \end{pmatrix} \text{ и } \begin{pmatrix} J_3 & I_3 & 0 \\ 0 & J_3 & I_3 \\ I_3 & 0 & J_3 \end{pmatrix},$$

а также получаемым из них с помощью перестановок. Из этих клик выбираются $1+63+2\cdot 28=120$, которые считаются прямыми. Чтобы сделать это «естественным» образом, 9 позиций отождествляются с точками в PG(1, 8) и используется действие группы PSL(2, 8). С деталями можно ознакомиться в [37].

Эти примеры привели де Клерк, Дай и Тас к третьей конструкции, а затем и к открытию новой бесконечной серии, а именно серии pg$(2^{2n-1}, 2^{2n-1}+1, 2^{2n-2})$. Конструкция следующая. Пусть Q^+ — гиперболическая квадрика в PG$(4n-1, 2)$. Множество максимальных вполне изотропных пространств в Q^+ разбивается на два пересекающихся семейства D_1 и D_2. Если H — проективное пространство размерности $n-2$ в Q^+, то в Q^+

содержатся два максимальных вполне изотропных подпространства, проходящих через H, по одному для каждого семейства. Вместе они определяют $2n$-мерное пространство, которое содержит единственную гиперплоскость $M(H)$, проходящую через H и не лежащую в Q^+. Мы замечаем, что $M(H)\setminus H$ содержит 2^{2n-1} точек, не лежащих на Q^+. Пусть Ψ — покрытие Q^+, состоящее из элементов семейства D_1. Положим $X:=\{$точки не на $Q^+\}$; $\mathbf{L}:=\{$все пространства $M(H)$, где H — гиперплоскость, являющаяся элементом некоторого покрытия $\Psi\}$.

Мы называем элементы из $\mathbf{L}$ прямыми и выбираем естественное отношение инцидентности. Тогда $(X, \mathbf{L})$ является $\mathrm{pg}(2^{2n-1}, 2^{2n-1}+1, 2^{2n-2})$. С доказательством можно ознакомиться в [20].

Эта идея использовать покрытия для определения сильно регулярного графа и частичной геометрии была обобщена Кантором (см. п. 6E). Он также доказал, что $\mathrm{pg}(8, 9, 4)$ из описанной бесконечной серии изоморфна геометрии, двойственной той, которую построили Хэмерс и ван Линт. Для них A_9 является группой автоморфизмов.

F. Возможная бесконечная серия $\mathrm{pg}(3^{2h+1}, 3^{2h+1}+1, 2\cdot 3^{2h})$

В [71] Тас обобщил конструкцию, описанную выше в п. 11E, используя квадратики в $\mathrm{PG}(4h+3, 3)$. И в этом случае построение опирается на существование покрытий. Только при $h=0$ и при $h=1$ известно существование таких покрытий. Случай $h=0$ приводит к тривиальной геометрии, а при $h=1$ получается новая частичная геометрия $\mathrm{pg}(27, 28, 18)$. Пока это спорадический пример.

G. Спорадическая геометрия $\mathrm{pg}(5, 18, 2)$

Замечательная спорадическая частичная геометрия была построена Хэмерсом в [35] с использованием графа Хоффмана — Синглтона. Этот граф содержит 525 графов Петерсена в качестве индуцированных подграфов. Определяется специальный класс из 105 таких графов. Пусть ребра графа Хоффмана — Синглтона будут точками геометрии и определим прямые как 1-факторы в специальных подграфах Петерсена. Более подробно см. п. 10B.

H. Некоторые интересные открытые случаи

В п. 11B мы упомянули, что $\mathrm{pg}(6, 9, 4)$ связана с проективной плоскостью порядка 10. Ожидалось, что к концу 1982 г. будет известно, существует ли такая pg. (Теперь известно, что ее нет.)

В списке блок-схем, приведенном в книге Холла [38], первая неизвестная схема — это схема № 35: 2-(46, 6, 1). Если такая схема существует, то она приводит к pg(9, 6, 6) и к srg(69, 20, 7, 5), которые неизвестны.

Следующий открытый случай — это pg(5, 8, 2), отвечающая неизвестному srg(75, 32, 10, 16). Поскольку в этой геометрии через точку проходят восемь прямых, а общее число прямых такое же, как и в pg(9, 8, 4), можно надеяться, что искомую схему можно найти, удалив подходящие 60 точек из pg(9, 8, 4). Однако в [37] показано, что эта идея не работает.

ЛИТЕРАТУРА

[1] Belevitch V. Theory of $2n$-terminal networks with application to conference telephony. — Elect. Commun., 1950, v. 27, p. 231—244.

[2] Benson C. T., Losey N. E. on a graph of Hoffman and Singleton. — J. Comb. Th., 1971, v. 11, p. 67—79.

[3] Berlekamp E. R., van Lint J. H., Seidel J. J. A strongly regular graph derived from the perfect ternary Golay code. — In: A Survey of Combinatorial Theory. J. N. Srivastava e. a. (eds.). — North-Holland, 1973, p. 25—30.

[4] Bose R. C. Strongly regular graphs, partial geometries, and partially balanced designs. — Pacific J. Math., 1963, v. 13, p. 389—419.

[5] Bose R. C., Dowling T. A. A generalization of Moore graphs of diameter two. — J. Comb. Th. (B), 1971, v. 11, p. 213—226.

[5a] Broué M. Enguehard M. La géometrie de Graham Higman invariante par le group d'Higman — Sims. — Exposé au Séminaire Claude Chevalley, Avril — Mai 1974.

[6] Brouwer A. E. The uniqueness of the strongly reqular graph on 77 points. — Math. Centrum Report ZW 147/80, Amsterdam, 1980.

[7] Brouwer A E. Polarities of G. Higman's symmetric design and a strongly regular graph on 176 vertices. — Math. Centrum Report ZW 158/81, Amsterdam, 1981.

[8] Brouwer A. E., Neumaier A. Strongly regular graphs where $\mu = 2$ and λ is large. — Math. Centrum Report 151/81, Amsterdam, 1981.

[8a] Brouwer A. E., Schrijver A., Wilbrink H. A. Частное сообщение.

[9] Bussemaker F. C., Haemers W. H., Mathon R., Wilbrink H. A. Частное сообщение.

[9a] Cameron P. J. Partial quadrangles. — Quart. J. Math. Oxford, 1975, v. 26, p. 61—73.

[10] Cameron P. J. Strongly regular graphs. — In: Selected topics in graph theory, L. W. Beineke and R. J. Wilson (eds.). — Academic Press, 1978, p. 337—360.

[10a] Cameron P. J. Частное сообщение.

[11] Cameron P. J., Goethals J.-M., Seidel J. J. Strongly regular graphs having strongly regular subconstituents. — J. Algebra, 1978, v. 55, p. 257—280.

[12] Cameron P. J., Goethals J.-M., Seidel J. J. The Krein condition, spherical designs, Norton algebras and permutation groups. — Proc. KNAW A81 (= Indag. Math., v. 40). 1978. p. 196—206.

[13] Cameron P. J., Goethals J.-M., Seidel J. J., Shult E. E. Line graphs, root systems and elliptic geometry. — J. Algebra, 1976, v. 43, p. 305—327.

[14] Cameron P. J., van Lint J. H. Graphs, Codes and Designs. — London Math. Soc. Lecture Note Series, v. 43, Cambridge, 1980. [Имеется пере-

вод: Камерон П., ван Линт Дж. Теория графов, теория кодирования и блок-схемы. — М.: Наука, 1980.]
[15] Cameron P. J., van Lint J. H. On the partial geometry pg(6, 6, 2). — J. Comb. Th (A). 1982, v. 32, p. 252—255.
[16] Chang L. C. The uniqueness and nonuniqueness of triangular association schemes. — Sci. Record, 1949, v. 3, p. 604—613.
[17] Chang L C. Association schemes of partially balanced block designs with parameters $v = 28$, $n_1 = 12$, $n_2 = 15$ and $p_{11}^2 = 4$. — Sci. Record, 1950, v. 4, p. 12—18.
[18] Clatworthy W. H. Partially balanced incomplete block designs with two associate classes and two treatments per block. — J. Res. Nat. Bur. Standards. 1955, v. 54, p. 177—190.
[19] Clerck F. de. Partial Geometries. — Thesis University of Ghent. 1978.
[20] Clerck F. de. Dye R. H., Thas J. A. An infinite class of partial geometries associated with the hyperbolic quadric in PG($4n - 1$, 2). — Eur. J. Combinatorics, 1980, v. 1, p. 323—326.
[21] Cohen A. M. A new partial geometry with parameters $(s, t, \alpha) = (7, 8, 4)$. — J. Geometry, 1981, v. 16, p. 181—186.
[22] Connor W. S. The uniqueness of the triangular association scheme. — Ann. Math. Stat., 1958, v. 29, p. 262—266.
[23] Cvetković D. M., Doob M., Sachs H. Spactra of Graphs. — Theory and Application New York etc.: Academic Press, 1980. [Имеется перевод: Цветкович Д., Дуб М., Захс Х. Спектры графов. Теория и применение. — Наукова думка, Киев, 1984.]
[24] Debroey I. Semi partiéle meetkunden. — Thesis, University of Ghent, 1978.
[25] Debroey I., Thas J. A. On semi partial geometries. — J. Comb. Th. (A), 1978, v. 25 p. 242—250.
[26] Delsarte P An Algebraic approach to the association schemes of coding theory. — Philips Res. Repts. Suppl., 1973, v. 10. [Имеется перевод: Дельсарт Ф. Алгебраический подход к схемам отношений теории кодирования. — М.: Мир, 1976.]
[27] Delsarte P., Goethals J.-M., Seidel J. J. Bounds for systems of lines and Jacobi polynomials. — Philips Res. Repts., 1975, v. 30, p. 91*—105*.
[28] Dixmier S., Zara F. Essai d'une méthode d'étude de certains graphes liés aux groupes classiques. — C. R. Acad. Sc. Paris, v. 282, Série A, p. 259—262.
[29] Dixmier S., Zara F. Etude d'un quadrangle généralisé autour deux de ses points non lies (препринт).
[29a] Faima G., Cecconi G. A finite Buekenhout oval which is not projective. — Simon Stevin, 1982, v. 56. p. 121—127.
[30] Games R. Частное сообщение.
[31] Gewirtz A. The uniqueness of $g(2, 2, 10, 56)$. — Trans. New York Acad. Sci., 1969. v. 31, p. 656—675.
[32] Gewirtz A. Graphs with maximal even girth. — Can. J. Math., 1970, v. 21, p. 915—934.
[33] Goethals J.-M., Seidel J. J. Strongly regular graphs derived from combinatorial designs. — Can. J. Math., 1970, v. 22, p. 597—614.
[34] Goethals J.-M. Seidel J. J. The regular two-graph on 276 vertices. — Discrete Math., 1975, v. 12, p. 143—158.
[35] Haemers W. H. Eigenvalue techniques in design and graph theory. — Thesis (Eindhoven) 1979 = Math. Centre Tract, v. 121, Amsterdam, 1980.
[36] Haemers W. H. A new partial geometry consturcted from the Hoffman — Singleton graph. — In: Finite Geometries and Designs, P. J. Cameron, J. W. P. Hirschfeld and D. R. Huges (eds.). — London Math. Soc. Lecture Note Series v. 49. Cambridge 1981, p. 119—127.

[37] Haemers W. H., van Lint J. H. A partial geometry pg(9, 8, 4). — Annals of Discr. Math., 1982, v. 15, p. 205—212.
[38] Hall M., Jr. Combinatorial Theory. — Blaisdell, 1967. [Имеется перевод: Холл М. Комбинаторика. — М.: Мир, 1970.]
[39] Higman D. G. Invariant relations, coherent configurations and generalized polygons. — In: Combinatorics, M. Hall, Jr. and J. H. van Lint (eds.). — Math Centre Tracts 57, Amsterdam, 1974, p. 27—43.
[40] Higman G On the simple group of D. G. Higman and C. C. Sims. — Illinois J. Math., 1969, v. 13, p. 74—80.
[41] Hill R. Caps and codes. — Discrete Math., 1978, v. 22, p. 111—137.
[42] Hoffman A. J. On the uniqueness of the triangular association scheme. — Ann. Math. Stat., 1960, v. 31, p. 492—497.
[43] Hoffman A. J., Singleton R. R. On Moore graphs with diameter 2 and 3. — IBM J. Res. Develop., 1960, v. 4, p. 497—504.
[44] Hollman H. D. L. Association schemes. — Master's thesis, Eindhoven University of Technology, 1982.
[45] Hubaut X L. Strongly regular graphs. — Discrete Math., 1975, v. 13, p. 357—381. [Имеется перевод: настоящий сборник, с. 160—185.]
[46] Kageyama S., Saha G. M., Das A. D. Reduction of the number of association classes of hypercubic association schemes. — Ann. Inst. Stat. Math., 1978, v. 30, p. 115—123.
[47] Kantor W. M. Strongly regular graphs defined by spreads.—Isr. J. Math., 1982, v. 41 p. 298—312.
[48] Kantor W. M., Liebler R. A. The rank three representations of the finite classical groups. — Trans. Amer. Math. Soc., 1982, v. 271, p. 1—71.
[49] Koornwinder T. H. A note on the absolute bound for systems of lines. — Proc. KNAW A79 (=Indag. Math., v. 38), 1976, p. 152—153.
[50] Крейн М. Г. Эрмитово-положительные ядра на однородных пространствах II. — Укр. матем. ж., 1950, № 1, с. 10—59.
[50a] Lam C. W. H. Thiel L., Swiercz S., McKay J. The nonexistence of ovals in a projective plane of order 10. — Discr. Math., 1983, v. 45, p. 319—321.
[51] van Lint J. H., Seidel J. J. Equilateral point sets in elliptic geometry. — Proc. KNAW A69 (=Indag. Math., v. 28), 1969. p. 335—348.
[52] van Lint J. H., Schrijver A. Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields. — Combinatorica, 1981, v. 1, 63—73.
[53] Mathon R. Three-class association schemes. — In: Proc. Conf. on Algebraic Aspects of Combinatorics, Toronto, 1975, p. 123—155.
[54] Mathon R. Symmetric conference matrices of order pq^2+1. — Can. J. Math., 1978, v. 30, p. 321—331.
[55] Mathon R. The partial geometries pg(5, 7, 3). — Congressus Numerantium, 1981, v. 31, p. 129—139.
[55a] Mathon R. Частное сообщение.
[55b] Mathon R., Rosa A. A new strongly regular graph. — J. Comb. Th. (A), 1985, v. 38, p. 84—86.
[56] Mesner D. M. A new family of partially balanced incomplete block designs with some Latin square properties. — Ann. Math. Stat., 1967, v. 38, p. 571—581.
[57] Neumaier A. Strongly regular graphs with smallest eigenvalue $-m$. — Arch. Math., 1979, v. 33, p. 392—400.
[58] Neumaier A. New inequalities for the parameters of an association scheme. — Combinatorics and Graph Theory, Springer Lectire Notes, 1981, v. 885, p. 365—367.
[59] Robertson N. Частное сообщение.
[60] Scott L. L. A condition on Higman's parameters. — Notices Amer. Math. Soc., 1973, 701-20-45 (page A-97).
[61] Seidel J. J. Strongly regular graphs with (—1, 1, 0) adjacency matrix

having eigenvalue 3. — Lin. Algebra and Appl., 1968, v. 1, p. 281—298.

[62] Seidel J. J. A survey of two-graphs. — In: Proc. Intern. Colloq. Theorie Combinatorie (Roma 1973), tomo I, Accad. Naz. Lincei, 1976, p. 481—511.

[63] Seidel J. J. Strongly regular graphs. — In: Surveys in Combinatorics, Proc. 7th Brit. Comb Conf, B. Bollobás (ed.), London Math. Soc. Lecture Note Series, v. 38, Cambridge, 1979, p. 157—180.

[64] Seidel J. J.. Taylor D. E. Two-graphs, a second survey. — In: Proc. Intern. Colloq. Algebraic Methods in Graph Theory, Szeged, 1978, Coll. Math. Soc. Bolyai, v. 25, p. 689—711.

[65] Shrikhande S. S. The uniqueness of the L_2 association scheme. — Ann. Math. Stat.. 1959, v. 30, p. 781—798.

[66] Sims C. C. On the isomorphism of two groups of order 44, 352, 000. — In: Theory of Finite Groups, Brauer and Sah (eds.), Benjamin, 1969.

[67] Smith M. S. On the isomorphism of two simple groups of order 44, 352, 000. — J. Algebra, 1976, v. 41, p. 172—174.

[68] Taylor D. E. Graphs and block designs associated with three-dimensional unitary groups. — In: Combinatorial Mathematics, Proc. 2nd Austr. Conf., D. A. Holton (ed.), Springer Lecture Notes, v. 403, Berlin etc. 1974, p. 128—131.

[69] Taylor D. E. Regular 2-graphs. — Proc. London Math. Soc., 1977, v. 35, p. 257—274.

[70] Thas J. A Combinatorics of partial geometries and generalized quadrangles. — In: Higher Combinatorics, M. Aigner (ed.). — Dordrecht: Reidel, 1977, p. 183—199. [Имеется перевод: Проблемы комбинаторного анализа. — М.: Мир, 1980, с. 82—100.]

[71] Thas J. A. Some results on quadrics and a new partial geometries. — Simon Stevin, 1981, v. 55, p. 129—139.

[71a] Tonchev V. D. The isomorphism of Cohen. Haemers — van Linst and De Clerck — Dye — Thas partial geometries. — Discr. Math., 1984, v. 49, p. 213—217.

[72] Wallis W. D., Street A. P., Wallis J. Seberry Combinatorics: room squares, sum-free sets, Hadamard matrices. — Springer Lecture Notes. v. 292, Berlin etc., 1972.

[73] Wilbrink H. A., Brouwer A. E. A(57, 14, 1) strongly regular graph does not exist. — KNAW A86 (= Indag. Math., v. 45), 1983. p. 117—121.

[74] Wilbrink H. A. Частное сообщение.

[75] Zara F. Частное сообщение.

Содержание

УВАЖАЕМЫЙ ЧИТАТЕЛЬ!

Ваши замечания о содержании книги, ее оформлении, качестве перевода и другие просим присылать по адресу: 129820, Москва, И-110, ГСП, 1-й Рижский пер., 2, издательство «Мир».

Научное издание

КИБЕРНЕТИЧЕСКИЙ СБОРНИК ВЫП 24

Сборник статей

Старший научн. ред. П. Я. Корсоюцкая
Младший научн. ред. Н. С Полякова
Художественный редактор В. И. Шаповалов
Художник Н. К. Сапожников
Технический редактор Л. В. Козлова
Корректор В. С. Соколов

ИБ № 6335

Сдано в набор 3.02.87г. Подписано к печати 13.07.87 г. Формат 60×90/16. Бумага типографская № 1. Печать высокая. Гарнитура литературная. Объем 7,25 бум. л. Усл. печ. л. 14,50. Усл. кр.-отт. 14,50. Уч.-изд. л. 14,40. Изд. № 1/5531. Тираж 3500 экз. Зак. № 1063 Цена 2 р. 60 коп.

ИЗДАТЕЛЬСТВО «МИР» 129820, ГСП, Москва, И-110, 1-й Рижский пер., 2

Отпечатано с матриц Ленинградской типографии № 2 головного предприятия ордена Трудового Красного Знамени Ленинградского объединения «Техническая книга» им. Евгении Соколовой Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 198052, Ленинград, Л-52, Измайловский проспект, 29 в Ленинградской типографии № 4 ордена Трудового Красного Знамени Ленинградского объединения «Техническая книга» им. Евгении Соколовой Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 191126, Ленинград, Социалистическая ул., 14.