ANNALS OF MATHEMATICS
Vol. 77, No. 1, January, 1963
Printed in Japan

THE WORD PROBLEM

BY JOHN L. BRITTON

(Received October 2, 1961)

It will be shown that the word problem for groups is unsolvable in general. Previous proofs have been given by Boone [1], [2], Higman [5], Novikov [7] and the author [4].

The starting point is the result of Post [8] that there is a semi-group given by a finite number of generators and a finite number of defining relations (i.e., a Thue system) with unsolvable word problem.

The aim has been to give a simple proof using the concepts and vocabulary of contemporary text books on group theory. Thus we use free products with amalgamated subgroups (Kurosh [6, Chap. IX]) and the theorem of Higman, B. H. Neumann and H. Neumann (Kurosh [6, Chap. X, § 38]) but, for example, we are precluded from using (as was done in [4]) the results of Tartakovskii [9], [10], [11] and of the author [3] which are, as yet, relatively unfamiliar.

The group whose word problem will be shown to be unsolvable is virtually the same as in Boone [2][1], but the method of proof is group-theoretical rather than combinatorial.

0. Informal discussion

Without attempting to be precise, we may distinguish between the group-theoretical and the combinatorial approaches to problems in the theory of generators and defining relations as follows. Suppose a group G is given by generators $a_1, a_2, \cdots, a_m$ and defining relations $A_i = B_i$ $(i = 1, 2, \cdots, n)$. Let U and V be words in $a_1, a_2, \cdots, a_m$. We know that the elements of G corresponding to U, V are equal if and only if there is a finite sequence of operations

$$W_1 \to W_2 \to \cdots \to W_k$$

transforming U into V, where W_1 is U, W_k is V and, for $j = 1, 2, \cdots, k-1$, $W_j \to W_{j+1}$ denotes one of the following operations:

(a) cancellation: replace a word of the form $Xa_s a_s^{-1} Y$ or $Xa_s^{-1} a_s Y$ by XY.

(b) insertion: the converse process of (a),

(c) replace a word of the form XA_iY by XB_iY, or conversely.

Any argument involving such a sequence of operations may be called

[1] We have deleted the generator t_1 and replaced t_2 by t. Our group is a quotient group of Boone's group.

The author is very grateful to Prof. Boone for his advice and encouragement throughout.

combinatorial. In contrast, an argument circumventing *explicit* reference to a sequence of this kind, especially avoiding any mention of insertions, may be called group-theoretical.

It is not always trivial to correlate the group-theoretical and the combinatorial statements of essentially the same result. Let G' be the group obtained from the above group G by adding the new generator t and the defining relation $a_3t = ta_3$. Let $At = tA$ in G', where A is a word in a_1, $a_2, \cdots, a_m$. Then it can be shown (e.g., by Lemma 2 below) that

(i) the element A belongs to the subgroup of G generated by a_3; thus there is an integer h such that $A = a_3^h$ in G (hence also $A = a_3^h$ in G'). The conclusion (i) can be stated combinatorially as follows:

(ii) At can be transformed into tA by a sequence of the above kind (in G') without using insertions of t^{-1} (that is, operations of the form $XY \to Xtt^{-1}Y$ or $XY \to Xt^{-1}tY$).

To see that (i) implies (ii), note that one can first transform At into $a_3^h t$, then by using the defining relation $a_3t = ta_3$ transform $a_3^h t$ into ta_3^h, and finally transform ta_3^h into tA.

To show that (ii) implies (i), one first proves that a single operation, not an insertion of t^{-1}, applied to a word of the form PtQ where P and Q do not involve t or t^{-1} yields $P'tQ'$, where $P^{-1}P' = a_3^d$ in G and $QQ'^{-1} = a_3^d$ in G, and where d is either $0, 1$ or -1; now (i) follows by a simple induction argument.

Similarly, in the proof below of Lemma 6, part (k), the statement that $\Sigma^{-1}t\Sigma$ belongs to a certain subgroup of G_1 corresponds to the combinatorial statement that in G the word $\Sigma k \Sigma^{-1}$ can be transformed into $t\Sigma k \Sigma^{-1}t^{-1}$ without using insertions of k^{-1}; this is essentially Theorem III of Boone [2].

The conclusion of the principal lemma (Lemma 4) below is equivalent to the statement that W can be transformed into the empty word without using insertions of any p_v^{-1}.

It might be objected that in the proof of Lemma 7 below we have used an evidently combinatorial argument; but there we are dealing with a semi-group, not a group. However the major part of the paper concerns groups, and we use group-theoretical arguments. Indeed, from now on, there will be no further mention of insertions.

1. Preliminaries

By a *word over* S, where S is a finite or countable set of symbols $s_1, s_2, \cdots$, or a *word in* these symbols, we mean an expression

$$s_{b_1}^{e_1} s_{b_2}^{e_2} \cdots s_{b_n}^{e_n}$$

where $e_i = \pm 1$ ($i = 1, 2, \cdots, n$). The word is *positive* if every e_i is 1. n is called the *length* of the word. When $n = 0$ we have the empty word 1; it is to be positive. $X \equiv Y$ means that the words X, Y are identical. The product of two words and the inverse of a word are defined as usual. If $W \equiv XYZ$ then Y is a *subword* of W. A word over S is *reduced* if it contains no subword of the form $s_b s_b^{-1}$ or $s_b^{-1} s_b$. A word over S *involves* s_4, say, if it contains s_4 or s_4^{-1} as a subword.

A *presentation* $H = (S; D)$ consists of a set S of symbols (called generators) and a set D of formal equations (called defining relations), each of the form $X = Y$, where X, Y are words over S. D is finite or countable, as is S. In a well known way, a presentation H determines a group, also denoted by H, which is unique to within isomorphism. The element of the group determined by the word W is also denoted by W.

Let $H_1 = (S_1; D_1)$ and $H_2 = (S_2; D_2)$ be presentations. We write $H_1 \leqq H_2$ if $S_1 \subset S_2$, $D_1 \subset D_2$, and if for every word W over S_1, we have $W = 1$ in H_1 if and only if $W = 1$ in H_2; H_1 may then be identified with a subgroup of H_2.

LEMMA 1. *Let P be the free product of groups $G_\gamma (\gamma \in \Gamma)$ with amalgamated subgroup Q. If $x_1, x_2, \cdots, x_k$ ($k \geqq 1$) are elements of P not in the subgroup Q, each belonging to a constituent group, say $x_i \in G_{\gamma_i}$ ($i = 1, 2, \cdots, k$), and if $\gamma_j \neq \gamma_{j+1}$ ($j = 1, 2, \cdots, k-1$), then the element $y = x_1 x_2 \cdots x_k$ does not belong to Q. In particular, $y \neq 1$.*

PROOF. For each $\gamma \in \Gamma$ take a set of representatives of the left cosets of Q in G_γ such that the representative of Q is the identity element 1. Every element z of P can now be expressed uniquely in the form

$$z = u r_1 r_2 \cdots r_n ,$$

where $u \in Q$, $n \geqq 0$, each r_i is a representative different from the identity in some constituent group, and r_j, r_{j+1} belong to different constituent groups ($j = 1, 2, \cdots, n-1$). n is called the weight of z.

It is easy to prove by induction that the element y in the statement of the lemma has weight k. The lemma now follows, since any element of Q has weight zero.

LEMMA 2. *Let $H = (S; D)$ and*

$$H^* = \big(S, t; D, t^{-1} X_i t = X_i (i \in I)\big)$$

be presentations, where each X_i is a word over S. Let W be a word in the generators of H^* which involves t. If $W = 1$ in H^* then W contains a subword $t^{-1}Ct$ or tCt^{-1}, where C is a word over S, and C, regarded as an element of the group H, belongs to the subgroup X of H generated by *the* $X_i\,(i \in I)$.

PROOF. 1°. First we prove that $H \leqq H^*$, and that H^* is a free product with amalgamated subgroup.

Let X' be an isomorphic copy of X. Take a presentation of X' of the form $(x_i(i \in I);\, w_j(x_i) = 1(j \in J))$, where x_i corresponds to X_i for each $i \in I$. Let Y be the direct product of X' and the free cyclic group $(t;\, \varnothing)$. Form the free product P of H and Y, amalgamating the subgroup X of H with the subgroup X' of Y. Then a presentation of P is

$$\big(S, t, x_i(i \in I);\, D, w_j(x_i) = 1, t^{-1}x_i t = x_i, x_i = X_i(i \in I, j \in J)\big)\,,$$

hence another presentation of P is

$$\big(S, t;\, D, w_j(X_i) = 1, t^{-1}X_i t = X_i(i \in I, j \in J)\big)\,.$$

On the other hand this last presentation is a presentation of H^*, since we have $w_j(X_i) = 1$ in H, hence also in H^*. Thus P is just H^*. Hence H is a subgroup of H^*, and $H \leqq H^*$.

2°. The lemma is obviously true if W contains a subword $t^{-1}t$ or tt^{-1}; there remains the case when W has the form

$$W_0 t^{a_1} W_1 \cdots t^{a_r} W_r\,,$$

where $r \geqq 1$, each a_i is a non-zero integer and $W_0, W_1, \cdots, W_r$ are words over S of which only W_0 and W_r may be empty. Each t^{a_i} belongs to Y but not to the amalgamated subgroup X. Each W_i belongs to H, and may or may not belong to X. We proceed by induction on r.

If $r = 1$ then $W \equiv W_0 t^{a_1} W_1$, and since $W = 1$ in H^* we have

$$t^{a_1} = W_0^{-1} W_1^{-1} \in H \cap Y = X\,;$$

this contradiction shows that the lemma is true when $r = 1$.

For the induction step, since $W = 1$ in H^*, we have by Lemma 1 that at least one $W_j (1 \leqq j \leqq r - 1)$ belongs to X. If a_j and a_{j+1} have opposite sign, we have finished. Now let a_j and a_{j+1} have the same sign. In H^*,

$$W \equiv \cdots t^{a_j} W_j t^{a_{j+1}} W_{j+1} \cdots = \cdots t^{a_j + a_{j+1}} W_j W_{j+1} \cdots\,,$$

and the induction hypothesis can be applied to the last word. Since $a_j + a_{j+1}$ has the same sign as both a_j and a_{j+1}, and since $W_j W_{j+1} \in X$ if and only if $W_{j+1} \in X$, we deduce that W contains a subword of the required form.

2. Stable letters. The principal lemma

Let $E = (S;\, D)$ be any presentation. A presentation E^* is said to have *stable letters* $p_v(v \in V)$ and corresponding *basis* E if it has the form

$$E^* = \left(S, p_v(v \in V); D, F_i p_{v_i} G_i = H_i p_{v_i} K_i (i \in I)\right) ,$$

where $v_i \in V$ and F_i, G_i, H_i, K_i are words over S, and if, for each $v \in V$, at least one of the defining relations involves p_v, that is, the set J_v of all i in I such that $v_i = v$ is non-empty.

We shall consider the following further conditions, in which we use the notation $A_i \equiv H_i^{-1} F_i$, $B_i \equiv K_i G_i^{-1}$.

The *strong isomorphism condition* is that there is an isomorphism of the subgroup A of the basis E generated by the $A_i(i \in I)$ onto the subgroup B of E generated by the $B_i(i \in I)$ in which $A_i \to B_i$; this implies the *isomorphism condition*, that for each $v \in V$ there is an isomorphism of the subgroup $A(v)$ of the basis E generated by $A_i(i \in J_v)$ onto the subgroup $B(v)$ of the basis E generated by $B_i(i \in J_v)$ such that $A_i \to B_i$.

Note. In the proofs of the two lemmas which follow, E_1^* denotes the presentation

$$\left(S, p_v(v \in V); D, p_{v_i}^{-1} A_i p_{v_i} = B_i (i \in I)\right) .$$

Clearly, for any word W, $W = 1$ in E_1^* if and only if $W = 1$ in E^*; hence $E \leqq E_1^*$ if and only if $E \leqq E^*$.

LEMMA 3. *Let E^* be a presentation with certain stable letters $p_v(v \in V)$ and basis $E = (S; D)$. Let the isomorphism condition be satisfied. Then $E \leqq E^*$.*

PROOF. By the theorem[2] of Higman, Neumann and Neumann (see Kurosh [6, Ch. X, § 38, Lemma 2], there is a group E_0 containing E and elements $p_v(v \in V)$ such that $p_v^{-1} A_i p_v = B_i$ whenever $v \in V$ and $i \in J_v$; equivalently, $p_{v_i}^{-1} A_i p_{v_i} = B_i$ for all $i \in I$. Clearly we may assume that E_0 is generated by E and the elements $p_v(v \in V)$. It is now clear that a presentation of E_0 can be obtained from E_1^* by adding (a possibly empty set of) further defining relations. Now let W be a word over S. If $W = 1$ in E_1^*, then $W = 1$ in E_0, and since E is a subgroup of E_0, it follows that $W = 1$ in E. Conversely, it is trivial that $W = 1$ in E implies $W = 1$ in E_1^*. Hence $E \leqq E_1^*$, so that $E \leqq E^*$.

LEMMA 4. (The principal lemma). *Let E be a presentation with stable letters p_v $(v \in V)$ and basis $E = (S; D)$. Let the isomorphism condition be satisfied. In the notation of the first three paragraphs of this section, if $W = 1$ in E^*, where W is a word involving at least one stable letter, then W contains a subword*

$$p_v^{-1} C p_v, \text{ where } C \text{ belongs to } A(v) \text{ and hence to } A ,$$

or

[2] Lemma 3 is essentially a re-statement of this theorem.

$$p_v C p_v^{-1}, \text{ where } C \text{ belongs to } B(v) \text{ and hence to } B\,;$$

in both cases C is a word over S.

Note. (i) This lemma for one stable letter was proved in [4], but an extra condition was needed.

(ii) A word C over S clearly belongs to the subgroup A of E if and only if there exist $i_1, i_2, \cdots, i_r$ in I ($r \geqq 0$) and integers $e_1, e_2, \cdots, e_r$, each being either 1 or -1, such that

$$C = A_{i_1}^{e_1} A_{i_2}^{e_2} \cdots A_{i_r}^{e_r} \text{ in } E\,.$$

Sometimes we prefer to write (with a change of notation) $CA_{i_1}^{e_1} \cdots A_{i_r}^{e_r} = 1$ in E.

(iii) In §§ 3, 4 the strong isomorphism condition is always satisfied.

PROOF. 1°. We first prove the lemma in the case that there is only one stable letter, p. Since $W = 1$ in E^*, we have $W = 1$ in

$$E_1^* = (S, p;\, D,\, p^{-1}A_i p = B_i(i \in I))\,;$$

and we have to prove that W contains a subword $p^{-1}Cp(C \in A)$ or pCp^{-1} $(C \in B)$, C being a word over S. This is certainly true if W contains a subword $p^{-1}p$ or pp^{-1}; there remains the case when W has the form

$$W \equiv W_0 p^{a_1} W_1 \cdots p^{a_r} W_r\,,$$

where $r \geqq 1$, each a_i is a non-zero integer and $W_0, W_1, \cdots, W_r$ are words over S of which only W_0 and W_r may be empty.

By Lemma 3, $E = (S; D) \leqq E^*$, so $E \leqq E_1^*$. Hence, obviously, $E \leqq H$, where

$$H = (S, q;\, D,\, q^{-1}A_i q = B_i(i \in I))\,.$$

With Lemma 2 in mind, consider

$$H^* = (S, q, t;\, D,\, q^{-1}A_i q = B_i,\, t^{-1}B_i t = B_i(i \in I))\,.$$

Adding the new generator p and the defining relation $p = qt$ we see that H^* is isomorphic to K, where

$$K = (S, q, t, p;\, D,\, q^{-1}A_i q = B_i,\, p = qt,\, p^{-1}A_i p = B_i(i \in I))\,.$$

Since K contains all generators and defining relations of E_1^*, we have $W = 1$ in K. Hence

$$W_0(qt)^{a_1} W_1 \cdots (qt)^{a_r} W_r = 1$$

in K, and hence in H^*. By Lemma 2 this word contains a subword $t^e C t^{-e}$ $(e = \pm 1)$ where C belongs to the subgroup of H generated by the B_i. Since $E \leqq H$, this means that $C \in B$. If $e = 1$, C has the form W_j for some j $(1 \leqq j \leqq r - 1)$ and we have finished. If $e = -1$ then C has the form $q^{-1}W_jq$ for some j, and we have $q^{-1}W_jq \in B$, hence $W_j \in qBq^{-1} = A$.

2°. Now consider the general case. Denote the elements of the index set V by $1, 2, 3, \cdots$. Let $D(v)$ consist of the defining relations $p_{v_i}^{-1}A_ip_{v_i} = B_i$ of E_1^* such that $i \in J_v$ (that is, $v_i = v$). Since $W = 1$ in E_1^* we have $W = 1$ in E_r for some r, where

$$E_r = \big(S, p_1, p_2, \cdots, p_r ; D, D(1), D(2), \cdots, D(r)\big) .$$

It is straightforward to prove that $E \leqq E_1 \leqq E_2 \leqq \cdots$. Choosing s maximal so that W involves p_s, we deduce that $W = 1$ in E_s. Now p_s is a stable letter for E_s, the basis being E_{s-1}, hence W contains a subword $p_s^eCp_s^{-e}$ where for example $e = 1$ and C belongs to the subgroup of E_{s-1} (hence of E) generated by $B_i\,(i \in J_s)$. If C is a word over S we have finished, but if C involves some of $p_1, \cdots, p_{s-1}$ then $C = C'$ in E_{s-1} where C' is a word over S, namely a product of $B_i^{\pm 1}$ where $i \in J_s$. Thus $CC'^{-1} = 1$ in E_{s-1} and, by an induction hypothesis CC'^{-1} (hence C and hence W) contains a subword of the required type.

3. The semi-group T and the group G

Let T be a semi-group with generators

$$s_b,\ q_a \qquad (b = 1, 2, \cdots, M;\ a = 0, 1, 2, \cdots, N)$$

and defining relations

$$\Sigma_i = \Gamma_i \qquad (i = 1, 2, \cdots, P)$$

where each Σ_i and Γ_i is a *special word*, i.e., a word of the form Sq_aS' where S and S' are positive words in $s_1, s_2, \cdots, s_M$. Thus if U, V are positive words in the generators of T then $U = V$ in T if and only if U can be transformed into V by a finite sequence of elementary transformations, each of the form

$$X\Sigma_iY \to X\Gamma_iY \quad \text{or} \quad X\Gamma_iY \to X\Sigma_iY .$$

We shall denote q_0 also by q.

From Post [8] we have (cf. Appendix (I)),

LEMMA 5. *For a certain choice of T, it is recursively unsolvable to determine for an arbitrary special word Σ whether or not $\Sigma = q$ in T.*

Let G be the group with generators

$$s_b,\ q_a,\ k,\ t,\ x,\ y,\ l_i,\ r_i$$

and defining relations

$$\left.\left.\left.\left.\begin{array}{ll} s_b y = yys_b\ , & xs_b = s_b xx\ , \\ s_b l_i = yl_i ys_b\ , & r_i s_b = s_b x r_i x\ , \\ \multicolumn{2}{c}{\Sigma_i = l_i \Gamma_i r_i\ ,} \\ tl_i = l_i t\ , \quad ty = yt\ , & \\ r_i k = kr_i\ , & xk = kx\ , \\ \multicolumn{2}{c}{(q^{-1}tq)k = k(q^{-1}tq)\ ,} \end{array}\right\} G_1 \right\} G_2 \right\} G_3 \right\} G_4$$

where $b = 1, 2, \cdots, M$; $a = 0, 1, \cdots, N$; $i = 1, 2, \cdots, P$.

We shall prove the following two lemmas.

LEMMA 6. *If Σ is a special word and*

$$(1) \qquad (\Sigma^{-1}t\Sigma)k = k(\Sigma^{-1}t\Sigma) \text{ in } G$$

then $\Sigma = q$ in T.

LEMMA 7. *Conversely if Σ is a special word and $\Sigma = q$ in T then* (1) *holds.*

It will follow that

THEOREM. *The word problem for G is unsolvable.*

PROOF OF LEMMA 7. 1°. Suppose that for the special word Σ, $\Sigma = q$ in T. We first prove that $\Sigma = LqR$ in G, where L is a word in l_i, y, and R is a word in r_i, x. There is a sequence of elementary transformations

$$\Sigma \equiv W_1 \to W_2 \to \cdots \to W_n \equiv q$$

where for each $j = 1, 2, \cdots, n-1$, one of the words W_j, W_{j+1} has the form $X\Sigma_i Y$ and the other has the form $X\Gamma_i Y$. Since Σ is a special word, all of $W_1, W_2, \cdots, W_n$ are special, so that X and Y are positive words in the s_b. Hence, by repeated use of the defining relations $s_b y = yys_b$, $s_b l_i = yl_i ys_b$, we see that $Xl_i = L'X$ in G for some word L' in l_i, y; similarly, $r_i Y = YR'$ for some word R' in r_i, x. Therefore

$$X\Sigma_i Y = Xl_i\Gamma_i r_i Y = L'X\Gamma_i YR'\ ,$$

so that $W_j = L_j W_{j+1} R_j$ where L_j is a word in l_i, y, and R_j is a word in r_i, x. The result follows if we take $L \equiv L_1 L_2 \cdots L_{n-1}$, $R \equiv R_{n-1} \cdots R_2 R_1$.

2°. In G we have (proving (1))

$$\begin{aligned}(\Sigma^{-1}t\Sigma)k &= R^{-1}q^{-1}L^{-1}tLqRk = R^{-1}q^{-1}tqkR = R^{-1}kq^{-1}tqR \\ &= kR^{-1}q^{-1}L^{-1}tLqR = k(\Sigma^{-1}t\Sigma)\ .\end{aligned}$$

4. Completion of the proof

To complete the proof that the word problem for G in unsolvable, it remains to prove Lemma 6. The proof is in five parts, called (k), (t), (z),

(l), (s). Throughout the proof, Σ is to be a fixed special word for which (1) holds.

Part (k). k is a stable letter for G, the basis being the group G_1 whose defining relations consist of those defining relations of G indicated above, and whose generators are those of G, less k. Now (1) gives

$$k^{-1}(\Sigma^{-1}t\Sigma)k\Sigma^{-1}t^{-1}\Sigma = 1 \text{ in } G ;$$

hence by Lemma 4 (or Lemma 2) we have that $\Sigma^{-1}t\Sigma$ belongs to the subgroup of G_1 generated by $r_i, x, q^{-1}tq$ $(i = 1, \cdots, P)$. By *Note* (ii) after the statement of Lemma 4, there exist $\varphi_1, \cdots, \varphi_n$ and $e_1, \cdots, e_n$ such that

$$\Sigma^{-1}t\Sigma\varphi_1^{e_1} \cdots \varphi_n^{e_n} = 1 \text{ in } G_1 , \tag{2}$$

where $n \geqq 0$, each $e_j = \pm 1$, and each φ_j is one of $r_i, x, q^{-1}tq$. We shall assume that n is minimal.

Part (t). t is a stable letter for G_1, the basis being the group G_2 whose defining relations are indicated above and whose generators are those of G, less k, t. Denoting the left side of (2) by W, Lemma 4 (or Lemma 2) shows that W contains a subword t^eCt^{-e} $(e = \pm 1)$, where C belongs to the subgroup of G_2 generated by l_i, y $(i = 1, \cdots, P)$. Thus $C = L$ in G_2, for some word L in l_i, y. We shall prove that, in G_2,

$$\Sigma = LqR \tag{3}$$

for some word R in r_i, x. (This result corresponds to Boone [2, Th. VI, p. 219].)

Case 1. t^e is the displayed t in (2) and t^{-e} occurs in some factor $\varphi_j^{e_j}$. Here $e = 1$ and C has the form $\Sigma R'q^{-1}$, where R' is a word in r_i, x, so (3) follows.

Case 2. t^e occurs in $\varphi_a^{e_a}$ and t^{-e} occurs in $\varphi_b^{e_b}$ $(a < b)$. Here $W \equiv \cdots (q^{-1}t^eq)R'(q^{-1}t^{-e}q) \cdots$, where R' is a word in r_i, x, hence $C \equiv qR'q^{-1}$. In view of the defining relations $tl_i = l_it$, $ty = yt$, we have, in G_1,

$$t^eqR'q^{-1}t^{-e} \equiv t^eCt^{-e} = t^eLt^{-e} = L = C \equiv qR'q^{-1} ;$$

hence

$$W = \cdots q^{-1}qR'q^{-1}q \cdots = \cdots R' \cdots ,$$

so that we have reduced by two the number of factors $\varphi_j^{e_j}$ in (2); this contradicts the assumption that n is minimal in (2).

Part (z). Let us write the defining relations $\Sigma_i = \Gamma_i$ of T in more detail as $F_iq_{s_i}G_i = H_iq_{g_i}K_i$, and the fixed word Σ as Fq_sG.

Let H_2 be the free product of G_2 and the infinite cyclic group $(z; \varnothing)$. Then (3) holds in H_2. To H_2 add superfluous generators $p_a (a = 0, 1, \cdots, N)$

and corresponding defining relations $p_a = q_a z^{-1}$. In the remaining defining relations of H_2, we may replace every q_a by $p_a z$. The generators q_a are now superfluous; removing them with the defining relations $p_a = q_a z^{-1}$, we obtain a presentation for H_2 whose generators are z, s_b, p_a, x, y, l_i, r_i, and whose defining relations are those of G_2 with q_a replaced everywhere by $p_a z$. Thus instead of $\Sigma_i = l_i \Gamma_i r_i$ we now have

$$F_i p_{s_i} z G_i = l_i H_i p_{g_i} z K_i r_i \ ;$$

and instead of (3), we have (writing p for p_0)

$$(4) \qquad E p_s z G = L p z R \text{ in } H_2 \ .$$

z is a stable letter for H_2, the basis being the group G_3 whose defining relations have been given earlier, and whose generators are s_b, p_a, x, y, l_i, r_i. The isomorphism condition is satisfied if the mapping $A_i \rightarrow B_i$ generates an isomorphism between two subgroups of G_3, where

$$A_i \equiv p_{g_i}^{-1} H_i^{-1} l_i^{-1} F_i p_{s_i} \ , \qquad B_i \equiv K_i r_i G_i^{-1} \ .$$

In fact, both subgroups are free. For example, if

$$(5) \qquad A_{v_1}^{e_1} \cdots A_{v_m}^{e_m} = 1 \text{ in } G_3$$

then, adding defining relations $s_b = p_a = x = y = r_i = 1$, we deduce that

$$l_{v_1}^{-e_1} \cdots l_{v_m}^{-e_m} = 1$$

in the free group with generators l_i. Hence j exists such that $v_j = v_{j+1}$ and $e_j = -e_{j+1}$, which means that two factors cancel in (5).

Note that $z^{-1} A_i z = B_i$ in H_2. Now (4) gives

$$R^{-1} z^{-1} (p^{-1} L^{-1} F p_s) z G = 1 \text{ in } H_2 \ ,$$

so by Lemma 4 and *Note* (ii) following it, $p^{-1} L^{-1} F p_s$ belongs to the subgroup of the basis G_3 generated by A_i ($i = 1, 2, \cdots, P$), or equivalently $v_1, \cdots, v_n, e_1, \cdots, e_n$ exist such that

$$(6) \qquad (p^{-1} L^{-1} F p_s) A_{v_1}^{e_1} \cdots A_{v_n}^{e_n} = 1 \text{ in } G_3 \ ,$$

where $1 \leqq v_j \leqq P$ and $e_j = \pm 1$.

Further, since $z^{-1} A_i z = B_i$, (6) gives

$$z^{-1} (p^{-1} L^{-1} F p_s) z B_{v_1}^{e_1} \cdots B_{v_n}^{e_n} = 1 \text{ in } H_2 \ ,$$

hence

$$(7) \qquad R G^{-1} B_{v_1}^{e_1} \cdots B_{v_n}^{e_n} = 1 \text{ in } H_2 \ .$$

In fact, equation (7) is true in G_3. This follows from Lemma 3, since the left hand side of (7) does not involve z, which is a stable letter for H_2 with basis G_3.

To prove Lemma 6 it is evidently sufficient to prove

LEMMA 8. *Let* $\Sigma \equiv Fq_sG$ *be any special word. If* $v_1, \cdots, v_n$ *and* $e_1, \cdots, e_n$ *and words* L *(in* l_i, y*),* R *(in* r_i, x*) exist such that* (6) *and* (7) *hold, then, in the semi-group* T, Σ *can be transformed into* q *by a sequence of at most* n *elementary transformations.*

PROOF. We use induction on n. If $n = 0$, then by adding defining relations $x = y = l_i = r_i = 1$ we obtain, from (6), (7),

$$p^{-1}Fp_s = 1 \quad \text{and} \quad G^{-1} = 1$$

in the free group on generators s_b, p_a. Hence $G \equiv 1$, $F \equiv 1$ and $p_s \equiv p$ (that is, $s = 0$), so we have

$$\Sigma \equiv Fq_sG \equiv q_0 \equiv q \ ;$$

and the lemma is true.

For the induction step, we may assume that L is of minimal length in (6) and that R is of minimal length in (7). Assume also that Σ can not be transformed into q by at most n elementary transformations in T. We have to obtain a contradiction. First consider (6):

Part (l). If we add the defining relations $r_i = x = 1$ to G_3, we obtain the group

$$G_3^L = (s_b,\ p_a,\ y,\ l_i;\ s_by = yys_b,\ s_bl_i = yl_iys_b) \ ,$$

and (6) holds in G_3^L. The letters l_i are stable for this group, the basis being

$$G_4^L = (s_b,\ p_a,\ y;\ s_by = yys_b) \ .$$

Lemma 4 will be available if the mapping $y^{-1}s_b \rightarrow ys_b$ ($b = 1, 2, \cdots, M$) generates an isomorphism between two subgroups, say M_1 and M_2 respectively, of G_4^L. In fact, both M_1, M_2 are free. For example, considering M_2, if $(ys_{b_1})^{e_1} \cdots (ys_{b_m})^{e_m} = 1$ in G_4^L, then by adding the defining relation $y = 1$ to G_4^L, we deduce that $s_{b_1}^{e_1} \cdots s_{b_m}^{e_m} = 1$ in the free group on s_b, p_a. Hence j exists such that $b_j = b_{j+1}$, $e_j = -e_{j+1}$.

Therefore since $n > 0$ the left side of (6) contains a subword $l_i^eCl_i^{-e}$, C being a word in s_b, p_a, y, where either $e = -1$ and C belongs to M_1, or $e = 1$ and C belongs to M_2.

Case 1. This subword is a subword of $Fp_sA_{v_1}^{e_1} \cdots A_{v_n}^{e_n}$. Then l_i^e occurs in $A_{v_j}^{e_j}$ say and l_i^{-e} occurs in $A_{v_{j+1}}^{e_{j+1}}$. Thus $v_j = i = v_{j+1}$ and $e_j = -e = -e_{j+1}$. Therefore

$$A_{v_j}^{e_j}A_{v_{j+1}}^{e_{j+1}} = 1 \quad \textit{and also} \quad B_{v_j}^{e_j}B_{v_{j+1}}^{e_{i+1}} = 1 \ .$$

By the induction hypothesis, Σ can be transformed into q in at most $n - 2$ steps, contrary to one of our assumptions.

Case 2. The subword is a subword of $p^{-1}L^{-1}$. Here C is a word in y only. Since L^{-1} is reduced, C has the form y^k where the integer k is not zero. $C \equiv y^k$ belongs to M_1 or M_2. We shall prove that $y^k = 1$ in G_3.

Suppose $y^k \in M_1$, the other case being similar. Thus

$$y^k = (y^{-1}s_{b_1})^{d_1} \cdots (y^{-1}s_{b_r})^{d_r} \text{ in } G_4^L .$$

Put $y = 1$; then

$$1 = s_{b_1}^{d_1} \cdots s_{b_r}^{d_r}$$

in the free group on generators s_b, p_a. Hence $r = 0$, or two letters cancel. It follows that $y^k = 1$ in G_4^L, hence $y^k = 1$ in G_3.

Thus *Case* 2 leads to the contradiction that the L^{-1} in (6) can be replaced by L'^{-1} of smaller length.

Case 3. The remaining *case* is when l_i^e occurs in L^{-1} and l_i^{-e} occurs in $A_{v_1}^{e_1}$. Here $e = e_1$ and $i = v_1$. Thus either

$$e_1 = 1 , \qquad C \equiv YFp_s p_{g_i}^{-1} H_i^{-1} \text{ and } C \in M_2 ,$$

or

$$e_1 = -1 , \qquad C \equiv YFp_s p_{s_i}^{-1} F_i^{-1} \text{ and } C \in M_1 ,$$

Y being a word in y only.

We shall consider the case $e_1 = 1$ only; the other case is similar.

First we have $s = g_{v_1} (= g_i)$; for if we put $s_b = y = 1$, then the statement $C \in M_2$ becomes: $p_s p_{g_i}^{-1} = 1$ in the free group on generators p_a.

Hence $b_1, \cdots, b_r, d_1, \cdots, d_r$ exist such that

$$(8) \qquad YFH_i^{-1}(ys_{b_1})^{d_1} \cdots (ys_{b_r})^{d_r} = 1 \text{ in } G_4^L ,$$

where $1 \leqq b_j \leqq M$, $d_j = \pm 1 \, (j = 1, 2, \cdots, r)$. We assume that r is minimal in (8); it can be zero.

Part (s). The s_b are stable letters for G_4^L, the basis being the free group on generators p_a, y. The isomorphism condition is satisfied if the mapping $yy \to y$ generates an isomorphism between two subgroups of this free group (namely the cyclic subgroups generated by y^2 and y); but this is so.

The reader is reminded that, in (8), F and H_i are *positive* words (possibly empty) in the s_b, and Y is a word in y only. We shall prove that F has the form $F \equiv UH_{v_1}$ (i.e., the form UH_i), for some word U. Now positive words W, F', H_i' in the s_b certainly exist such that $F \equiv F'W$, $H_i \equiv H_i'W$, and we suppose W has maximal length, so it is sufficient to prove that $H_i' \equiv 1$. Assume that $H_i' \not\equiv 1$.

Let us replace F and H_i^{-1} in (8) by F' and $H_i'^{-1}$ respectively; we obtain a true equation in G_4^L which we label (8′). At least one stable letter occurs in (8′) so, by Lemma 4, the left hand side contains a subword $J \equiv s_b^e C s_b^{-e}$, where C is a word in p_a, y. But (8′) involves no letters p_a, hence C is a word in y only; and either $e = -1$ and C is a word in y^2, or $e = 1$ and C is a word in y. J can not be a subword in $(ys_{b_1})^{d_1} \cdots (ys_{b_r})^{d_r}$ since r is minimal. s_b^e can not occur in $H_i'^{-1}$, since if it did we would have $e = -1$, and $s_b^{-e} \equiv s_b$ would occur in $(ys_{b_1})^{d_1}$; hence $d_1 = 1$. Thus $C \equiv y$ which is not a word in y^2. It follows that s_b^e occurs in F', s_b^{-e} occurs in $H_i'^{-1}$, and C is empty. Thus the last letter of F' is the inverse of the first letter of $H_i'^{-1}$, contrary to the assumption that W is of maximal length.

Thus we have proved about equation (6) that if $e_1 = 1$, then F has the form UH_{v_1} for some word U. Dually, we can prove that in (7), if $e_1 = 1$ then G^{-1} has the form $V^{-1}K_{v_1}^{-1}$ for some word V^{-1}. This dual argument will now be outlined briefly.

Adding $l_i = y = 1$, (7) holds in

$$G_3^R = (s_b,\ p_a,\ x,\ r_i;\ xs_b = s_b xx,\ r_i s_b = s_b x r_i x)\ .$$

The letters r_i are stable, the basis being $G_4^R = (s_b,\ p_a,\ x;\ xs_b = s_b xx)$. By Lemma 4, the left hand side of (7) contains a subword $r_h^f C' r_h^{-f}$ $(1 \leqq h \leqq P)$ where C' is a word in s_b, p_a, x and either $f = -1$ and C' belongs to the subgroup of G_4^R generated by the $s_b x$, or $f = 1$ and C' belongs to the subgroup generated by the $s_b x^{-1}$. If this subword is a subword of $G^{-1}B_{v_1}^{e_1} \cdots B_{v_n}^{e_n}$, then following *Case* 1 we obtain the contradiction that Σ can be transformed into q in at most $n - 2$ steps. If the subword is a subword of R, we contradict the assumption that R has minimal length in (7). The remaining case is when r_h^f occurs in R and r_h^{-f} occurs in $B_{v_1}^{e_1}$. Here $f = -1$ and $h = v_1$. C' then has the form $XG^{-1}K_h$, where X is a word in x only, and instead of (8) we have, say,

$$XG^{-1}K_h(s_{b_1}x)^{d_1} \cdots (s_{b_r}x)^{d_r} = 1 \text{ in } G_4^R\ .$$

It is now easy to follow the previous argument and obtain $G^{-1} \equiv V^{-1}K_h$ for some word V^{-1}, as required.

We recall that it has also been proved that in (6) the subscripts, s, v_1 are connected by the equation $s = g_{v_1}$. Denoting v_1 by i, we have

$$\Sigma \equiv Fq_sG \equiv UH_iq_sK_iV \equiv UH_iq_{g_i}K_iV\ .$$

Put $\Sigma^* \equiv UF_iq_{s_i}G_iV$. Then in T, the word Σ can be transformed into Σ^* by one elementary transformation. Write $F^* \equiv UF_i$ and $G^* \equiv G_iV$ so that $\Sigma^* \equiv F^*q_{s_i}G^*$. In G_3 we have

$$\begin{aligned}(p^{-1}L^{-1}Fp_s)A_{v_1}^{e_1} &\equiv p^{-1}L^{-1}UH_ip_{g_i}A_i \\ &\equiv p^{-1}L^{-1}UH_ip_{g_i}(p_{g_1}^{-1}H_i^{-1}l_i^{-1}F_ip_{s_i}) = p^{-1}L^{-1}Ul_i^{-1}F_ip_{s_i}\ .\end{aligned}$$

Since U is a positive word in the s_b, a word L_0 in l_i, y exists such that the last word is equal in G_3 to

$$p^{-1}L_0^{-1}UFp_{s_i} \equiv p^{-1}L_0^{-1}F^*p_{s_i} .$$

Thus (6) becomes

$$(6^*) \qquad (p^{-1}L_0^{-1}F^*p_{s_i})A_{v_2}^{e_2} \cdots A_{v_n}^{e_n} = 1 \text{ in } G_3 .$$

Similarly, in G_3,

$$\begin{aligned} RG^{-1}B_{v_1}^{e_1} &\equiv RV^{-1}K_i^{-1}B_i \equiv RV^{-1}K_i^{-1}K_ir_iG_i^{-1} \\ &= RV^{-1}r_iG_i^{-1} = R_0V^{-1}G_i^{-1} \equiv R_0G^{*-1} , \end{aligned}$$

for some word R_0 in r_i, x. Thus (7) becomes

$$(7^*) \qquad (R_0G^{*-1})B_{v_2}^{e_2} \cdots B_{v_n}^{e_n} = 1 \text{ in } G_3 .$$

By the induction hypothesis $\Sigma^* \equiv F^*q_{s_i}G^*$ can be transformed into q in at most $n-1$ steps. But Σ can be transformed into Σ^* in one step, hence Σ can be transformed into q in at most n steps. This completes the induction step for the case $e_1 = 1$.

When $e_1 = -1$ only slight changes have to be made. We find that, in (6), $F \equiv UF_{v_1}$ and $s = s_{v_1}$; in (7), $G^{-1} \equiv V^{-1}G_{v_1}^{-1}$ (for some words U, V^{-1}). The definitions of Σ^*, F^*, G^* in this case are

$$\Sigma^* \equiv UH_iq_{q_i}K_iV , \qquad F^* \equiv UH_i , \qquad G^* \equiv K_iV .$$

This completes the proof of Lemma 8, and hence of the theorem.

Appendix

(I) A remark on Lemma 5. In [8] Post describes a semi-group with generators $s_1, \cdots, s_m, h, q_1, \cdots, q_{R+2}$ and a finite number of defining relations $A_i = B_i$, where each A_i and B_i has one of the forms (1) Sq_aS', (2) hSq_aS', (3) $Sq_aS'h$, where S, S' are possibly empty words in $s_1, \cdots, s_m$, and, for each i, A_i and B_i have the same form. In this semi-group, which we call T', it is recursively unsolvable to determine if an arbitrary word of the form $hSq_aS'h$ is equal to the fixed word $hq_{R+2}h$. If we now make the notational change $h = s_{m+1}$, and add the new generator q_0 with the defining relation $hq_{R+2}h = q_0$, we obtain Lemma 5, though in a different notation.

(II) The referee has pointed out that, in Lemma 5, one may take all the generators q_a to be equal (i.e., $N = 0$). If this is done, the introduction of the generator z in *Part* (z) of § 4 can be avoided, and there are one or two simplifications later in the proof.

To see this, add to the semi-group T' in (I) the new generator v and, in each defining relation such that A_i and B_i have type (3), replace h by v; we obtain a new semi-group T_1. Call a word of T_1 special if it has the form $hSq_aS'v$. It is easily deduced that in T_1 it is recursively unsolvable to determine for an arbitrary special word Σ whether or not $\Sigma = hq_{R+2}v$ in T_1. Now let T_2 be obtained from T_1 by adding the defining relation $hq_{R+2}v = 1$. Then, for any special word Σ of T_1, $\Sigma = hq_{R+2}v$ in T_1 if and only if $\Sigma = 1$ in T_2. (If $\Sigma = 1$ in T_2, one first shows that the last elementary transformation, if any, of the form "Replace XY by $Xhq_{R+2}vY$" can be dispensed with.) Let us re-name the generators of T_2, x_k ($k = 1, 2, \cdots, K$) and the defining relations $C_j = D_j$ ($j = 1, 2, \cdots, J$). Let T_3 be the semigroup whose generators are x_k, q and whose defining relations are $qC_j = qD_j$, $qx_k = x_kq$ ($k = 1, 2, \cdots, K; j = 1, 2, \cdots, J$). It is easily shown (cf. Boone [2, Th. X, p. 250]) that $\Sigma = 1$ in T_2 if and only if $q\Sigma = q$ in T_3. Thus T_3 has the desired properties that Lemma 5 is true for it and $N = 0$.

(III) The referee has asked whether or not Lemma 4 could be generalized to cover the case when E^* has the form

$$\mathcal{E}^* = \left(S, p_v(v \in V); D, F_ip_{v_i}G_i = H_ip_{w_i}K_i(i \in I)\right),$$

where now w_i need not equal v_i. Such a generalization is provided by Theorem A below.

First we need a definition. Let T, U be words over S and let $v, w \in V$. We say that Tp_v *produces* p_wU if the word Tp_v can be transformed into p_wU by a sequence of operations of the form

$$XA_ip_{v_i}Y \to Xp_{w_i}B_iY \quad \text{or} \quad XA_i^{-1}p_{w_i}Y \to Xp_{v_i}B_i^{-1}Y,$$

where X, Y are arbitrary words and, as in § 2, $A_i \equiv H_i^{-1}F_i$, $B_i \equiv K_iG_i^{-1}$.

If Tp_v produces p_wU, it is readily shown that T is a word in the A_i ($i \in I$), say $T \equiv w(A_i)$, and U is the corresponding word $w(B_i)$ in the B_i. Further, it is obvious that $Tp_v = p_wU$ in $\mathcal{E}^*$.

THEOREM A. *If the strong isomorphism condition holds, and if* $W = 1$ *in* $\mathcal{E}^*$, *where* W *involves at least one letter* $p_v(v \in V)$, *then* W *contains a subword* (i) $p_w^{-1}Cp_v$ *or* (ii) $p_wCp_v^{-1}$, *where* C *is a word over* S. *In case* (i) C *is equal in the basis* $(S; D)$ *to a word* $w(A_i)$ *and* $w(A_i)p_v$ *produces* $p_ww(B_i)$. *In case* (ii) C *is equal in the basis to a word* $w(B_i)$ *and, again,* $w(A_i)p_v$ *produces* $p_ww(B_i)$.

REMARKS. 1. The proof of Theorem A is fairly straightforward. The theorem can be reduced to Lemma 4 by making use of the idea that, if we choose one defining relation $F_ip_{v_i}G_i = H_ip_{w_i}K_i$ such that $v_i \neq w_i$, then we can eliminate the generator p_{v_i} from $\mathcal{E}^*$ by means of this defining relation, the equation $W = 1$ being modified accordingly.

2. Theorem A is true if we replace the strong isomorphism condition by the following weaker condition. Call $i, j \in I$ equivalent if $p_{v_i} = p_{v_j}$ in the free group obtained from $\mathcal{E}^*$ by putting all letters in S equal to 1. The new condition is that, for each equivalence class J, the mapping $A_i \rightarrow B_i (i \in J)$ generates an isomorphism between two subgroups of the basis.

3. The example $\mathcal{E}^* = (S, p_1, p_2; D, Fp_1G = Hp_2K)$ shows that even the weak condition is not necessary for Theorem A to be true. The weakest possible condition, at any rate when V, I are finite, would be a formalization of the statement "If $\mathcal{E}^*$ is reduced by Tietze transformations to the form of E^*, then the isomorphism condition of § 2 is satisfied."

4. *Part* (z) of § 4 would be simplified by having Theorem A in the place of Lemma 4, but only slightly so. The construction involving the new generator z would be avoided; but, apart from this, there would hardly be any saving.

5. The conclusion of Theorem A clearly implies that, in the language of § 0, W can be transformed into the empty word without using insertions of any p_v^{-1}. The converse can be proved.

UNIVERSITY OF ILLINOIS

REFERENCES

1. W. W. BOONE, *Certain simple unsolvable problems of group theory*, Nederl. Akad Wetensch. Ser. A
Part I, 57 (1954), 231-237;
Part II, 57 (1954), 492-497;
Part III, 58 (1955), 252-256;
Part IV, 58 (1955), 571-577;
Part V, 60 (1957), 22-27;
Part VI, 60 (1957), 227-232.
2. ———, *The word problem*, Ann. of Math., 70 (1959), 207-265.
3. J. L. BRITTON, *Solution of the word problem for certain types of groups*, Proc. Glasgow Math. Assoc.
Part I, Vol. III (1956), 45-54;
Part II, Vol. III (1957), 68-90.
4. ———, *The word problem for groups*, Proc. London Math. Soc. (3), 8 (1958), 493-506.
5. G. HIGMAN, *Subgroups of finitely presented groups*, in publication.
6. A. G. KUROSH, The Theory of Groups, Vol. II, Chelsea Publishing Co., 1956.
7. P. S. NOVIKOV, *On the algorithmic unsolvability of the word problem in group theory* (Russian), Trudy Mat. Inst. Steklov, no. 44, 1955. (An English translation is available: American Math. Soc. Translation.)
8. E. L POST, *Recursive unsolvability of a problem of Thue*, J. Symb. Logic, 12 (1947), 1-11.

9. V. A. Tartakovskii, *The sieve method in group theory*, Mat. Sbornik, N. S. 25 (67) (1949), 3-50.
10. ———, *Application of the sieve method to the solution of the word problem for certain types of groups*, Mat. Sbornik, N. S. 25 (67) (1949), 251-274.
11. ———, *Solution of the word problem for groups with a k-reduced basis for* $k > 6$, Isvestiya Akad. Nauk, SSSR, Ser. Mat., 13 (1949), 483-494.

(American Math. Soc. Translation no. 60 (1952) is a translation of 9, 10, 11.)