

AN ALGEBRAIC CHARACTERIZATION OF GROUPS WITH SOLUBLE WORD PROBLEM¹

Dedicated to the memory of Hanna Neumann

WILLIAM W. BOONE² and GRAHAM HIGMAN

(Received 10 July 1973)

Communicated by M. F. Newman

Introduction and Statement of Results

The following theorem is the focal point of the present paper. It stipulates an algebraic condition equivalent, in any finitely generated group, to the solubility of the word problem.

THEOREM I. *A necessary and sufficient condition that a finitely generated group G have a soluble word problem is that there exist a simple group H , and a finitely presented group K , such that G is a subgroup of H , and H is a subgroup of K .*

We also show the following result in the last section of this article.³

THEOREM II. *The exact analogue for semi-groups of Theorem I.*

For some time we have been aware of a parallel between the inconsistency or completeness, in the absolute sense, of a logical system on the one hand, and the triviality or simplicity of a group given by generators and relations on the other; however, even though, in logic, *complete* is often equivalent to *decidable*,

1. An abstract of this paper, as an address given to The Association for Symbolic Logic, Bristol, August 1973, will appear in *The Journal of Symbolic Logic*. The authors are indebted to J. L. Britton, D. J. Collins, P. M. Neumann and P. E. Schupp for various suggestions regarding exposition.

2. Research of the first author currently or recently supported by the United Kingdom Science Research Council, U.S. National Science Foundation and Air Force Office of Scientific Research. He is also very grateful to the Mathematical Institute, and All Souls' College, both of Oxford, whose hospitality made this joint work possible.

3. We define (*congruence*) *simple semi-group* in this last section.

it remained to Richard Thompson to note, in his oral presentation of McKenzie-Thompson [12]⁴ at the 1969 Irvine Conference, that a finitely presented simple group has a soluble word problem. This fact, while obvious after a moment's reflection, seems never to have been noted before, much less used. This idea was our starting point for Theorem I.

In the proof of the necessity of Theorem I, the H and K are constructed from G and $A(G)$, any algorithm solving the word problem for G . The proof of the sufficiency of the theorem furnishes us with an algorithm solving the word problem for this G via the H and the K , without reference to $A(G)$. It is now tempting to argue that the proof of Theorem I thus shows the existence of a uniform algorithm solving the word problem in all finitely generated groups having a soluble word problem. But such an argument is illusory: for while the procedure given is conceptually uniform, it does not constitute a uniform recursive method in the technical sense. Indeed, it is a result of Boone-Rogers [4] that such a uniform algorithm cannot exist.

We do have the following result regarding uniform algorithms, Theorem III, which was suggested to us by Peter Neumann as an improvement on Theorem III'.

THEOREM III.⁵ *A necessary and sufficient condition that any recursively enumerable class Γ of finitely presented groups have a uniformly soluble word problem is that there exist a simple group H , and a finitely presented group K , such that for each member G of Γ , G is a subgroup of H , and H is a subgroup of K .*

We show the sufficiency of Theorem III in the following constructive form.

THEOREM III'. *Let H, K be any fixed pair of groups such that H is simple, K is finitely presented, and H is a subgroup of K . Then there exists a partial recursive functional Φ , from finite presentations of groups to algorithms such that if G is, in fact a subgroup of H , then the result of applying Φ to any finite presentation of G is an algorithm solving the word problem for G .*

Following the proofs of Theorems III and III', we discuss informally an analogue of Theorem III' for groups which are not necessarily finitely presented.

Throughout this article we restrict considerations to groups and semi-groups

4. Numbers in square brackets [] refer to the references at the end of this paper.

5. By Theorem III and Boone-Rogers [3] just cited, there cannot exist some one simple group containing every finitely generated group with soluble word problem and which is itself contained in some finitely presented group.

Note that, in view of the Tietze Transformation Theorem, the existence of an algorithm uniformly solving the word problem for any collection of finitely presented groups is an algebraic invariant, in the following sense: given such an algorithm relative to any recursively enumerable collection of the corresponding finite presentations, we can find another such uniform algorithm relative to any other such collection presenting the same collection of abstract groups

which are countable, but not necessarily finitely generated. We admit group presentations, and semi-group presentations, consisting of an infinite number of generators and a completely arbitrary set of defining relations; but, without explicitly saying so, we always require the (symbols for the) generators to form a recursive set. (Indeed, in principle we could always take the positive integers as the generators.) If a group — or semi-group — G is not finitely generated, then the solubility of the word problem for G is not an algebraic invariant, but the solubility of the word problem for any particular presentation is still well defined. Any group, or semi-group, does have at least one presentation, — that given by its Cayley table. We leave it to the interested reader to see that a proof of Theorem IV.1 is given, with only minor changes of wording, by our proof of the necessity of Theorem I, and at the end of that proof, we make the few comments needed to further obtain Theorem IV.2.

THEOREM IV. *Let G be any group and $\Pi(G)$ any presentation of G . Then (IV.1) there exists a simple group H with presentation $\Pi(H)$, such that G is a subgroup of H and the word problems for $\Pi(G)$ and $\Pi(H)$ are Turing equivalent. Further, (IV.2) if $\Pi(G)$ has soluble word problem, then there exists a group K with finite presentation $\Pi(K)$ such that H is a subgroup of K and $\Pi(K)$ has soluble word problem (as well as $\Pi(G)$ and $\Pi(H)$).*

Let S be any set of positive integers. Then the group presentation with generators g_1, g_2, \dots and defining relations $g_i = 1$ if and only if $i \in S$ has word problem Turing equivalent to the decision problem for S . Thus we have the following result.

COROLLARY TO THEOREM IV. *For any Turing degree of insolubility D , not necessarily recursively enumerable, there exists a presentation $\Pi(H)$ of a simple group H such that the word problem for $\Pi(H)$ has degree D .*

Except for Theorem IV.2, each of our results about groups has an exact analogue for semi-groups whose proof should be clear to the reader from the proof of the original group result plus the proof of Theorem II. Except in our comments about Theorem IV.2, we do not discuss the matter further. In giving the proof of Theorem II in our last section, beyond a certain point, we do not give all details when these should be clear by analogy with the proof of Theorem I. Our original proof of Theorem II was a modification of the well-known construction of Markov [13, 14] showing that certain properties of finitely presented semi-groups cannot be recursively recognized. The present proof contains a modification suggested to us by Dana Scott.

Various natural questions suggest themselves. Is every finitely generated group G with soluble word problem embeddable in some finitely presented simple group? (By Theorem 6, page 428, Clapham [7], 'No' would imply 'No, even for finitely presented G .') Can one algebraically characterize finitely generated groups

with soluble conjugacy (i.e., transformation) problem? What about algebraically characterizing classes of groups with soluble isomorphism problem? ⁶

Preliminaries

At this point the reader must have section 2 of Britton [5] and section 2 of Boone [3] before him, — but no other portions of these papers are required. (Instead of Boone [3], one could refer to Clapham [6], or, presumably, Fridman [8] just as well.) We note that Lemmas 3 and 4 of Britton [5] (“Britton’s Lemma”) hold for our group presentations consisting of a recursive set of generators and an arbitrary set of defining relations. For even if one assumes these lemmas only for extensions having a finite number of stable letters over a given basis, the lemmas then follow, by a trivial compactness argument, for extensions having an infinite number of stable letters. This is clear since any consequence is a consequence of a finite subset of the defining relations. Lemma 1 of Boone [3] also holds for presentations in our sense, — if, where f_v is the isomorphism from $A(v)$ to $B(v)$, the decision problem P_3 is interpreted as the problem to determine of an arbitrarily given pair U, v , U a word of E , $v \in V$, whether or not $U \in A(v)$ (alternatively, $B(v)$) and, when the answer be ‘yes’ to determine $f_v(U)$ (alternatively, $f_v^{-1}(U)$). The proof as originally given remains valid. Indeed, it is a demonstration of the existence of a recursive functional which, when it is applied to an algorithm solving $WP(E)$, i.e., the word problem for E , and P_3 as newly interpreted, yields an algorithm solving $WP(E^*)$. Or, as we shall say, $WP(E^*)$ is uniformly soluble in $WP(E)$ and P_3 .

We now assume some fixed recursive procedure to recursively enumerate all the words of an arbitrarily given presentation of a group or semi-group. We call this enumeration the *canonical ordering*. From now on, we use the same letter for a group and its presentation, but we often say ‘the group G ’ or ‘the presentation G ’ when what is meant might not otherwise be clear. Except in the final section on semi-groups, ‘presentation’ means group presentation.

Theorem I: Proof of Necessity; Theorem IV 2.

We show the necessity of Theorem I in the following strengthened form which we require for application later.

THEOREM I’. *Suppose G is any presentation such that WP (presentation G) is soluble. Then one can construct a presentation of a simple group H , and a finite presentation of a group K , such that G is a subgroup of H , and H is a subgroup of K .*

⁶. It is trivial that Theorem I is false in the variety of abelian groups.

Where G is any presentation and W_i is the i th word in the canonical ordering of the words of G , G^\dagger is to be the presentation whose generators consist of the generators of G plus the generators $t, u_i, v_i, i = 1, 2, \dots$; and whose defining relations consist of the defining relations of G plus

- (1) $u_i^{-1}tu_i = tW_i, \quad i = 1, 2, \dots;$
- (2) $v_j^{-1}tv_j = t^{-1}W_j^{-1}tW_j, \quad j = 1, 2, \dots \text{ and } W_j \neq 1 \text{ in } G.$

Again where G is any presentation and W any word of G , G^W is the presentation obtained from G by adding $W = 1$ as an additional defining relation. Clearly, the group G is simple if and only if for each word W of G such that $W \neq 1$ in G , the group G^W is trivial.

LEMMA 0. *Let G be any presentation and W a word of G such that $W \neq 1$ in G . Then for all words Y of G , $Y = 1$ in G^{tW} .*

From $W=1$ and the relations (2), $t = 1$ in G^{tW} . Hence $Y = 1$ in G^{tW} by the relations (1).

LEMMA 1. *For any presentation G , the group G is embedded in the group G^\dagger via the identity map.*

Clearly G is embedded in $G * \langle t \rangle$, the free product of G and $\langle t \rangle$, the infinite cyclic group on t . We wish to complete the argument by showing that the presentation G^\dagger is the kind of extension of presentation $G * \langle t \rangle$ considered in Higman-Neumann-Neumann [11], i.e., apply Lemma 3 of Britton [5]. To do this, it is only necessary to verify what Britton calls the isomorphism condition, for certainly the generators and relations of presentation G^\dagger are of the appropriate form. But to check this condition we need only observe, as follows from the normal form theorem for free products, that each of the following subgroups of $G * \langle t \rangle$ is infinite cyclic on the displayed generator: $\langle t \rangle$ itself; for each $i, i = 1, 2, \dots$, $\langle tW_i \rangle$, the subgroup generated by tW_i ; for each $j, j = 1, 2, \dots$, such that $W_j \neq 1$ in G , $\langle [t, W_j] \rangle$, the subgroup generated by $t_j^{-1}W_j^{-1}tW_j$.

LEMMA 2. *For any presentation G , WP (presentation G^\dagger) is uniformly soluble in WP (presentation G).*

The lemma will follow at once from Lemma 3 of Boone [3] — recall our remark at the end of Preliminaries —, if we can show that each of the following decision problems is uniformly reducible to WP (presentation G). Here, generalizing the notation of the proof of Lemma 1, $\langle [t, W_j] \rangle$ is the trivial subgroup if $W_j = 1$ in G . Where W is an arbitrarily given word of the presentation $G * \langle t \rangle$ and i is an arbitrarily given positive integer, to determine whether or not

(2.1) $W \in \langle t \rangle;$

(2.2) $W \in \langle tW_i \rangle;$

(2.3) $W \in \langle [t, W_i] \rangle.$

We show 2.3 is uniformly soluble in WP (presentation G), — the other problems are handled similarly. Suppose given W, i ; bear in mind constantly that we have an algorithm solving WP (presentation G) and the normal form theorem for free products. If $W_i = 1$ in G , then $W \in \langle [t, W_i] \rangle$ if and only if $W = 1$ in G . Suppose $W_i \neq 1$ in G . Then freely reduce W , — to say W' . If W' is 1 then $W \in \langle [t, W_i] \rangle$. If W' is not 1 but t -free, then $w \notin \langle [t, W_i] \rangle$. If W' is not 1 and not t -free suppose W' is

$$P_0 t^{\varepsilon_1} P_1 t^{\varepsilon_2} \dots t^{\varepsilon_n} P_n$$

where the $\varepsilon_m = \pm 1$ and the P_m are t -free. Then $W \in \langle [t, W_i] \rangle$ if and only if n is even, $\varepsilon_1 = -1$, and $\varepsilon_{m+1} = -\varepsilon_m, m = 1, 2, \dots, n - 1$, and either (A) $P_0 = 1$ in G , and for $m \neq 0, P_m = W_i^{\varepsilon_m}$ in G ; or (B) $P_n = 1$ in G , and for $m \neq n, P_m = W_i^{-\varepsilon_m}$.

Now for any presentation G , let $G^{(0)}$ be G , and $G^{(n+1)}$ be $G^{(n)\dagger}$. Further, let $G^{(\infty)}$ be the presentation having as generators and defining relations, the generators and defining relations of all the $G^{(n)}, n = 0, 1, \dots$. We now write $W_{i,n}$ for the i th term of the canonical ordering of words of $G^{(n)}$; and $t_{n+1}, u_{i,n+1}, v_{i,n+1}$, respectively, for the t, u_i, v_i of $G^{(n)\dagger}$. The rank of a word W of $G^{(\infty)}$ is the maximum last subscript on any u, v , or t occurring in W , but 0 if W is a word of $G^{(0)}$.

LEMMA 3. *For any presentation G , where $m, n = 0, 1, \dots, m \leq n$, the group $G^{(m)}$ is embedded in the group $G^{(n)}$ via the identity map.*

By induction on $n - m$ using Lemma 1.

LEMMA 4. *For any presentation G , suppose $W = 1$ in $G^{(\infty)}$. Then $W = 1$ in $G^{(N)}$ where W is of rank N .*

For $W = 1$ in $G^{(\infty)}$ as a consequence of only a finite number of defining relations of $G^{(\infty)}$ involving only a finite number of generators, say all falling within $G^{(m)}$ so that $W = 1$ in $G^{(m)}$. But $N \leq m$ and $W = 1$ in $G^{(N)}$ by Lemma 3.

LEMMA 5. *Where $n = 0, 1, \dots$, the group $G^{(n)}$ is embedded in the group $G^{(\infty)}$ via the identity map.*

Immediate, by Lemmas 3 and 4.

LEMMA 6. *For any presentation G , the group $G^{(\infty)}$ is simple.*

Suppose W and Y are words of $G^{(\infty)}$, $W \neq 1$ in $G^{(\infty)}$; let N be the maximum of their ranks. By Lemma 5, $W \neq 1$ in $G^{(N)}$. By Lemma 0, $Y = 1$ in $G^{(N+1)W}$. Since each generator and relation of $G^{(N+1)W}$ is among those of $G^{(\infty)W}$, $Y = 1$ in $G^{(\infty)W}$.

LEMMA 7. For any presentation G , WP (presentation $G^{(\infty)}$) is uniformly soluble in WP (presentation G).

For any word W of $G^{(\infty)}$, $W = 1$ in $G^{(\infty)}$ if and only if $W = 1$ in $G^{(N)}$ where W has rank N , as follows by Lemmas 4 and 5. To obtain an algorithm solving $WP(G^{(N)})$ make an N -fold application of the recursive functional of Lemma 2 to the algorithm solving $WP(G)$.

It is now an easy matter to complete the proof of the necessity of Theorem I. Let G be an arbitrary finitely generated group with soluble word problem. Then by Lemmas 5 and 6, the group $G^{(\infty)}$ is the desired simple group H in which G is embedded. But further, the group $G^{(\infty)}$ has a presentation in terms of a recursive set of generators, $t_n, u_{i,n}, v_{i,n}, i, n = 1, 2, \dots$, and a certain recursive set of defining relations, viz., $W = 1$ for each word W of $G^{(\infty)}$ such that, in fact, $W = 1$ in $G^{(\infty)}$. By Lemma 7 this is a recursive set. Penultimately, then, by a result of Higman-Neumann-Neumann [11], $G^{(\infty)}$ can be embedded in a group N having a presentation consisting of two generators and a recursively enumerable set of defining relations. Finally, by the central result of Higman [10], N can be embedded in a finitely presented group K .⁷

Remark regarding Theorem IV.2: To see this result holds, (A) check that the two generator embedding of Higman-Neumann-Neumann [11] preserves the Turing degree; (B) refer to Theorem 6, p. 428, Clapham [7] which asserts that the embedding result of Higman [10] that we have just cited can also be carried out so as to preserve the Turing degree. There is a known semi-group analogue of the embedding result of Higman [10], viz., that given by Murskii [16], cited below in the final section on semi-groups. But, since no one has yet shown the semi-group analogue of the Clapham result just noted, the present paper does not give in principle a proof of the semi-group analogue of Theorem IV.2.⁸

Theorem I: Proof of Sufficiency

We first remark that (+) *there exists a recursive functional Ω which, when applied to a finite presentation V of a group, yields $\Omega(V)$ a recursive enumeration of all the consequent relations of V .*

Assume now the algebraic condition of Theorem I. If H is trivial so also is G and thus has a soluble word problem. Suppose H non-trivial. Let P_0 be a word of

⁷. Or, for a recent proof by Aanderaa of Higman's result, see Aanderaa [1] or the last chapter of Rotman [17].

⁸. The two-generator embedding result of Hall [9] cited below in the semi-group section does have a Turing degree preserving form, i.e., Equivalence Theorem 2, page 562 of Boone [2].

H such that $P_0 \neq 1$ in H . The word P_0 is to remain fixed throughout our discussion. Let ϕ be the map embedding G in H and ψ the one embedding H in K . The map, consisting of ϕ followed by ψ , embedding G in K is recursive, since its behaviour is determined by its behaviour on the finitely many generators of G . Using $\{U\}_X$ for the normal closure of the element U in the group X , we have that for any P of H , $P \neq 1$ in H ,

$$\psi(P_0) \in \psi(H) = \psi(\{P\}_H) \subseteq \{\psi(P)\}_K.$$

This is so by the assumed embeddings and since H is simple. Thus, for any element W of G , if $W \neq 1$ in G , then $\phi(W) \neq 1$ in H and $\psi(P_0) \in \{\psi(\phi(W))\}_K$, i.e., $\psi(P_0) = 1$ in the presentation $K^{\psi(\phi(W))}$. Conversely, if, where W is any element of G , $\psi(P_0) = 1$ in the presentation $K^{\psi(\phi(W))}$, then $W \neq 1$ in G .

Now suppose W is an arbitrarily given word of G for which we wish to determine ‘Is $W = 1$ in G ?’ First, compute $\psi(\phi(W))$. Second, apply the Ω of remark + to both K and $K^{\psi(\phi(W))}$. Thirdly, check simultaneously through the recursive enumerations $\Omega(K)$ and $\Omega(K^{\psi(\phi(W))})$ until either $\psi(\phi(W)) = 1$ is located in the first or $\psi(P_0) = 1$ in the second. And the answer is, accordingly as the first or second alternative, ‘Yes’ or ‘No’.

Proof of Theorem III

Suppose Γ has a uniformly soluble word problem. Then, by the normal form theorem for free products, G_Γ , the obvious presentation of the free product of the members of Γ , has a soluble word problem and contains each member of Γ as a subgroup. Applying Theorem I’ to G_Γ gives the necessity of Theorem III.

To show the sufficiency of Theorem III, i.e., Theorem III’, let presentation G be arbitrarily given with the group G embedded in H and hence in K . We now use a technique of Miller [15], page 43. Since presentation G has only a finite number of defining relations there is a recursive enumeration, say $\sigma_1, \sigma_2, \dots$, of all homomorphisms of G into K . If H is trivial so is G ; so let P_0 be some fixed element of H , $P_0 \neq 1$ in H , and ψ the map embedding H in K . Then for any word W of presentation G , $w \neq 1$ in G if and only if $\Omega(K^{\sigma_i(W)})$ for some $i, i = 1, 2, \dots$, contains the consequence $\psi(P_0) = 1$. The argument is exactly like our proof of necessity of Theorem I and Ω has the meaning given there. By checking along the finite diagonals of a recursive enumeration of recursive enumerations

$$\Omega(K^{\sigma_1(W)}), \Omega(K^{\sigma_2(W)}), \Omega(K^{\sigma_3(W)}), \dots$$

to locate the consequence $\psi(P_0) = 1$, if, in fact $W \neq 1$ in G we shall determine that such is the case. I.e., the set of words $\neq 1$ in G is recursively enumerable. Since the set of words $= 1$ in G is also, we have an algorithm solving $WP(G)$.

A Variation of Theorem III'

Let the groups H and K be as in Theorem III, and, to avoid a triviality, say H is non-trivial. Let ψ be the map embedding H in K . Suppose that we somehow know that a certain finitely generated group G is embedded in H .

Suppose that, in addition to presentation K , we are given the following items of mathematical notation: (1) Where g_1, g_2, \dots, g_N , represent a set of generators of G , and λ is the map embedding G in K ,

$$\lambda(g_1), \lambda(g_2), \lambda(g_3), \dots, \lambda(g_N)$$

as N words of the presentation K ; (2) Where P_0 is an element of H , $P_0 \neq 1$ in H ,

$$\psi(P_0)$$

as a word of presentation K . Then, on the basis of these items of information alone, we have an algorithm solving $WP(G)$. Given a word W of G , i.e., a word on the g_i 's, for which we wish to determine 'Is $W = 1$ in G ?', compute $\lambda(W)$. Then, much as in the proofs of Theorems I' and III, $W = 1$ in G if and only if $\Omega(K)$ contains $\lambda(W) = 1$; and $W \neq 1$ in G if and only if $\Omega(K^{\lambda(W)})$ contains the consequence $\psi(P_0) = 1$.

Semi-groups

Now 'presentation' is always to mean semi-group presentation. We extend the notation WP and the term 'uniformly soluble' given at the end of Preliminaries for groups, to semi-groups. Lest it be misunderstood, the term 'simple semi-group' is defined in a moment. As with groups, we tolerate a notational confusion between a semi-group and its presentation. Any semi-group is to have a unity, 1.

The necessity of Theorem II is shown in the following strengthened form.

THEOREM II' *Suppose S is any presentation such that WP (presentation S) is soluble. Then one can construct a presentation of a simple semi-group H , and a finite presentation (i.e., Thue system) presenting a semi-group K , such that S is a sub-semi-group of H , and H is a sub-semi-group of K .*

Where S is any presentation, and H_i is the i th word in the canonical ordering of the words of S , S^\dagger is the presentation whose generators are those of S plus

$$b, c_i, d_i, \quad i = 1, 2, \dots$$

and whose relations are those of S plus the following. Here $i = 1, 2, \dots$ throughout.

$$c_i G d_i = 1 \quad \text{for each word } G \text{ of } S \text{ such that } G \neq H_i \text{ in } S;$$

$$c_i H_i d_i = b$$

$$bW = b, Wb = b, \quad \text{for each word } W \text{ of } S^\dagger.$$

Again where S is any presentation and U, V any words of S , $S^{U,V}$ is the presentation whose generators are those of S and whose defining relations are those of S plus $U = V$. Essentially the definition of (congruence) simplicity for semi-groups is this: the semi-group S is called simple if, for any words U, V of S such that $U \neq V$ in S , the semi-group $S^{U,V}$ is trivial.

LEMMA A. *Suppose U, V are any words of S such that $U \neq V$ in S . Then for any word W of S^\dagger , $W = 1$ in $S^{U,V}$. I.e., $S^{U,V}$ is trivial.*

Where V is H_i , $1 = c_i U d_i$ and $c_i V d_i = b$ are defining relations in S^\dagger , hence hold in $S^{U,V}$. Thus, since $U = V$ in $S^{U,V}$, $1 = b$ in $S^{U,V}$. Consequently for any word W of S^\dagger , $W = Wb = b = 1$ in $S^{U,V}$. This is so since $Wb = b$ is a defining relation of S^\dagger and thus holds in $S^{U,V}$.

We now⁹ use $U =_0 V$ in S^\dagger to mean that $U = V$ in S^\dagger without application of the defining relations $1 \rightarrow c_i G d_i$ where $G \neq H_i$ in S , i.e., without replacement of 1 by $c_i G d_i$. Further, \bar{H}_i is a variable for words of S which are $\neq H_i$ in S ; \bar{b} , for words of S^\dagger having form $c_i G d_i$ where $G = H_i$ in S , for some i , or b itself.

LEMMA B. *Suppose W and U are words of S^\dagger neither containing as subword any \bar{b} or $c_i \bar{H}_i d_i$ for any i , $i = 1, 2, \dots$. Then $W = U$ in S^\dagger implies $W =_0 U$ in S^\dagger .*

The idea of the argument goes back to Markov [13, 14]. No step of a proof from W to U in S^\dagger contains a \bar{b} . If the proof uses n applications of the rule that 1 can be replaced by $c_i G d_i$, $G \neq H_i$ in S , consider, if $n > 0$, the last such application. It must be followed by a replacement of $c_i G' d_i$ by 1 , where $G = G'$ and $G' \neq H_i$ in S , since U contains no subword of form $c_i \bar{H}_i d_i$. Following Markov, the lemma now is seen to hold by induction on n .

LEMMA C. *For any words W and U of S , $W = U$ in S if and only if $W = U$ in S^\dagger . I.e., the semi-group S is embedded in the semi-group S^\dagger by the identity map.*

Suppose $W = U$ in S^\dagger . Then by Lemma B, since W and U are words of S , $W =_0 U$ in S^\dagger . But this last proof from W to U in S^\dagger is free of \bar{b} , c_i , and d_i for each i , and thus valid in S .

LEMMA D. *For any presentation S , WP (presentation S^\dagger) is uniformly soluble in WP (presentation S).*

For any word X of S^\dagger , let $c[X]$ be the result of removing from X all subwords of the form $c_i \bar{H}_i d_i$ in some canonical way, so that, since $WP(S)$ is soluble, $c[X]$ is recursively computable. Obviously, since $c_i \bar{H}_i d_i = 1$ is a defining relation of S^\dagger ,

⁹. One should read $P = Q$ in presentation T as meaning there exists a *proof* from P to Q in T , i.e., a finite sequence of 'steps' passing from P to Q , with each step resulting from the preceding step by use of a defining relation of T .

$c[X] = X$ in S^\dagger for any word X of S^\dagger . Where $U_0, U_1, \dots, U_m, V_0, V_1, \dots, V_n$ are words of S and where $u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_n$ are each one of the c_i or d_j of S^\dagger ,

$$\text{Cond}_*(U_0 u_1 U_2 \dots U_{m-1} u_m U_m, V_0 v_1 V_1 \dots V_{n-1} v_n V_n)$$

means (i) $m = n$; (ii) u_j is $v_j, j = 1, 2, \dots, n$; (iii) $U_j = V_j$ in $S, j = 0, 2, \dots, n$.

Then the following table determines recursively of two arbitrarily given words W, U of S^\dagger whether or not $W = U$ in S^\dagger .

Does $c[W]$ contain some b as a subword?	Does $c[U]$ contain some b as a subword?	Is $W = U$ in S^\dagger ?
Yes	Yes	Yes
Yes	No	No
No	Yes	No
No	No	$W = U$ in S^\dagger if and only if $\text{Cond}_*(c[W], c[U])$

That the table specifies an algorithm is trivial. In view of the first paragraph of the proof of this lemma and Lemma B we have that $W = U$ in S^\dagger if and only if $c[W] =_0 c[U]$ in S^\dagger . From this last fact, it is easy to see, moreover, that this algorithm furnishes the correct answer.¹⁰

The last part of the statement of the lemma follows from the uniformity of our construction.

For any presentation S , let $S^{(0)}$ be S , and $S^{(n+1)}$ be $S^{(n)\dagger}, n = 0, 1, \dots$. Further let $S^{(\infty)}$ be the presentation having as generators and defining relations the generators and defining relations of all the $S^{(n)}$.

The remainder of the argument for Theorem II' is the exact analogue of that for Theorem I', with $S^{(\infty)}$ playing the role of $G^{(\infty)}$, and we leave details to the reader. Analogous to Lemma 5, 6, and 7, one has that the semi-group S is embedded in the semi-group $S^{(\infty)}$ via the identity map, that the semi-group $S^{(\infty)}$ is simple, and that WP (presentation $S^{(\infty)}$) is uniformly soluble in WP (presentation

¹⁰. The last line of the table is seen to hold by induction on the number of steps of a proof verifying $c[W] =_0 c[U]$ in S^\dagger . Such a proof is valid in the system obtained from S by adding c_i and d_i as additional generators; it thus consists of independent vertical strips lying between the 'free' c_i and d_i and each of which is a valid proof in S . Cf. Lemma 31 of Boone [2], but the present situation is much simpler.

S). Finally, to embed $S^{(\infty)}$ in a semi-group K , one first uses Hall [9] to embed $S^{(\infty)}$ in a semi-group N having a presentation consisting of two generators and a recursively enumerable set of defining relations; and then uses Murskii [16], to embed N in a finitely presented semi-group K . This shows Theorem II'.

For the proof of the sufficiency of Theorem II, we use $\{T\}$ for the collection of equations which are consequences of the semi-group presentation T . Suppose, then, that ϕ embeds the finitely generated semi-group S in the simple semi-group H , and that ψ embeds H in the finitely presented semi-group K . We wish to solve $WP(S)$. If H is trivial so is S . Assuming H non-trivial, let U_0, V_0 be some fixed pair of words of H , such that $U_0 \neq V_0$ in H , which remains fixed throughout the discussion. Then for any pair of words, U, V , of H such that $U \neq V$ in H ,

$$\psi(U_0) = \psi(V_0) \in \psi\{H^{U,V}\} \subseteq \{K^{\psi(U),\psi(V)}\}$$

Here, $\psi\{H^{U,V}\}$ is the collection of consequences of K of form $\psi(P) = \psi(Q)$ where $P = Q \in \{H^{U,V}\}$. The reader should now be able to complete the argument because of a strong analogy with the proof of sufficiency of Theorem I. ¹¹

¹¹. *Added in proof, July 1974*: Since the submission of this article, we have learned of its relation to the work of Kuznecov on the one hand and that of B. H. Neumann, Simmons and MacIntyre on the other. In his note, *Uspehi Mat. Nauk*, (1958), page 240, A. V. Kuznecov announced, without proof, that the class \mathfrak{S} of finitely generated groups with soluble word problem is characterized by embeddability in a simple algebra which is finitely presented in a suitable variety. It would thus seem that it was Kuznecov who here first noted that a finitely presented simple group always has a soluble word problem. Still another algebraic characterization of \mathfrak{S} , viz., embeddability in every non-trivial algebraically closed group, is, in effect, given by the following: Neumann, 'The isomorphism problem for algebraically closed groups', pp. 553–562 of *Word problems: Decision problems and the Burnside problem in group theory*, publication data in reference [1]; H. Simmons, 'The word problem for absolute presentations', *J. London Math. Soc.* (2), 6 (1973), 275–280; A. MacIntyre, 'Omitting quantifier-free types in generic structures', *Jour. Symbolic Logic*, 37 (1972) 512–520. That this is so follows from their results as formally stated (see page 512 of MacIntyre's paper) and the total triviality that any finitely generated group with soluble word problem has a recursive presentation. See Boone, 'Between logic and group theory', *Second Intern. Congress for Group Theory at Canberra*, Springer-Verlag (1974).

References

- [1] S. Aanderaa, 'A proof of Higman's embedding theorem, using Britton extensions of groups', 1–17 of *Word problems: decision problems and the Burnside problem in group theory*, W. W. Boone, F. B. Cannonito, R. C. Lyndon, editors, *Studies in Logic and Foundations of Mathematics Series*, North-Holland Publishing Company, Amsterdam-London, 1973.
- [2] W. W. Boone, 'Word problems and recursively enumerable degrees of unsolvability. A first paper on Thue systems', *Annals of Mathematics* 83 (1966), 520–571.

- [3] W. W. Boone, 'Word problems and recursively enumerable degrees of unsolvability. A sequel on finitely presented groups', *Annals of Mathematics* 84 (1966), 49–84.
- [4] W. W. Boone, and H. Rogers, Jr., 'On a problem of J. H. C. Whitehead and a problem of Alonzo Church', *Math. Scand.* 19 (1966), 185–192.
- [5] J. L. Britton, 'The word problem', *Annals of Mathematics* 77 (1963), 16–32.
- [6] C. R. J. Clapham, 'Finitely presented groups with word problems of arbitrary degrees of insolubility', *Proc. London Math. Soc. Series 3*, 14 (1964), 633–676.
- [7] C. R. J. Clapham, 'An embedding theorem for finitely generated groups', *Proc. London Math. Soc. (Ser. 3)*, 17 (1967), 419–430.
- [8] A. A. Fridman, Degrees of unsolvability of the problem of identity in finitely presented groups (in Russian), Izdalel'sto 'Nauka', Moscow 1967, 193.
- [9] M. Hall, Jr., 'The word problem for semi-groups with two generators', *J. Symbolic Logic*, 14 (1949), 115–118.
- [10] G. Higman, 'Subgroups of finitely presented groups', *Proceedings of the Royal Society A*, 262 (1961), 455–475.
- [11] G. Higman, B. H. Neumann, and H. Neumann, 'Embedding theorems for groups', *J. London Math. Soc.* 24 (1949), 247–254.
- [12] R. McKenzie and R. J. Thompson, 'Unsolvable word problems', 457–478 of Word problems: decision problems and the Burnside problem in group theory. Publication data are above in reference [1].
- [13] A. A. Markov, 'Impossibility of algorithms for recognizing some properties of associative systems' (in Russian), *Doklady Akademii Nauk SSSR*, 77 (1951), 953–956. (This paper can be understood completely from a review in *The Journal of Symbolic Logic*, 17 (1952), page 151, by A. Mostowski.)
- [14] A. A. Markov, *Theory of algorithms* (published for the U.S. National Science Foundation by the Israel Program for Scientific Translations, 1961. Available from the Office of Technical Services, U.S. Department of Commerce).
- [15] C. F. Miller, III, *On group-theoretic decision problems and their classification*, *Annals of Mathematics Studies*, No. 68 (Princeton University Press and University of Tokyo Press, 1971).
- [16] V. L. Murskii, 'Isomorphic embedding of a semi-group with an enumerable set of defining relations in a finitely presented semi-group' \mathcal{D} (in Russian), *Mathem. Sametki*, 1, (1967), 217–224.
- [17] J. J. Rotman, *The theory of groups: an introduction*, second edition (Allyn and Bacon, Boston, 1973.)

University of Illinois
 Urbana-Champaign
 Illinois
 U.S.A.

Mathematical Institute
 University of Oxford
 24-29 St Giles
 Oxford OXI, 3LB, England.