

THE WORD PROBLEM*

BY WILLIAM W. BOONE

UNIVERSITY OF MANCHESTER

Communicated by Deane Montgomery, July 7, 1958

INTRODUCTION; SUMMARY OF RESULTS

RESULT a. *There is exhibited a group given by a finite number of generators and a finite number of defining relations and having an unsolvable word problem.*

In the present account the finite presentation of a group used for Result a is much simpler in form than that of UG;¹ moreover, the symmetry argument of Theorem III*, Case 2, UG, Part V, is replaced by the very simple Lemma 7 of UG, Part II. The idea behind this change is that the inverses of the group generators relative to which a presentation is given can be taken as an anti-isomorphic copy of the generators. Since in any group \mathbf{A}^{-1} equals \mathbf{B}^{-1} is a consequence of \mathbf{A} equals \mathbf{B} , \mathbf{PAP}^{-1} equals \mathbf{QAQ}^{-1} of $\mathbf{AP}^{-1}\mathbf{Q}$ equals $\mathbf{P}^{-1}\mathbf{QA}$ —and vice versa—the connection between the old and the new arguments can be seen from the well-known Tietze transformation theorems.²

To obtain Result a, we use a certain Thue system of Post,³ but Result b shows that one may use, instead, any Thue system with an unsolvable word problem.

RESULT b. *There is explicitly given a recursive mapping, φ , from the set of Thue systems into the set of finite presentations of groups such that the equality of the arbitrary words \mathbf{A} and \mathbf{B} in the Thue system \mathfrak{T} is equivalent to the equality of certain words—recursively specified in terms of \mathbf{A} and \mathbf{B} —in the finite group presentation $\varphi(\mathfrak{T})$. Thus if \mathfrak{T} has an unsolvable word problem, so also has $\varphi(\mathfrak{T})$.⁴*

Magnus⁵ has shown that any finite presentation of a group consisting of one non-trivial defining relation has a solvable word problem. The group presentation of Result a has an extremely large number of defining relations. A natural question is this: What is the smallest number of defining relations which a finite presentation of a group with unsolvable word problem can have? How long and how “complicated” must these relations be? Result c gives a program for producing, from Thue systems, “simple-looking” finite presentations of groups having unsolvable word problems. Using an unsolvability result of Dana Scott⁶ on Thue systems, a result noted by Marshall Hall,⁷ and an imbedding theorem for groups of Higman, Neumann, and Neumann,⁸ it follows from Result c that one may exhibit a group given by two generators and thirty-two defining relations and having an unsolvable word problem.

RESULT c. *Let g_1, g_2, \dots, g_N and $\mathbf{A}_1 = \mathbf{B}_1, \mathbf{A}_2 = \mathbf{B}_2, \dots, \mathbf{A}_M = \mathbf{B}_M$ be the generators and defining relations of an arbitrary Thue system \mathfrak{T} . Let \mathbf{P} be any fixed word of \mathfrak{T} . Then $\mathfrak{T}_{\mathbf{P}}$ is the finite presentation of a group depending on \mathfrak{T} and \mathbf{P} and described as follows:*

The $N + 9$ generators of $\mathfrak{T}_{\mathbf{P}}$:

$$g_1, g_2, \dots, g_N; q, t_1, t_2, k, a, b, c, d, e.$$

The $6N + M + 13$ non-trivial defining relations of $\mathfrak{T}_{\mathbf{P}}$:

$$\begin{aligned}
 q\mathbf{A}_j &= d^j e^j a c^j d^j q \mathbf{B}_j b^j c^j a e^j b^j, j = 1, 2, \dots, M \\
 \left. \begin{aligned}
 gq_i &= g_i q \\
 ag_i &= g_i a \\
 cg_i &= g_i c \\
 eg_i &= g_i e
 \end{aligned} \right\} i = 1, 2, \dots, N \\
 \left. \begin{aligned}
 g_i d &= d^{M+1} a d^{M+1} g_i \\
 t_u a &= a t_u \\
 t_u c &= c t_u \\
 t_u d &= d t_u \\
 t_u e &= e t_u
 \end{aligned} \right\} u = 1, 2 \\
 \left. \begin{aligned}
 bg_i &= g_i b^{M+1} a b^{M+1} \\
 ak &= ka \\
 bk &= kb \\
 ck &= kc \\
 ek &= ke
 \end{aligned} \right\}
 \end{aligned}$$

$$t_1 q \mathbf{P} k \mathbf{P}^{-1} q^{-1} t_1^{-1} = t_2 q \mathbf{P} k \mathbf{P}^{-1} q^{-1} t_2^{-1}.$$

For any word \mathbf{W} of \mathfrak{X} , \mathbf{W} equals \mathbf{P} in \mathfrak{X} if and only if

$$t_1 \mathbf{W} k \mathbf{W}^{-1} t_1^{-1} \text{ equals } t_2 \mathbf{W} k \mathbf{W}^{-1} t_2^{-1}$$

in \mathfrak{X}_P . Thus, if it is recursively unsolvable to determine for an arbitrary word \mathbf{W} of \mathfrak{X} whether or not \mathbf{W} equals \mathbf{P} in \mathfrak{X} , then the word problem for \mathfrak{X}_P is unsolvable.

Finally we note a very easy direct proof of the unsolvability of the word problem for the finitely generated infinitely related case.

Demonstration of Result a. The Thue system \mathfrak{X}_1 given below can be taken to be any Thue system having the form stipulated. The Thue system \mathfrak{X}_2 , which depends on \mathfrak{X}_1 , is a finite presentation of a group. We use $\Sigma, \Sigma', \dots, \Gamma, \Gamma', \dots$ as a variable for words on \mathfrak{Z}_1 (i.e., consisting of the symbols of \mathfrak{Z}_1) which are of the form $\Delta q_\alpha \Pi$, where Δ and Π are words on s_1, s_2, \dots, s_M and q_α is q, q_1, \dots or q_N .

$$\begin{aligned}
 \mathfrak{X}_1 \\
 \mathfrak{Z}_1: & \quad s_1, s_2, \dots, s_M; \quad q_1, q_2, \dots, q_N, q; \\
 \mathfrak{U}_1: & \quad \Sigma_1 = \Gamma_1, \Sigma_2 = \Gamma_2, \dots, \Sigma_P = \Gamma_P. \\
 \mathfrak{X}_2
 \end{aligned}$$

\mathfrak{Z}_2 : All symbols of \mathfrak{Z}_1 ; t_1, t_2, k, x, y ; $l, r, \iota = 1, 2, \dots, P$; Each of the above symbols with superscript -1 added.

\mathfrak{U}_2 : Where $\iota = 1, 2, \dots, P, \alpha = 1, 2$, and $\beta = 1, 2, \dots, M$, the following:

$$\begin{aligned}
 2.1 \quad \Sigma_\iota &= l_\iota \Gamma r_\iota \\
 2.2 \quad s_\beta l_\iota &= y l_\iota y s_\beta & 2.6 \quad r_\iota s_\beta &= s_\beta x r_\iota x \\
 2.3 \quad s_\beta y &= y y s_\beta & 2.7 \quad x s_\beta &= s_\beta x x \\
 2.4 \quad t_\alpha l_\iota &= l_\iota t_\alpha & 2.8 \quad r_\iota k &= k r_\iota \\
 2.5 \quad t_\alpha y &= y t_\alpha & 2.9 \quad x k &= k x \\
 2.10 \quad k q^{-1} t_1^{-1} t_2 q &= q^{-1} t_1^{-1} t_2 q k.
 \end{aligned}$$

Where \mathbf{a} and \mathbf{a}^{-1} are symbols of \mathfrak{Z}_2 the following:

$$\begin{aligned}
 2.11 \quad \mathbf{a}^{-1} \mathbf{a} &= 1 \quad (\text{where } 1 \text{ is the empty word}) \\
 2.12 \quad \mathbf{a} \mathbf{a}^{-1} &= 1.
 \end{aligned}$$

A proof of $\mathbf{A/B}$ in $\mathfrak{X}_i, i = 1, 2$, is a finite sequence of words on \mathfrak{Z}_i called steps, say $\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_n$, such that \mathbf{C}_1 is \mathbf{A} and \mathbf{C}_n is \mathbf{B} ; each \mathbf{C}_ν and $\mathbf{C}_{\nu+1}, \nu = 1, 2, \dots, n - 1$, are \mathbf{PDQ} and \mathbf{PEQ} where $\mathbf{D} = \mathbf{E}$ is a rule of \mathfrak{U}_i for some \mathbf{P} and \mathbf{Q} , possibly void.⁹ We abbreviate "there is a proof of $\mathbf{A/B}$ in \mathfrak{X}_i " to $\mathbf{A} \vdash_i \mathbf{B}$.

MAIN THEOREM. For any choice of \mathfrak{X}_1 and $\Sigma, \Sigma \vdash_{-1} q$ if and only if

$$t_1 \Sigma k \Sigma^{-1} t_1^{-1} \vdash_{-1} t_2 \Sigma k \Sigma^{-1} t_2^{-1}.$$

From Post³ we have that for a certain choice of \mathfrak{X}_1 it is unsolvable to determine for arbitrary Σ on \mathfrak{Z}_1 whether or not $\Sigma \vdash iq$. Thus the Main Theorem implies Result a. The "only if" part of the Main Theorem is easy. Let Ξ (Let Ω) be a variable for words on y, y^{-1} , and the symbols l_i, l_i^{-1} of \mathfrak{Z}_2 (on x, x^{-1} , and the symbols r_i, r_i^{-1} of \mathfrak{Z}_2). Suppose $\Sigma \vdash iq$. Then for some Ξ and $\Omega, \Sigma \vdash {}_2\Xi q\Omega$. Consequently—noting $t_1 q k q^{-1} t_1^{-1} \vdash {}_2 t_2 q k q^{-1} t_2^{-1}$ —we have $t_1 \Sigma k \Sigma^{-1} t_1^{-1} \vdash {}_2 t_2 \Sigma k \Sigma^{-1} t_2^{-1}$.

To show the Main Theorem in the non-trivial direction, we first stipulate three additional group presentations, $\mathfrak{X}_3, \mathfrak{X}_4$, and \mathfrak{X}_5 . We define \mathfrak{Z}_3 to be \mathfrak{Z}_2 ; \mathfrak{U}_3 to be \mathfrak{U}_2 with each $ak = ka$ of $\mathfrak{U}_{2,9}$ or $\mathfrak{U}_{2,9}$ replaced by $ak = k$ and $\mathfrak{U}_{2,10}$ replaced by $t_1 q k = t_2 q k$. We define \mathfrak{Z}_4 to be \mathfrak{Z}_3 ; \mathfrak{U}_4 to be \mathfrak{U}_3 with each $at_v = t_v a$ of $\mathfrak{U}_{2,4}$ or $\mathfrak{U}_{2,5}$ replaced by $t_v a = t_v$ and $t_1 q k = t_2 q k$ excluded. We define \mathfrak{Z}_5 to be \mathfrak{Z}_4 with k, k^{-1}, t_v, t_v^{-1} excluded; \mathfrak{U}_5 to be \mathfrak{U}_4 with the rules containing k, k^{-1}, t_v, t_v^{-1} excluded. Let $\mathbf{A} \vdash {}_i \mathbf{B}$, $i = 1, 2, \dots, 5$, mean $\mathbf{A} \vdash \mathbf{B}$ with no occurrences of $q^{-1}, q_0^{-1}, \dots, q_N^{-1}$ in any step. Then the plan of the argument is given below in the first column; the first statement in each brace implies the second.

$t_1 \Sigma k \Sigma^{-1} t_1^{-1} \vdash {}_2 t_2 \Sigma k \Sigma^{-1} t_2^{-1}$	}	¹⁰ Cf. UG, Part II, Sec. 5-7, especially Lemma 7.
$t_1 \Sigma k \Sigma^{-1} t_1^{-1} \vdash {}_2 t_2 \Sigma k \Sigma^{-1} t_2^{-1}$		Roughly speaking, erase all symbols right of k in each step of the \mathfrak{X}_2 proof.
$t_1 \Sigma k \vdash {}_3 k t_2 \Sigma k$		Cf. UG, Part II, Sec. 5-7, especially Lemma 7.
$t_1 \Sigma k \vdash {}_3 k t_2 \Sigma k$		See i below.
$t_1 \Sigma k \vdash {}_4 k t_1 q k$		See ii below.
$\Sigma \vdash {}_5 \Xi q \Omega$ for some Ξ and Ω		See iii below.
$\Sigma \vdash {}_5 \Xi q \Omega$		Cf. UG, Part VI, Sec. 20.
$\Sigma \vdash {}_5 q \Xi q \Omega$		Erase the symbols l_i , or r_i, l_i^{-1}, r_i^{-1} , everywhere in the \mathfrak{X}_5 proof.
$\Sigma \vdash {}_5 q s \Xi q \Omega$		
$\Sigma \vdash iq$		

(i) Omit from the \mathfrak{X}_3 proof all steps following the first application of $t_1 q k = t_2 q k$; then erase from each step remaining all symbols left of t_1 , all right of k . (ii) It is sufficient to show $\mathbf{M}_i \vdash {}_5 \Xi' \mathbf{M}_{i+1} \Omega'$ for some Ξ' and Ω' , where $t_1 \mathbf{M}_i k$ is the i th step of the \mathfrak{X}_4 proof. (iii) Cf. UG, Part II, Sec. 5-7, and Part III. But the argument of Part III can be replaced by an almost trivial one using the techniques of UG, Part VI, Sec. 20 and 21 and the fact that the set of words l_i, l_i^{-1} (or words r_i, r_i^{-1}) is *independent*.¹¹

Demonstration of Result b. Throughout this section, $\mathfrak{X}_0, \mathfrak{X}_*, \mathfrak{X}_{(\mathbf{W})}$, are Thue systems depending on the arbitrary Thue system \mathfrak{X} (with symbols \mathfrak{Z} and rules \mathfrak{U})— $\mathfrak{X}_{(\mathbf{W})}$ depending on the word \mathbf{W} on \mathfrak{Z} as well. Let \mathfrak{Z}_0 contain p, v and \mathbf{a}, \mathbf{a} for each \mathbf{a} of \mathfrak{Z} and let \mathfrak{U}_0 contain the rules of \mathfrak{U} and $\mathbf{a}\mathbf{b} = \mathbf{b}\mathbf{a}, p\mathbf{a}\mathbf{a} = \mathbf{a}p, \mathbf{a}pv = pv$ for each \mathbf{a} of \mathfrak{Z} . Let \mathbf{W} and \mathbf{V} be words on \mathfrak{Z} , \mathbf{V}_0 the word obtained from \mathbf{V} by replacing \mathbf{a} by \mathbf{a} . Then $p\mathbf{V}_0\mathbf{W}v \vdash {}_x p\mathbf{v}$ if and only if $\mathbf{W} \vdash {}_x \mathbf{V}$. Let \mathfrak{Z}_* consist of \mathfrak{Z} and q_1 ; \mathfrak{U} con-

tains $q_1\mathbf{A} = q_1\mathbf{B}$, $q_1\mathbf{a} = \mathbf{a}q_1$ for each $\mathbf{A} = \mathbf{B}$ of \mathfrak{U} and \mathbf{a} of \mathfrak{B} . Then for any \mathbf{W} and \mathbf{V} on \mathfrak{B} , $q_1\mathbf{W} \vdash_{\mathfrak{T}_*} q_1\mathbf{V}$ if and only if $\mathbf{W} \vdash_{\mathfrak{T}} \mathbf{V}$. Let $\mathfrak{B}_{(W)}$ consist of \mathfrak{B} and q ; $\mathfrak{U}_{(W)}$, of \mathfrak{U} and $\mathbf{W} = q$. Then, for any \mathbf{V} on \mathfrak{B} , $\mathbf{V} \vdash_{\mathfrak{T}_{(W)}} q$ if and only if $\mathbf{V} \vdash_{\mathfrak{T}} \mathbf{W}$. Thus for any \mathfrak{T} and words \mathbf{A} and \mathbf{B} on \mathfrak{B} the following statements are equivalent: $\mathbf{A} \vdash_{\mathfrak{T}} \mathbf{B}$; $p\mathbf{B}_0\mathbf{A}v \vdash_{\mathfrak{T}_0} pv$; $q_1p\mathbf{B}_0\mathbf{A}v \vdash_{\mathfrak{T}_{0*}} q_1pv$; $q_1p\mathbf{B}_0\mathbf{A}v \vdash_{\mathfrak{T}_{0*}(q_1pv)} q$. This shows Result b since $\mathfrak{T}_{0*}(q_1pv)$ has the form of \mathfrak{T}_1 used in the demonstration of Result a.

Demonstration of Result c. The argument is a revision of that for Result a. The main points are: (1) the proof of Result a is valid if the q of $\mathfrak{U}_{2,10}$ is interpreted as some fixed special word of \mathfrak{T}_1 and $\mathfrak{U}_{2,10}$ rewritten in the symmetric form of the last relation listed in Result c; (2) if \mathfrak{T} is any Thue system then the \mathfrak{T}_* used for Result b has the form of \mathfrak{T}_1 used for Result a; (3) the set of words $c^j e^j$, $j = \pm 1, \pm 2, \dots$, $\pm M$ is independent,¹¹ as is the set $c^{\pm 1}, e^{\pm 1}, d^{\pm 1}, b^{M+1}ab^{M+1}, b^j c^j a^j b^j$ $j = 0, \pm 1, \dots$, $\pm M$.

Result c and \mathfrak{T}_0 . Starting with an arbitrary system \mathfrak{T} , the Thue system \mathfrak{T}_0 (see Result b) can be identified with the \mathfrak{T} of Result c. Thus if \mathfrak{T} has an unsolvable word problem, so has \mathfrak{T}_{0pv} . Using this construction in connection with Scott's result yields a forty defining relation group with unsolvable word problem that can actually be written down in a few minutes' time.¹²

*The Word Problem for the Finitely Generated Infinitely Related Case.*¹³ Where S is any set of ordered pairs of positive integers, let \mathfrak{T}_S be the following group presentation.

$$\begin{aligned} \mathfrak{B}_S: & \quad z, x_1, x_2, q \\ \mathfrak{U}_S: & \quad z^m x_1^n q x_1^{-n} = x_2^n q x_2^{-n} \quad \text{for each } (m, n) \text{ of } S. \\ & \quad z = 1 \end{aligned}$$

THEOREM. $x_1^n q x_1^{-n} \vdash_{\mathfrak{T}_S} x_2^n q x_2^{-n}$ if and only if there is an m such that (m, n) is a member of S .

The theorem implies the desired unsolvability result, for we may take any well-known S such that (1) there is a recursive procedure to determine for an arbitrary pair of positive integers, (m, n) , whether or not (m, n) is a member of S ; (2) there is no recursive procedure to determine for arbitrary n whether or not there is an m such that (m, n) is a member of S .¹⁴

* The author is a John Simon Guggenheim Memorial Fellow. This research was supported earlier by the Institute for Advanced Study, National Science Foundation contract G-1974, and the U.S. Educational Foundation in Norway.

¹ W. W. Boone, "Certain Simple Unsolvable Problems of Group Theory," *Koninkl. Ned. Akad. Wetenschap.*, Ser. A, Part I, 57, 231-237, 1954; Part II, pp. 492-497; Part III, 58, 252-256, 1955; Part IV, pp. 571-577; Part V, 60, 22-27, 1957; Part VI, pp. 227-232. In Part V, last line of p. 24, read "and 7" after "6" and "their" for "its." We have attempted to make the present note as self-contained as possible.

² The relation of our work to P. S. Novikov, *On the Algorithmic Unsolvability of the Word Problem in Group Theory* (Trudy Mat. Inst. Steklov, No. 44 [1955]) (in Russian), is still essentially unknown to us (see A. A. Markov, *Math. Rev.*, 17, 706; an A.M.S. translation of Novikov by K. A. Hirsch is in preparation). Through J. L. Britton we do know that Novikov uses the symmetry argument of UG, Part V. At the British Mathematical Colloquium, Nottingham, September, 1957, Britton announced a new proof of the unsolvability of the word problem based to some extent on Novikov's proof. Our Results b and c were presented at this colloquium. Result a—using the \mathfrak{T}_2 given below but with the old symmetry argument—on a Fulbright Inter-Foundation Lectureship tour in the United Kingdom in May, 1957.

³ E. L. Post, *J. Symb. Logic*, 12, 1–11, 1947.

⁴ In the sense of Post, the word problem for \mathfrak{X} is *reducible to that for* $\varphi(\mathfrak{X})$.

⁵ W. Magnus, *Math. Annalen*, 106, 295–307, 1932.

⁶ Dana Scott, abstract, *J. Symb. Logic*, 21, 111–112, 1956.

⁷ Marshall Hall, *J. Symb. Logic*, 14, 115–118, 1949.

⁸ G. Higman, B. H. Neumann, and H. Neumann, *J. London Math. Soc.*, 24, 247–254, 1949.

⁹ As defined, UG, Part I, p. 234.

¹⁰ Also provable by Theorem I of Higman, Neumann, and Neumann, *op. cit.*, as pointed out to us by Higman.

¹¹ The set of words A_1, A_2, \dots, A_K on \mathfrak{B} is *not* independent if there is a product of the A 's, with no adjacent A 's inverses of each other, which equals 1 in the free group on \mathfrak{B} .

¹² The 32 defining relation group mentioned above has one relation which is astronomical in length.

¹³ Included in a report filed with the National Science Foundation on contract G-1974, May 28, 1956—but in a form more akin to UG, Parts V–VI, than Result a as presently shown (cf. W. Craig, *J. Symb. Logic*, 18, 30–32, 1953, and B. H. Neumann, *J. London Math. Soc.*, 12, 125, Theorem (13), 1937).

¹⁴ For related material see W. W. Boone, abstract, *Bull. A.M.S.*, 62, 148, 1956.

*NON-ADDITIVE FUNCTORS, THEIR DERIVED FUNCTORS,
AND THE SUSPENSION HOMOMORPHISM*

BY ALBRECHT DOLD AND DIETER PUPPE

MATHEMATISCHES INSTITUT DER UNIVERSITÄT HEIDELBERG

Communicated by Saunders Mac Lane, July 3, 1958

1. *Derived Functors of Non-additive Functors.*—Let T be a (covariant) functor of modules over a ring Λ to modules over a ring Λ' . If T is additive its derived functors have been defined by Cartan-Eilenberg.² Additivity is used to show that T applied to a chain homotopy again gives a chain homotopy (cf.² IV, 5, and V, 3). Using *FD-complexes*⁴ instead of chain complexes, we define left derived functors for arbitrary functors T .

1.1. *Definition.*—A *projective FD-resolution of type n* of the module M is an *FD-module* P such that (i) $P_j = 0$ for $j < n$, (ii) P_j is projective for all j , (iii) $H_n(P) = M, H_j(P) = 0$ for $j \neq n$.

Passing from an *FD-module* to its normal(ized) chain module establishes a 1 to 1 correspondence (up to natural equivalences) between *FD-modules*, *FD-maps*, *FD-homotopies* and chain modules, chain maps, chain homotopies.³ In particular, it establishes such a correspondence between projective *FD-resolutions* P of type n of M and chain modules C for which $C_j = 0$ for $j < n$ and

$$0 \leftarrow M = H_n(C) \leftarrow C_n \leftarrow C_{n+1} \leftarrow C_{n+2} \leftarrow \dots \tag{1.2}$$

is an ordinary projective resolution² of M . From the corresponding properties of ordinary resolutions it follows: Every module has a projective *FD-resolution* of any given type n . If $f: M \rightarrow M'$ is a homomorphism and P, P' are projective *FD-resolutions* of type n of M, M' resp., then there exists an *FD-map* $F: P \rightarrow P'$ such that $F_*: H_n(P) \rightarrow H_n(P')$ equals f . Moreover, if F' is another such map, then F, F' are *FD-homotopic* (cf. Cartan-Eilenberg,² V, 1).