

# THE ORDER PROBLEM AND THE POWER PROBLEM FOR FREE PRODUCT SIXTH-GROUPS

by JAMES McCOOL

(Received 17 August, 1967)

**Introduction.** Let  $G$  be a group given in terms of generators and defining relations. The *order problem* is said to be solvable for (the given presentation of)† the group  $G$  if, given any element  $W$  of  $G$  (as a word in the given generators of  $G$ ), we can determine the order of  $W$  in  $G$ . The *power problem* is solvable for  $G$  if, given any pair  $X, Y$  of elements of  $G$ , we can determine whether or not  $X$  belongs to the cyclic subgroup  $\{Y\}$  of  $G$  generated by  $Y$ . It is easy to see that if either of these problems is solvable for  $G$ , then the word problem is also solvable for  $G$ .

A solution to the order problem for free sixth-groups is contained in the work of Greendlinger [4], while Lipschutz [6] has solved the power problem for such groups. In [6] Lipschutz conjectured that similar results hold for the free product sixth-groups (FPS-groups) studied by Britton [2], [3]. In this paper we show that this is the case, by obtaining conditions under which the order problem and the power problem are solvable for FPS-groups. These conditions are derived from the algebraic results of [3] and [7], together with a result (Theorem 1) which we state without proof. The proof of Theorem 1 will be given in a later paper.

The FPS-groups we study may have an infinite number of generators and defining relations, and we show by means of two examples that the order problem and the power problem are not solvable in general for presentations of such groups, even when they have solvable word problems.

**1. Notation.** Let  $S$  be a set. A *word* in the elements of  $S$  is a finite sequence of elements of  $S$ , each with an index  $+1$  or  $-1$ . The inverse  $\omega^{-1}$  of the word

$$\omega = x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n} \quad (x_i \in S, \epsilon_i = \pm 1, i = 1, 2, \dots, n)$$

is the word  $x_n^{-\epsilon_n} x_{n-1}^{-\epsilon_{n-1}} \dots x_1^{-\epsilon_1}$ . Let  $D$  be a subset of the set  $W(S)$  of all words in  $S$ . In a well known way the *presentation*  $(S; D)$  determines an abstract group  $G$ . Thus every word  $\omega$  in  $S$  represents a unique element of  $G$  denoted by  $\|\omega\|$ ; the empty word represents the identity element  $I$  of  $G$ , and two words  $\omega, \omega'$  represent the same element of  $G$  if (and only if) one can be obtained from the other by a finite number of deletions or insertions of words of the form  $x^{+1}x^{-1}$  or  $x^{-1}x^{+1}$  or  $R^{\pm 1}$  ( $x \in S, R \in D$ ).

The group  $G$  is said to be *recursively presented* if there is given a presentation  $(S; D)$  of  $G$  such that the set  $S$  of *generators* is effectively enumerable and the set  $D$  of *defining relators* is recursively enumerable; that is,  $D$  is given as  $u_1, u_2, u_3, \dots$ , where, in some given effective enumeration of  $W(S)$  (obtained from the effective enumeration of  $S$ ),  $u_n$  is the  $f(n)$ th element of  $W(S)$ , and  $f(n)$  is a recursive function of  $n$ . This definition is due to Higman [5].

† The presence of this phrase in such statements is necessary, as the examples of §5 show; we shall omit it however when no ambiguity is likely to arise.

A

Let  $\Pi$  be the free product of the set of groups  $\{G_\gamma; \gamma \in \Gamma\}$  and let the following conditions be satisfied.

(a) The set  $\Gamma$  is effectively enumerable.

(b) Each  $G_\gamma$  ( $\gamma \in \Gamma$ ) is given by a recursive presentation  $(S_\gamma; D_\gamma)$ , where the sets  $S_\gamma$  are pairwise disjoint.

Then  $\Pi$  has generators  $S = \bigcup_{\gamma \in \Gamma} S_\gamma$  and defining relators  $D = \bigcup_{\gamma \in \Gamma} D_\gamma$ , and it is clear that  $(S; D)$  is a recursive presentation of  $\Pi$ . In particular, given any element  $s$  of  $S$ , we can determine the  $S_\gamma$  containing  $s$  in a finite number of steps.

We say that a word  $\omega$  in  $S$  is  $\Pi$ -reduced if it is a word of the form

$$\omega_{\gamma(1)}\omega_{\gamma(2)} \dots \omega_{\gamma(n)},$$

where  $n \geq 1$ ,  $\omega_{\gamma(i)} \in S_{\gamma(i)}$ ,  $\gamma(i) \neq \gamma(i+1)$  ( $i = 1, 2, \dots, n-1$ ) and  $\|\omega_{\gamma(i)}\| \neq I$  ( $i = 1, 2, \dots, n$ ). If  $\omega$  is  $\Pi$ -reduced it follows that  $\|\omega\|$  has free product normal form  $\|\omega_{\gamma(1)}\| \|\omega_{\gamma(2)}\| \dots \|\omega_{\gamma(n)}\|$  and free product length  $n$ .

We impose a further condition on  $\Pi$ .

(c) The word problem is solvable for each  $G_\gamma$ , that is, given any pair of words  $x, y$  in the elements of  $S_\gamma$ , we can determine whether or not  $\|x\| = \|y\|$ .

We can now give an algorithm (first described in [2]) to obtain from an arbitrary word  $\omega$  in  $S$  a word  $\omega'$  such that  $\|\omega\| = \|\omega'\|$  and  $\omega'$  is either  $\Pi$ -reduced or is the empty word. We first bracket together the symbols in the word  $\omega$  so that all symbols in a bracket belong to the same set  $S_\gamma$  and symbols in adjacent brackets belong to different sets. We then have  $\omega = \omega_1 \omega_2 \dots \omega_n$  say, where  $\omega_i \in S_{\gamma(i)}$  and  $\gamma(i) \neq \gamma(i+1)$  ( $i = 1, 2, \dots, n-1$ ). We next delete each  $\omega_i$  for which  $\|\omega_i\| = I$ ; this is possible since the word problem is solvable for each  $G_\gamma$ . After a finite number of repetitions of these steps we arrive at the required word  $\omega'$ .

It follows that the word problem is solvable for  $\Pi$ , since a  $\Pi$ -reduced word does not represent the identity element of  $\Pi$ . In view of this, and in order to simplify the terminology, we shall work from now on in terms of elements of  $\Pi$  rather than in terms of words in  $S$ . Thus we restate the result of the paragraph above as: Given an element  $W$  of  $\Pi$ , we can determine the normal form of  $W$  and the length of  $W$ .

We shall denote elements of  $\Pi$  of length one by small letters and general elements of  $\Pi$  by capital letters. We write  $x \sim y$  or  $x \sim' y$  according to whether  $x$  and  $y$  belong to the same constituent group  $G_\gamma$  of  $\Pi$  or not. We define  $\beta(X, Y)$  and  $\varepsilon(X, Y)$  to be the number of cancellations and amalgamations, respectively, in the product  $X.Y$ , and put

$$\alpha(X, Y) = \beta(X, Y) + \varepsilon(X, Y).$$

Clearly, given  $X$  and  $Y$ , we can determine  $\beta(X, Y)$  and  $\varepsilon(X, Y)$ . If  $X = X_1.X_2 \dots X_r$  and  $l(X) = \sum_{i=1}^r l(X_i)$ , we write  $X = X_1 X_2 \dots X_r$ . If the element  $W$  of  $\Pi$  has normal form  $x_1 x_2 \dots x_n$  ( $n \geq 1$ ), we put  $\text{In}(W) = x_1$ ,  $\text{Fin}(W) = x_n$ . If  $n \geq 2$  and  $x_1 \sim' x_n$ , the elements

$$x_r x_{r+1} \dots x_n x_1 x_2 \dots x_{r-1} \quad (r = 1, 2, \dots, n)$$

are called the cyclic arrangements of  $W$ .

We define the *cyclic length* of  $W \in \Pi$ , written  $l^0(W)$ , by

$$l^0(W) = \text{Min} \{l(X) : X \text{ a conjugate of } W\}.$$

It is easy to describe a finite process to obtain from any element  $W$  of  $\Pi$  a conjugate element  $X$  of  $\Pi$  such that  $l^0(W) = l(X)$ .

**2. The set  $\Omega$ .** Let  $\Omega$  be a set of elements of  $\Pi$  and  $[\Omega]$  the normal subgroup of  $\Pi$  generated by  $\Omega$ , where the quotient group  $\Pi/[\Omega]$  of  $\Pi$  is an FPS-group; i.e., for any elements  $R, R'$  of  $\Omega$ , the following conditions are satisfied:

- (1)  $l(R) \geq 7$ .
- (2)  $\text{In}(R) \sim' \text{Fin}(R)$ .
- (3) Every cyclic arrangement of  $R$  and  $R^{-1}$  belongs to  $\Omega$ .
- (4) Either  $R' = R^{-1}$  or  $6\alpha(R', R) < \text{Min}(l(R'), l(R))$ .
- (5)  $\text{Max} \alpha(R_1, V) \neq 0$ , where  $R_1$  is a cyclic arrangement of  $R$  or  $R^{-1}$  and  $V$  is an element of  $\Omega$  such that  $R_1 \cdot V \neq I$ .

We denote by  $|X|$  the image of the element  $X$  of  $\Pi$  under the natural homomorphism of  $\Pi$  onto  $\Pi/[\Omega]$ , and write  $X \approx Y$  if  $X$  and  $Y$  are elements of  $\Pi$  such that  $|X| = |Y|$ .

We define the subset  $\Omega_1$  of  $\Pi$  to consist of all elements  $U$  of  $\Pi$  such that  $U$  is a subword of some element  $R$  of  $\Omega$  (i.e.,  $R = XUY$  for some  $X$  and  $Y$ ) and  $l(U) \geq [\frac{1}{2}l(R)]$ . We impose the following conditions on  $\Pi/[\Omega]$ .

- (d) The set  $\Omega$  is recursively enumerable.
- (e) Given any element  $W$  of  $\Pi$ , we can determine whether or not  $W$  belongs to  $\Omega_1$ .

Let  $W$  be an element of  $\Omega_1$ . It follows from properties (3) and (4) of  $\Omega$  that there exist unique elements  $R, T$  of  $\Pi$  such that  $R = WT$  and  $R \in \Omega$ . (For, since  $W \in \Omega_1$ , there exists  $R_1 \in \Omega$  such that  $R_1 = XWY$ , and then  $R = WYX$  belongs to  $\Omega$ . Now, if  $R' = WT'$  belongs to  $\Omega$ , then  $\alpha(R^{-1}, R') \geq l(W) \geq [\frac{1}{2}l(R)] > \frac{1}{6}l(R)$  and so  $R = R'$ .) Given  $W \in \Omega_1$ , we can determine this  $R$  and  $T$ , for, since  $\Omega$  is recursively enumerable, we have an explicit enumeration  $R_1, R_2, \dots$  of the elements of  $\Omega$ . We test if  $R_1$  is of the form  $WT$ , and, if not, then we test  $R_2, R_3, \dots$ ; the testing process must terminate since we know that some  $R_i$  in the enumeration has the required form. The element  $T^{-1}$  is called the *complement* of  $W$ , written  $\mathcal{C}W$ . We note that  $\mathcal{C}W \approx W$  since  $R \approx I$ . If  $W$  is a subword of the element  $Z$  of  $\Pi$ ,  $Z = XWY$  say, then the element  $P = X \cdot T^{-1} \cdot Y$  of  $\Pi$  is called the *result of replacing  $W$  in  $Z$  by  $\mathcal{C}W$* , and, if  $l(P) < l(Z)$ , we say that  $Z$  is  $\Omega$ -reducible by  $W$ . The element  $Z$  is said to be  $\Omega$ -reduced if  $Z \neq I$  and  $Z$  contains no subword by which it is  $\Omega$ -reducible. Britton [3] has proved (see Lemma 3 of [7]) that, if  $Z$  is  $\Omega$ -reduced, then  $Z \not\approx I$ . We note that, if  $Z$  is  $\Omega$ -reducible by  $W$  and  $P$  is the result of replacing  $W$  in  $Z$ , then  $P \approx Z$ , since  $W \approx \mathcal{C}W$ .

We now state a theorem concerning  $\Omega$ -reduced elements of  $\Pi$ . The proof of this result will be given in a later paper.

**THEOREM 1.** *Let  $A, B$  be  $\Omega$ -reduced elements of  $\Pi$  such that  $A \approx B$ . Put  $n = l(A), m = l(B)$ . Then  $n \leq 6^m m$ .*

**COROLLARY 1.** *Let  $A \approx B$ , where  $A$  is  $\Omega$ -reduced and  $l(B) = 1$ . Then  $A = B$ .*

*Proof.* It is easy to see that any element of length one is  $\Omega$ -reduced. Hence the conditions of Theorem 1 are satisfied and so we have  $l(A) \leq 6$ . Thus  $l(A \cdot B^{-1}) \leq 7$  and  $A \cdot B^{-1} \approx I$ . From (ii) of the theorem of [3], it follows that either  $A = B$  or  $A \cdot B^{-1} = AB^{-1} \in \Omega$ , since  $l_0 = \text{Min}\{l(R) : R \in \Omega\} \geq 7$ . Now, if  $AB^{-1}$  belongs to  $\Omega$ , then  $A$  belongs to  $\Omega_1$  and  $l(A) = 6$ . This contradicts the fact that  $A$  is  $\Omega$ -reduced, since replacing the subword  $A$  of  $A$  by  $\mathcal{C}A = B$  yields an element of length one. Hence we must have  $A = B$ .

The element  $Z$  of  $\Pi$  is said to be *cyclically  $\Omega$ -reduced* if either  $l(Z) = 1$ , or  $l(Z) > 1$  and the following conditions are satisfied:

- (i)  $\text{In}(Z) \sim' \text{Fin}(Z)$ .
- (ii)  $l(Z) \leq l^0(P)$  for any  $P$  which is the result of replacing a subword  $W$  of  $Z$ .
- (iii) Every cyclic arrangement of  $Z$  satisfies (ii).

We note that, if  $Z$  is cyclically  $\Omega$ -reduced, then so is every cyclic arrangement of  $Z$  or  $Z^{-1}$ ; also  $Z$  is  $\Omega$ -reduced.

**3. Preliminary results.**

**LEMMA 1.** *Given any element  $W$  of  $\Pi$ , we can determine whether or not  $W$  is cyclically  $\Omega$ -reduced. If  $W$  is not cyclically  $\Omega$ -reduced, then we can find  $U, V$  such that  $W \approx U^{-1} \cdot V \cdot U$  and  $V$  is either cyclically  $\Omega$ -reduced or is the identity.*

*Proof.* The proof is by induction on  $n = l(W)$ . The result holds if  $n = 1$ , since then  $W$  is cyclically  $\Omega$ -reduced, and also if  $n = 0$ , since then  $W = I$  and we can take  $U = V = I$ . We suppose that  $n > 1$  and that the result holds for any element of length less than  $n$ . If  $\text{In}(W) \sim \text{Fin}(W)$ , we put  $W' = \{\text{In}(W)\}^{-1} \cdot W \cdot \text{In}(W)$ . Then  $W'$  has length less than  $W$  and so, by the induction hypothesis, we can find  $U, V$  such that  $W' \approx U^{-1} \cdot V \cdot U$  and  $V$  is either cyclically  $\Omega$ -reduced or is the identity. Now  $W \approx \text{In}(W) \cdot U^{-1} \cdot V \cdot U \cdot \{\text{In}(W)\}^{-1}$  and so the result holds for  $W$ . Thus we can assume that  $\text{In}(W) \not\sim \text{Fin}(W)$ .

Since  $W$  has only finitely many cyclic arrangements and each cyclic arrangement has only finitely many subwords, we can determine all the cyclic arrangements  $W'$  of  $W$  which contain a subword belonging to  $\Omega_1$ . If no such  $W'$  is found, then  $W$  is cyclically  $\Omega$ -reduced and the result follows. If we find a  $W'$  containing a subword  $Y$  belonging to  $\Omega_1$ , then we can determine  $\mathcal{C}Y$  and hence the result  $W''$  of replacing  $Y$  in  $W'$ . Now, if we do not find a  $W''$  such that  $l^0(W'') < l(W)$ , then it follows that  $W$  is cyclically  $\Omega$ -reduced; if we find a  $W'$  and  $W''$  such that  $l^0(W'') < l(W)$ , then we can find elements  $T, T_1, A$  of  $\Pi$  such that  $W = T^{-1} \cdot W' \cdot T$ ,  $W'' = T_1^{-1} \cdot A \cdot T_1$  and  $l(A) = l^0(W'') < l(W)$ . Using the induction hypothesis, we can find elements  $U, V$  of  $\Pi$  such that  $A \approx U^{-1} \cdot V \cdot U$  and  $V$  is either cyclically  $\Omega$ -reduced or is the identity. Now, since  $W' \approx W''$ , we have  $W \approx T^{-1} \cdot T_1^{-1} \cdot U^{-1} \cdot V \cdot U \cdot T_1 \cdot T$ , and so the result holds for  $W$ . This concludes the proof of the lemma.

The following result is proved in a similar way.

**LEMMA 2.** *Given any element  $W$  of  $\Pi$ , we can determine whether or not  $W$  is  $\Omega$ -reduced. If  $W$  is not  $\Omega$ -reduced, then we can find an element  $W'$  of  $\Pi$  such that  $W' \approx W$  and  $W'$  is either  $\Omega$ -reduced or is the identity.*

Combining this result with the fact that, if  $Z$  is  $\Omega$ -reduced, then  $Z \approx I$ , we obtain (Theorem 2 of [2]).

**THEOREM 2.** *Let  $\Pi/[\Omega]$  be an FPS-group satisfying conditions (a) to (e). Then the word problem is solvable for  $\Pi/[\Omega]$ .*

We now impose another condition on  $\Pi/[\Omega]$ .

(f) Given any element  $J$  of  $\Pi$ , we can determine whether or not there exist a positive integer  $r$  and an element  $R$  of  $\Omega$  such that  $J^r = R$ .

We have

**LEMMA 3.** *Let  $W$  be an element of  $\Pi$  such that  $l(W) > 1$  and  $W$  is cyclically  $\Omega$ -reduced. Then we can determine the order of  $|W|$  in  $\Pi/[\Omega]$ .*

*Proof.* It was shown in [7] that  $|W|$  has finite order if and only if there exist  $J \in \Pi$ ,  $R \in \Omega$  and positive integers  $m, n$  such that  $W = J^m, R = J^n$ .

Now, if there is an element  $J$  of  $\Pi$  such that  $W = J^m$  for some positive integer  $m$ , then we must have  $l(J) \geq 2$ ,  $\text{In}(J) \sim' \text{Fin}(J)$  and  $J$  a subword of  $W$ , since  $l(W) \geq 2$  and  $\text{In}(W) \sim' \text{Fin}(W)$ . Clearly we can find all such subwords of  $W$  (note that  $W$  itself is such a subword).

We now determine, for each such  $J$ , whether or not there exist a positive integer  $n$  and an element  $R$  of  $\Omega$  such that  $J^n = R$ . If no such  $R$  exists, then  $|W|$  has infinite order. If for some  $J$  there exists such an  $R$ , then we can find it by examining in turn each of the elements  $R_1, R_2, \dots$  of  $\Omega$  until we come to one with the required form. Let  $t$  be the highest common factor of  $m$  and  $n$  (clearly the integers  $m$  and  $n$  are known). Then, by Theorem 2 of [7],  $|J|$  has order  $n$  and so  $|W|$  has order  $n/t$ .

**4. The main results.** We list two conditions that we shall need to impose on  $\Pi/[\Omega]$ .

(g) The order problem is solvable for each constituent group  $G_\gamma$  of  $\Pi$ .

(h) The power problem is solvable for each constituent group  $G_\gamma$  of  $\Pi$ .

We have

**THEOREM 3.** *Let  $\Pi/[\Omega]$  be an FPS-group satisfying conditions (a) to (g) listed above. Then the order problem is solvable for  $\Pi/[\Omega]$ .*

*Proof.* Given any element  $|W|$  of  $\Pi$ , we have to determine the order of  $|W|$  in  $\Pi/[\Omega]$ . By Lemma 1, we can find elements  $U, V$  of  $\Pi$  such that  $W \approx U^{-1} \cdot V$ .  $U$  and  $V$  is either cyclically  $\Omega$ -reduced or is the identity. Then  $|W| = |U|^{-1} |V| |U|$ , and so the order of  $|W|$  is equal to the order of  $|V|$ . Thus, to prove the theorem, we have to determine the order of  $|V|$ . If  $V = I$  then we are finished. If  $l(V) = 1, V \in G_\gamma$  say, then, by (ii) of Theorem 1 of [7], the order of  $|V|$  is equal to the order of  $V$ , and we can determine this since the order problem is solvable in  $G_\gamma$ . Finally, if  $l(V) > 1$ , then by Lemma 3 we can determine the order of  $|V|$ : This proves the theorem.

**THEOREM 4.** *Let  $\Pi/[\Omega]$  be an FPS-group satisfying conditions (a) to (f) and condition (h). Then the power problem is solvable for  $\Pi/[\Omega]$ .*

*Proof.* Given elements  $X$  and  $Y$  of  $\Pi$ , we have to determine whether or not  $|X| = |Y|^n$

for some integer  $n$ . Now, if either  $X \approx I$  or  $Y \approx I$ , then the result follows from Theorem 2, so we can assume that  $X \not\approx I$  and  $Y \not\approx I$ . It follows that we can find elements  $Z, W$  of  $\Pi$  such that  $Y \approx Z^{-1} \cdot W \cdot Z$  and  $W$  is cyclically  $\Omega$ -reduced, and an element  $P$  of  $\Pi$  such that  $P \approx Z \cdot X \cdot Z^{-1}$  and  $P$  is  $\Omega$ -reduced. Now  $X \approx Y^n$  if and only if  $P \approx W^n$ , so that the theorem will be proved if we can determine whether or not  $P \approx W^n$  for some integer  $n$ .

Suppose firstly that  $l(W) = 1$ . Then, if  $P \approx W^n$  for some  $n$ , we must have, by Corollary 1, that  $P = W^n$  and so, in particular,  $P$  and  $W$  must belong to the same constituent group of  $\Pi$ . Now we can determine whether or not  $P$  belongs to the same constituent group  $G_\gamma$  as  $W$ , and, if it does, then we can decide whether or not  $P = W^n$  for some integer  $n$ , since the power problem is solvable for  $G_\gamma$ . This proves the theorem for the case  $l(W) = 1$ .

Now suppose that  $l(W) > 1$ . Then, by Lemma 3, we can determine the order of  $|W|$ . If  $|W|$  has finite order, then we have to test whether or not  $|P|$  is equal to any one of a finite number of powers of  $|W|$ , and this we can do since the word problem is solvable for  $\Pi/[\Omega]$ . Hence we can assume that  $|W|$  has infinite order. We determine whether or not  $W^2$  is cyclically  $\Omega$ -reduced.

Suppose that  $W^2$  is cyclically  $\Omega$ -reduced. Then, since we know that the order of  $|W|$  is infinite, it follows from Lemma 5 of [7] that  $W^n$  is  $\Omega$ -reduced for all  $n$ . Also  $W, W^2, \dots$  are increasing in length, since  $l(W) > 1$  and  $\text{In}(W) \sim' \text{Fin}(W)$ . Now, by Theorem 1, we can find a positive integer  $s$  such that  $P \not\approx W^r$  and  $P^{-1} \not\approx W^r$  for any  $r \geq s$ . Hence, to determine whether or not  $P \approx W^n$  for some integer  $n$  in this case, we have only to determine whether or not  $P \approx W^n$  for  $-s < n < s$ , and this we can do since the word problem is solvable for  $\Pi/[\Omega]$ .

Now suppose that  $W^2$  is not cyclically  $\Omega$ -reduced. Then we can find a cyclic arrangement  $U$  of  $W$ , an element  $V$  of  $\Pi$  and an element  $S$  of  $\Omega_1$  such that  $U^2 = SV$ ,  $R = ST^{-1} \in \Omega$  and  $l^0(T \cdot V) < l(U^2)$ . It is easy to see that we can choose  $S$  and  $U$  so that  $\beta(T, V) = \beta(V, T) = 0$ . Then, by Corollary 2 of [7], writing  $W_2$  for  $V$ , we have  $U = W_1 W_2$  for some element  $W_1$  of  $\Pi$  (which we can clearly determine),  $(T \cdot W_2)^n$  is  $\Omega$ -reduced for all  $n$  and  $(T \cdot W_2), (T \cdot W_2)^2, \dots$  are increasing in length. We note that  $T \cdot W_2 \approx U^2$  since it is the result of replacing  $S = W_1 W_2 W_1$  in  $U^2 = (W_1 W_2 W_1) W_2$  by  $T$ . Now we have  $W = M^{-1} \cdot U \cdot M$  say, where  $M$  is known, and  $|P| = |W|^n$  if and only if  $|M \cdot P \cdot M^{-1}| = |U|^n$ . Put  $H = M \cdot P \cdot M^{-1}$ . The theorem will be proved if we can determine whether or not  $|H|$  is a power of  $|U|$ . Since  $T \cdot W_2 \approx U^2$  this will be so if and only if either  $|H| = |T \cdot W_2|^k$  or  $|H \cdot U^{-1}| = |T \cdot W_2|^k$  for some integer  $k$ . Using the fact that  $(T \cdot W_2)^n$  is  $\Omega$ -reduced for all  $n$  and that  $(T \cdot W_2), (T \cdot W_2)^2, \dots$  are increasing in length, it is clear that we can determine whether or not this is so. This concludes the proof of the theorem.

Theorems 3 and 4 can be used in various ways to extend the class of groups for which Britton solved the word problem. We give here one such extension. We need firstly modifications of two results due to Lipschutz (Lemma 2 and Theorem 5 of [6]).

**THEOREM 5.** *Let  $(S; D)$  and  $(S'; D')$  be presentations of groups  $A$  and  $B$ , respectively, for which both the order problem and the power problem are solvable. Let  $U, V$  be words in the symbols of  $S, S'$ , respectively, such that the corresponding group elements have the same order, and let  $G$  be the free product of  $A$  and  $B$  with the cyclic subgroup generated by these elements amalgamated, so that  $G$  has presentation*

$$\{S \cup S'; D \cup D' \cup (UV^{-1})\}.$$

Then the order problem and the power problem are solvable for  $G$ .

*Proof.* The conditions of the theorem imply that the word problem is solvable for  $A$  and  $B$ , so that we can work with group elements of  $A$  and  $B$  rather than with words in the symbols of  $S$  and  $S'$ . The solvability of the power problem for  $G$  follows easily from Lemma 2 and Theorem 5 of [6], so that we have only to solve the order problem for  $G$ .

Let  $W$  be any element of  $G$ . Then we can find a conjugate  $W'$  of  $W$  such that either

(i)  $W' = a_1 b_1 a_2 b_2 \dots a_n b_n$ , where  $a_i \in A$ ,  $b_i \in B$  ( $i = 1, 2, \dots, n$ ) and no  $a_i$  or  $b_i$  belongs to the amalgamated subgroup, or

(ii)  $W'$  is equal to an element of  $A$  or  $B$ .

If (i) holds, then  $W'$  (and therefore  $W$ ) has infinite order in  $G$ , while if (ii) holds, we can determine the order of  $W'$  since the order problem is solvable in  $A$  and  $B$ . This proves the theorem.

As a consequence of this theorem we have

**THEOREM 6.** *Let  $\mathcal{G}_1$  be a set of groups given by presentations for which the order problem and the power problem are solvable. Let  $\mathcal{G}_k$  ( $k > 1$ ) consist of groups  $G$  which are the free products of a finite number of groups in  $\mathcal{G}_{k-1}$  with a cyclic subgroup amalgamated, each amalgamation being specified in terms of the known presentations of the groups in  $\mathcal{G}_{k-1}$ , so that a presentation is obtained for each group in  $\mathcal{G}_k$ . Then the order problem and the power problem are solvable for each group in  $\mathcal{G}_k$ .*

Combining this result with Theorems 3 and 4, we have

**COROLLARY 2.** *If  $\mathcal{G}_1$  is a set of FPS-groups, each of which satisfies conditions (a) to (h), and  $\mathcal{G}_k$  ( $k > 1$ ) is defined as in Theorem 6, then the order problem and the power problem are solvable for each group in  $\mathcal{G}_k$ .*

**5. Two examples.** We now give the two examples mentioned in the introduction. These were suggested by Example 2 of [2]. It is worth noting that the presentation with unsolvable word problem given in that example is in fact a recursive presentation of the free group  $F$  on a countable number of generators. Thus if we take a more usual presentation of this group, say  $(S; D)$  where  $S = \{x_1, x_2, \dots\}$  and  $D$  is the empty set, then we have two presentations of  $F$  such that we cannot construct the isomorphism between them (since otherwise, as the word problem is solvable for  $(S; D)$ , it would be solvable for the presentation given by Britton). This is in complete contrast with the situation for finitely presented groups, for it is known (cf. Boone [1], p. 214) that, if two finite presentations represent the same group, then an isomorphism between them can be found, even when nothing is known about the solvability of the word problem for the presentations.

The examples we give depend on the result (Lemma 2.31 of [2]) that there is a one-one mapping  $\phi$  of the set of positive integers into itself such that the image  $\phi(n)$  of any given integer can be calculated, but there exists no finite process for deciding whether or not any given integer is an image under  $\phi$ .

EXAMPLE 1. A group  $\Pi_1$  with a recursive presentation  $P_1$  for which the power problem is solvable but the order problem is unsolvable.

For each positive integer  $n$  we define the group  $G_n$  by the presentation

$$(x_n; x_n^{m!} = 1 \text{ if } \phi(m) = n).$$

Thus  $G_n$  is an infinite cyclic group if there is no integer  $m$  such that  $\phi(m) = n$ , and in any case  $G_n$  is well defined since there is at most one integer  $m$  such that  $\phi(m) = n$ .

We take  $\Pi_1$  to be the free product of the set of groups  $\{G_n; n = 1, 2, \dots\}$  and  $P_1$  to have generators  $x_r$  ( $r = 1, 2, \dots$ ) and defining relations  $x_{\phi(r)}^{r!} = 1$  ( $r = 1, 2, \dots$ ). Then clearly the order problem is unsolvable for  $P_1$ , since given an integer  $n$  there is no finite process for determining whether or not there is an integer  $m$  such that  $\phi(m) = n$ .

To show that the power problem is solvable for  $P_1$ , it is sufficient, from the construction of  $\Pi_1$  as a free product, to prove that the power problem is solvable for each group  $G_n$ .

Thus, given elements  $x_n^\lambda, x_n^\mu$  of  $G_n$ , we have to determine whether or not there is an integer  $r$  such that  $x_n^\lambda = x_n^{\mu r}$  in  $G_n$ , that is whether or not  $x_n^{\lambda - \mu r} = 1$  in  $G_n$ .

Put  $\sigma = \max(|\lambda|, |\mu|)$ . Then we can determine whether or not  $\phi(m) = n$  for any integer  $m$  such that  $m \leq \sigma$ .

Suppose that we find such an  $m$ . Then  $G_n$  has presentation  $(x_n; x_n^{m!} = 1)$  and so  $x_n^{\lambda - \mu r} = 1$  for some integer  $r$  if and only if  $\lambda - \mu r \equiv 0 \pmod{m!}$ . If such an  $r$  exists, then there is one in the set  $(0, 1, 2, \dots, m! - 1)$ , so that we can determine whether or not there is such an  $r$ .

Now suppose there is no integer  $m$  such that  $m \leq \sigma$  and  $\phi(m) = n$ . We complete the proof that the power problem is solvable for  $G_n$  by showing that, in this case,  $x_n^{\lambda - \mu r} = 1$  for some integer  $r$  if and only if  $\lambda$  is a multiple of  $\mu$ .

Suppose firstly that there is no integer  $m$  such that  $\phi(m) = n$ . Then  $x_n^{\lambda - \mu r} = 1$  if and only if  $\lambda = \mu r$ , that is,  $x_n^{\lambda - \mu r} = 1$  for some integer  $r$  if and only if  $\lambda$  is a multiple of  $\mu$ .

Now suppose that there is an integer  $m$  such that  $\phi(m) = n$ . We note that  $\mu \mid m!$ , since we must have  $m > \sigma$ . Now, if  $x_n^{\lambda - \mu r} = 1$ , then  $\lambda - \mu r \equiv 0 \pmod{m!}$  and so  $\lambda = \mu r + km!$  for some integer  $k$ . Hence  $\lambda$  is a multiple of  $\mu$ , since  $\mu \mid m!$ . On the other hand, if  $\lambda$  is a multiple of  $\mu$ ,  $\lambda = \mu r$  say, then  $x_n^{\lambda - \mu r} = 1$ . This proves our assertion.

Thus we have shown that the power problem is solvable for each  $G_n$  and hence for  $P_1$ .

EXAMPLE 2. A group  $\Pi_2$  with a presentation  $P_2$  for which the order problem is solvable but the power problem is unsolvable.

For each positive integer  $n$  we define the group  $G_n$  by the presentation

$$(x_n, y_n; x_n y_n = y_n x_n, x_n = y_n^m \text{ if } \phi(m) = n).$$

We take  $\Pi_2$  to be the free product of the set of groups  $\{G_n; n = 1, 2, \dots\}$  and  $P_2$  to have generators  $x_r, y_r$  ( $r = 1, 2, \dots$ ) and defining relations  $x_r y_r = y_r x_r, x_{\phi(r)} = y_{\phi(r)}^r$  ( $r = 1, 2, \dots$ ). The power problem is unsolvable for  $P_2$ , since, given  $x_n, y_n$ , we have  $x_n = y_n^m$  if and only if  $\phi(m) = n$ , and we have no finite process for deciding whether or not there is an integer  $m$  such that  $\phi(m) = n$ .

To prove that the order problem is solvable for  $P_2$  it is sufficient, from the construction of  $\Pi_2$  as a free product, to show that it is solvable for each group  $G_n$ .

Any element of  $G_n$  can be written in the form  $x_n^\lambda y_n^\mu$ , and

$$(x_n^\lambda y_n^\mu)^r = x_n^{\lambda r} y_n^{\mu r} = 1 \quad (\lambda, \mu, r \neq 0)$$

if and only if there is an integer  $m$  such that  $\phi(m) = n$  and  $\lambda m r + \mu r = 0$ , that is, if and only if  $\phi(m) = n$  and  $\lambda m + \mu = 0$ . Clearly we can determine whether or not there is such an  $m$ . Thus we can solve the power problem for each  $G_n$  and hence for  $P_2$ .

We note that recursive presentations  $P'_1, P'_2$  of  $\Pi_1, \Pi_2$ , respectively, can be given for which both the order problem and the power problem are solvable; this answers a question raised by the referee. We need the fact that the set  $\mathcal{S}$  of positive integers which are not images under  $\phi$  is (countably) infinite; this follows easily from the definition of  $\phi$  given in Lemma 2.31 of [2]. Thus the subgroup of  $\Pi_1$  generated by the  $x_n$  for which  $n \in \mathcal{S}$  is a free group of infinite rank, and  $\Pi_1$  is the free product of this subgroup with the subgroup generated by the  $x_{\phi(r)}$  ( $r = 1, 2, \dots$ ); we take  $P'_1$  to have generators  $a_r, b_r$  ( $r = 1, 2, \dots$ ) and defining relations  $a_r^{r^1} = 1$  ( $r = 1, 2, \dots$ ). Also the subgroup of  $\Pi_2$  generated by the  $x_n, y_n$  for which  $n \in \mathcal{S}$  is the free product of an infinite number of free abelian groups of rank 2, while the subgroup of  $\Pi_2$  generated by the  $x_{\phi(r)}, y_{\phi(r)}$  ( $r = 1, 2, \dots$ ) is a free group of infinite rank generated by the  $y_{\phi(r)}$  ( $r = 1, 2, \dots$ ), and  $\Pi_2$  is the free product of these two subgroups; we take  $P'_2$  to have generators  $a_r, b_r, c_r$  ( $r = 1, 2, \dots$ ) and defining relations  $a_r b_r = b_r a_r$  ( $r = 1, 2, \dots$ ). It is clear that  $P'_1, P'_2$  have the properties stated above.

#### REFERENCES

1. W. W. Boone, The word problem, *Ann. of Math.* **70** (1959), 207–265.
2. J. L. Britton, Solution of the word problem for certain types of groups I, *Proc. Glasgow Math. Assoc.* **3** (1956), 45–54.
3. J. L. Britton, Solution of the word problem for certain types of groups II, *Proc. Glasgow Math. Assoc.* **3** (1956), 68–90.
4. M. Greendlinger, On Dehn's algorithms for the conjugacy and word problems, with applications, *Comm. Pure Appl. Math.* **13** (1960), 641–677.
5. G. Higman, Subgroups of finitely presented groups, *Proc. Roy. Soc.* **A262** (1961), 455–475.
6. S. Lipschutz, An extension of Greendlinger's results on the word problem, *Proc. Amer. Math. Soc.* **15** (1964), 37–43.
7. J. McCool, Elements of finite order in free product sixth-groups, *Glasgow Math. J.* **9** (1968), 128–145.

UNIVERSITY OF TORONTO  
TORONTO, CANADA