ON THE SUBSTITUTION PROBLEM FOR FREE GROUPS

PAUL E. SCHUPP

By a substitution problem for a group G we mean the following. Let $F=\langle \alpha_1, \cdots, \alpha_n\rangle$ be a free group. Let G be a group with presentation $\langle a_1, \cdots, a_m; R_1, \cdots, R_l\rangle$. Suppose we are given a reduced word $W(\alpha_1, \cdots, \alpha_n)$. We wish to decide, for $x\in G$ (where x is expressed in the generators $a_1, \cdots, a_m$ of G), whether or not x is of the form W, that is, to decide if there exist $u_1, \cdots, u_n$ in G such that $x=W(u_1, \cdots, u_n)$.

There exist groups in which it is even impossible to decide if an element is a commutator [1]. The question of solving substitution problems for free groups seems to arise in several contexts and we henceforth restrict ourselves to the case where G is free. Even here, the only results we know are that one can decide if an element of a free group is a kth power and the elegant method of Wicks [4] for deciding if an element of a free group is a commutator. This note presents a proof that the substitution problem is solvable for G a free group and $W(\alpha, \beta)$ any element of the free group on α and β.

LEMMA. *Let $F=\langle \alpha_1, \cdots, \alpha_n\rangle$ and $G=\langle a_1, \cdots, a_m\rangle$ be free groups. Let $W\in F$, and let $x\in G$. Suppose that $W(u_1, \cdots, u_n)=x$ for some $u_1, \cdots, u_n$ in G. Then there exist $W^*\in F$ and $v_1, \cdots, v_n$ in G such that*:

(i) *The set $\{v_1, \cdots, v_n\}$ is Nielsen reduced.*

(ii) *$W^*(v_1, \cdots, v_n)=x$ and W^* is the image of W under an automorphism of F.*

PROOF. We regard Nielsen transformations as acting on n-tuples (cf. [2]). Now there is a sequence $T_1, \cdots, T_k$ of Nielsen transformations and an n-tuple $(v_1, \cdots, v_n)$ of Nielsen reduced elements such that $(u_1, \cdots, u_n)\rightarrow(v_1, \cdots, v_n)$ by successively applying the transformations T_i. We use the same letters to denote both the corresponding Nielsen transformations applied to n-tuples of generators of F and the automorphisms of F which the transformations induce. Thus if T_1 is the Nielsen transformation sending $(a_1a_2^{-1}, a_2)\rightarrow(a_1, a_2)$, then $(\alpha_1, \alpha_2)\rightarrow(\alpha_1\alpha_2^{-1}, \alpha_2)$ under T_1^{-1} and the word $\alpha_1\alpha_2^2\alpha_1\rightarrow\alpha_1\alpha_2\alpha_1\alpha_2^{-1}$ under the automorphism T_1^{-1} induced by the Nielsen transformation. Suppose that $W\rightarrow W^*$ by the successive application of the auto-

Received by the editors December 9, 1968.

morphisms $T_1^{-1}, \cdots, T_k^{-1}$ of F. Then $W^*(v_1, \cdots, v_n)=x$ and W^* is the image of W under an automorphism of F.

For $y \in G$, let $|y|$ denote the length of y with respect to the generators $a_1, \cdots, a_m$. Similarly, for $Z \in F$, let $|Z|$ denote the length of Z with respect to $\alpha_1, \cdots, \alpha_n$. We will show that one can assume that $|v_i| \leq |x|$, $i=1, \cdots, n$, and, if for those α_i which actually occur in W^*, $v_i \neq 1$, then $|W^*| \leq |x|$. If α_j does not occur in W^*, then v_j can be replaced by 1 without altering the fact that the v_i are Nielsen reduced and that $W^*(v_1, \cdots, v_n)=x$.

Let t_q denote one of the $(v_i)^{\pm 1}$. Two cancellation properties of a Nielsen reduced set of nontrivial elements are that if $t_1 \cdots t_p$ is a product with no $t_q = t_{q+1}^{-1}$ then

(i) $|t_1 \cdots t_p| \geq p$, and

(ii) $|t_1 \cdots t_p| \geq \max_{1 \leq q \leq p} |t_q|$.

Since $W^*(v_1, \cdots, v_n)=x$ and we are assuming that no v_i which appears is 1, we conclude from (i) that $|W^*| \leq |x|$. By (ii), if α_j occurs in W^*, then $|v_j| \leq |x|$.

Now by Whitehead's Theorem on the automorphisms of a free group [**3**], we can effectively list all words $W' \in F$ such that $|W'| \leq |x|$ and W' is the image of W under an automorphism of F. We can then enumerate all n-tuples $(u_1', \cdots, u_n')$ such that maximum $|u_i'|$ does not exceed $|x|$ and substitute all such n-tuples into the W' obtained above. Since W' is obtained from W by an automorphism, $W'(u_1', \cdots, u_n')=x$ if and only if there exist $u_1, \cdots, u_n$ such that $W(u_1, \cdots, u_n)=x$.

So far, all that we have done is independent of the number of α_i. The difficulty is that we have, in general, no algorithm to decide if a word on the α's can be obtained from W by an automorphism and then replacing some letters by 1. However, the situation is manageable if $n=2$.

THEOREM. *Let $F=\langle \alpha, \beta \rangle$. Let W be a reduced word of F. Let G be a free group. Then there is an algorithm to decide, for $x \in G$, if x is of the form W.*

PROOF. Let $\sigma_\alpha(Y)$ denote the exponent sum of α in the word Y. Let $a=\sigma_\alpha(W)$, let $b=\sigma_\beta(W)$, and let d be the greatest common divisor of a and b. Since there exist integers s, t, such that $d=as+bt$, we have $v^d = W(v^s, v^t)$. Thus if $x \in G$ is a dth power, then x is of the form W. Suppose x is not a dth power and $W(u_1, u_2)=x$. Then in the process of obtaining a Nielsen reduced pair (v_1, v_2), neither v_1 nor v_2 is 1. For if we had, say $v_1=1$, then $x=v_2^r$ where r is a multiple of d. Hence x is either a dth power or we can decide if x is of the form W by examining a finite number of substitutions.

Bibliography

1. G. Baumslag, W. W. Boone and B. H. Neumann, *Some unsolvable problems about elements and subgroups of groups*, Math. Scand. **7** (1959), 191–201.

2. W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory*, Interscience, New York, 1966.

3. J. H. C. Whitehead, *On equivalent sets of elements in a free group*, Proc. London Math Soc. **41** (1936), 48–56.

4. M. J. Wicks, *Commutators in free products*, London Math. Soc. **37** (1962), 433–444.

University of Illinois, Urbana