ON BRITTON'S THEOREM A

CHARLES F. MILLER III[1]

In [1] Britton gives a "group-theoretic" proof of the unsolvability of the word problem for finitely presented groups. His proof uses a very powerful result [1, Lemma 4 (the principal lemma)] on presentations which has become known as Britton's Lemma and has since been used by several other authors. In the appendix to [1] Britton states a generalization of this lemma as Theorem A. Britton briefly indicates how Theorem A can be deduced from the previous lemma and how it may be further generalized. We give a direct proof of Theorem A in its most general form which specializes immediately to Britton's Lemma. Our proof appeals more directly to the theory of free products with amalgamation.

By $E=(S; D)$ we mean that the group E is presented by generators S and relations D. By $G=(A*B; H=K, \phi)$ we mean that G is the free product of groups A and B amalgamating their subgroups H and K via the isomorphism ϕ (ϕ will be omitted where the map is obvious from the context). The notation $w\equiv v$ will mean that w and v are identical as words, while $w=v$ refers to equality of words as elements of some appropriate group.

The following lemma is an immediate consequence of the normal form for free products with amalgamation:

LEMMA 1. *Suppose* $G=(A_1*A_2; H_1=H_2, \phi)$ *and let* $w\equiv hg_1\cdots g_n$ $(n\geqq 1)$, *where* $h\in H_1=H_2$ *and* $g_i\in A_{v(i)}$, *where* $v(i)\neq v(i+1)$, *so that the* g_i *lie in alternating factors. Then if* $w=1$ *in* G *there is some* i *such that* $g_i\in H_1=H_2$.

P will denote a set of letters indexed by a set V. We write $p(v)$ rather than p_v to avoid several levels of subscripting. Let $E=(S; D)$ be any presentation and assume P and S are disjoint. A presentation E^* is said to have *stable letters* P and corresponding *basis* E if it has the form

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

where $y_i, z_i\in V$ and A_i and B_i are words over S.[2]

Received by the editors June 2, 1967.

[1] This work was partially supported by National Science Foundation contract NSF-GP 6132.

[2] The concept of stable letters is motivated by a similarity to inner automorphisms and by an analogy to internal states of a Turing machine. See [3, Chapter 12], in this connection.

We write $p(y) \sim p(z)$ if $p(y) = p(z)$ in the free group obtained from E^* by setting all the letters of S equal to 1. Let $K(v) = \{i \in I: p(y_i) \sim p(v)\}$ denote the induced equivalence classes in I. $A(v)$ denotes the subgroup of E generated by the A_i such that $i \in K(v)$, and similarly for $B(v)$.

E^* as above satisfies the *generalized isomorphism condition* (*GIC*) if for each $K(v)$ the map $A_i \to B_i$ $(i \in K(v))$ defines an isomorphism between $A(v)$ and $B(v)$.

Let T, U be words over S and let $y, z \in V$. We say $Tp(y)$ *produces* $p(z)U$ if the $Tp(y)$ can be transformed into $p(z)U$ by a sequence of operations of the form

$$XA_i p(z_i) Y \to Xp(y_i) B_i Y \quad \text{or} \quad XA_i^{-1} p(y_i) Y \to Xp(z_i) B_i^{-1} Y,$$

where X, Y are words over S.

It can be shown that if $Tp(y)$ produces $p(z)U$, then T is a word in $A(y)$, say $T \equiv w(A_i)$, and U the corresponding word $w(B_i)$ in $B(y)$. Moreover $Tp(y) = p(z)U$ in E^*.

A word W *involves* the letter p if either p or p^{-1} is a subword of W. (In particular, the word pp^{-1} involves p.)

THEOREM A. *Suppose E^* as above satisfies the GIC. Then*

(I) *E is embedded in E^* and*

(II) *if $W = 1$ in E^* where W involves at least one letter $p \in P$, then W contains a subword* (1) $p(y)^{-1} C p(z)$ *or* (2) $p(y) C p(z)^{-1}$ *where C is a word over S. In case* (1), *C is equal in E to a word $w(A_i) \in A(y)$ and $w(A_i)p(z)$ produces $p(y)w(B_i)$. In case* (2), *C is equal in E to a word $w(B_i) \in B(y)$ and $w(A_i)p(z)$ produces $p(y)w(B_i)$.*

PROOF. Let $[a(v)(v \in V)]$ denote the free group generated by the $a(v)$. Generally, $\langle Q \rangle$ denotes the subgroup generated by the set Q. Define the (ordinary) free products:

$$F = [a(v)(v \in V)] * E, \qquad G = [b(v)(v \in V)] * E.$$

Consider the subgroups $M_v = \langle a(y_i)^{-1} A_i a(z_i) (i \in K(v)) \rangle$ of F and $N_v = \langle b(y_i) B_i b(z_i)^{-1} (i \in K(v)) \rangle$ of G.

Then $M_v = M_t$ if and only if $K(v) = K(t)$. Also $\langle M_v, M_t \rangle \cong M_v * M_t$ if $K(v) \neq K(t)$ and $\langle M_v, E \rangle \cong M_v * E$ for each v as subgroups of F. Similar considerations apply to the N_v in G.

By the GIC it follows that $M_v \cong N_v$ by the obvious map. Now we put

$$Y = \langle a(y_i)^{-1} A_i a(z_i) (i \in I) \rangle * E \subset F,$$
$$Z = \langle b(y_i) B_i b(z_i)^{-1} (i \in I) \rangle * E \subset G.$$

Hence $Y \cong Z$ under the map $E \to E$ and $M_v \to N_v$, i.e., $a(y_i)^{-1}A_i a(z_i) \to b(y_i)B_i b(z_i)^{-1}$ for each i. Now setting

$$\overline{E} = (S, a(v), b(v)(v \in V); \quad D, a(y_i)^{-1}A_i a(z_i) = b(y_i)B_i b(z_i)^{-1}(i \in I)),$$

we see immediately that $\overline{E} \cong (F*G;\ Y=Z)$. The map $S \to S$, $p(v) \to a(v)b(v)$ embeds E^* in $\overline{E}$. To see this, observe that the relations of $\overline{E}$ are exactly the relations of E^* under this map, so it is certainly a homomorphism. Moreover, if a word $W(S, p(v)) \to W(S, a(v)b(v)) = 1$ in $\overline{E}$, W must also equal 1 in the group T obtained from $\overline{E}$ by setting $b(v) = 1$. But clearly $T \cong E^*$ via the map $S \to S$, $a(v) \to p(v)$. Since the composite of all these maps is the identity on E^*, $W(S, p(v)) = 1$ in E^*. Hence E is embedded in E^* and $\overline{E}$ by $S \to S$ for $E \subset Y = Z$.

Now to prove the theorem we may assume W is freely reduced in E^* and

$$W \equiv S_1 p(v_1)^{\alpha_1} S_2 p(v_2)^{\alpha_2} \cdots S_n p(v_n)^{\alpha_n} S_{n+1},$$

where $n \geqq 1$ and all $\alpha_i \neq 0$ and $S_i \in E$. Since $W = 1$ in E^* we must have for its embedded image in $\overline{E}$

$$W \equiv S_1 (a(v_1)b(v_1))^{\alpha_1} S_2 \cdots S_n (a(v_n)b(v_n))^{\alpha_n} S_{n+1} = 1 \qquad \text{in } \overline{E}.$$

Notice that $a(v) \in F \backslash Y$, $b(v) \in G \backslash Z$ and $S_i \in Y = Z$ since $\overline{E} \cong (F*G;\ Y=Z)$. By hypothesis $n \geqq 1$. From Lemma 1 we conclude that for some i one of the following holds:

(1) $\alpha_i < 0$ and $\alpha_{i+1} > 0$ and $a(v_i)^{-1} S_{i+1} a(v_{i+1}) \in Y$.
(2) $\alpha_i > 0$ and $\alpha_{i+1} < 0$ and $b(v_i) S_{i+1} b(v_{i+1})^{-1} \in Z$.
(3) $\alpha_i < 0$ and $\alpha_{i+1} \leqq 0$ and $a(v_i)^{-1} S_{i+1} \in Y$.
(4) $\alpha_i > 0$ and $\alpha_{i+1} \geqq 0$ and $b(v_i) S_{i+1} \in Z$.

But cases (3) and (4) are clearly impossible. So consider case (1). It follows from notation and free products that $a(v_i)^{-1} S_{i+1} a(v_{i+1}) \in M_v$ for some v, since $Y \cong E*R$ where R is the free product of the distinct M_v and such a word must have free product normal form length 1 (cancelling $a(v)$ pairs must come from generators of the same M_v by our notation). Hence $S_{i+1} = w(A_l)$ in E for $w(A_l) \in A(v)$. Indeed, we have

$$a(v_i)^{-1} S_{i+1} a(v_{i+1}) = \prod_{j=1}^{m} a(t_j)^{-1} A_{l_j}^{\epsilon_j} a(t_{j+1})$$

and

$$w(A_l) \equiv \prod_{j=1}^{m} A_{l_j}^{\epsilon_j}, \quad \text{where} \quad \epsilon_j = \pm 1$$

and $a(v_i) = a(t_1)$ and $a(t_{m+1}) = a(v_{i+1})$ and where the $a(t_j)^{-1} A_{l_j}^{\epsilon_j} a(t_{j+1})$

are generators of M_v or their inverses. Hence W contains a subword equal to

$$b(v_i)^{-1}a(v_i)^{-1}w(A_l)a(v_{i+1})b(v_{i+1}),$$

which as a word of E^* has the form $p(v_i)^{-1}w(A_l)p(v_{i+1})$. But in $\overline{E}$ we have

$$\begin{aligned} a(v_i)^{-1}S_{i+1}a(v_{i+1}) &= a(v_i)^{-1}w(A_l)a(v_{i+1}) \\ &= b(v_i)w(B_l)b(v_{i+1})^{-1}, \end{aligned}$$

where $w(A_l)\in A(v)$ and $w(B_l)\in B(v)$. Moreover, $p(v_i)^{-1}w(A_l)p(v_{i+1}) = w(B_i)$ and $w(A_l)p(v_{i+1})$ produces $p(v_i)w(B_l)$ by use of the relations corresponding to the sequence of $a(t_j)$'s. This completes the proof in the situation arising in case (1) of the theorem.

Similarly, case (2) can be handled by the dual proof.||

COROLLARY 1. *Let E^* and E be as in Theorem* A. *Let n be a positive integer. Then E^* has elements of order n if and only if E has elements of order n.*

PROOF. The claim is true for $\overline{E}$ (and hence E^*) by properties of free products with amalgamation, see [2].||

A group $G = E_n \geqq E_{n-1} \geqq \cdots \geqq E_0 = E$ is called a *Britton tower* over E if each $E_i \geqq E_{i-1}$ satisfies the conditions for $E^* \geqq E$ of Theorem A.

COROLLARY 2. *Let G be a Britton tower over E. Let n be a positive integer. Then G has elements of order n if and only if E has elements of order n.*

PROOF. By induction and Corollary 1.||

In the special case

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

we have $p(v)\sim p(w)$ if and only if $p(v) = p(w)$. Then the GIC becomes the isomorphism condition of Britton (see [1] or [3, Chapter 12]). Also $Tp(v)$ produces $p(w)U$ implies $p(v) = p(w)$. Hence Theorem A just becomes Britton's Lemma. A consequence of E being embedded in E^* is a well-known theorem of Higman, Neumann and Neumann (see [3, Chapter 11]).

REFERENCES

1. J. L. Britton, *The word problem*, Ann. of Math. **77** (1963), 16–32.

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

3. J. Rotman, *The theory of groups*, Allyn and Bacon, Boston, Mass., 1965; Chapters 11 and 12.

UNIVERSITY OF ILLINOIS