TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCITEY
Volume 178, April 1973

ELEMENTARY PROPERTIES OF FREE GROUPS

BY

GEORGE S. SACERDOTE

ABSTRACT. In this paper we show that several classes of elementary properties (properties definable by sentences of a first order logic) of groups hold for all nonabelian free groups. These results are obtained by examining special embeddings of these groups into one another which preserve the properties in question.

1. It has long been conjectured that the finitely generated nonabelian free groups are elementarily equivalent. (That is, they satisfy the same sentences of first order group theory.) The truth of this conjecture would yield the elementary equivalence of all of the nonabelian free groups. There have been several partial results in this area. The most notable are [1] (1) (Oral tradition) All nonabelian free groups satisfy the same Π_2 sentences; (2) (Merzlyakov's Theorem) If $m > m' \geq 2$ are integers, then a positive sentence Φ in the language of $F_{m'}$ (the free group of rank m') holds in F_m (under the standard embedding) if and only if it holds in $F_{m'}$.

In this paper we shall apply the graph-theoretic techniques of small cancellation theory as developed by Lyndon, Schupp, and Weinbaum to prove a general lemma (hereafter called the Principal Lemma) from which both of these results and others can easily be obtained. More precisely, we shall prove

A. Any Π_3 sentence in the language of $F_{m'}$ which holds in F_m (under the standard embedding) holds in $F_{m'}$.

B. Let Φ be a positive sentence in the language of a free group $F_{m'}$; then Φ holds in $F_{m'}$ if and only if an instance of Φ, obtained by replacing the existentially bound variables of Φ by terms involving the generators and the preceding (in the prefix of Φ) universally bound variables and deleting the quantifiers, is valid in $F_{m'}$.

C. Merzlyakov's Theorem.

D. Given a positive sentence Φ in the language of F_m, there is an embedding of F_m into $F_{m'}$ such that F_m satisfies Φ if and only if $F_{m'}$ satisfies Φ.

In addition we will prove

Received by the editors December 7, 1971.

AMS (MOS) subject classifications (1970). Primary 02H05, 02H15, 20A05, 20E05.

[1] Mal'cev has attributed the following result to A. D. Taimanov. All nonabelian free groups satisfy the same Π_4 sentences. Unfortunately this proof is unavailable to the author.

E. F_m is not an elementary subgroup of $F_{m'}$.

The author wishes to acknowledge the helpful conversations with K. I. Appel, W. W. Boone, and R. C. Lyndon which have contributed greatly to this work. This research was conducted while the author held an NSF Traineeship and a NATO Postdoctoral Fellowship.

The basic language of this paper will be the first order language of group theory with individual variables (subscripted x's, y's and z's), an individual constant 1, the operation symbols $\cdot$ and $^{-1}$, the predicate $=$, and the logical symbols $\&$, $\vee$, $\sim$, $\forall$, and $\exists$. Given a group H, the *language of* H, L^H will be our basic language with the addition of a new constant $'h'$ (name of h) for each element h of H. In particular L^1 is L. Where no confusion can arise $'h'$ will be written h. All sentences will be assumed to be in prenex normal form with their matrices in disjunctive normal form. All atomic formulas will be assumed to be in the form $t = 1$ for some term t. A sentence will be called Π_n if it is logically equivalent to a sentence whose initial quantifier is $\forall$ and whose prefix has at most $n-1$ alternations of quantifier type. In particular a Π_0 sentence is quantifier free. The negation of a Π_n sentence is Σ_n. A sentence will be called *positive* if it is logically equivalent to a sentence which does not involve the negation symbol $\sim$.

Let $F_{m'} = \langle \beta, \gamma, \zeta_3, \cdots, \zeta_{m'} \rangle$ and let $F_m = F_{m'} * \langle \zeta_{m'+1}, \cdots, \zeta_m \rangle$. Let $\alpha_i = \beta^i \gamma \beta^{-i}$ for all integers i, and, given a positive integer μ, let $\Gamma(i, \mu) = \alpha_{2i\mu+1} \alpha_{2i\mu+2} \cdots \alpha_{2(i+1)\mu}$. Let $\mathbf{x}$ and $\mathbf{y}$ be t- and s-tuples of distinct individual variables. Suppose that $M(\mathbf{x}, \mathbf{y})$ is an open formula of our basic language and that $\mathbf{u}$ is an arbitrary t-tuple of elements of F_m.

The Principal Lemma. *Suppose that* $\mu > \mathrm{BIG}(M, \mathbf{u})$ (*an effectively calculable function of certain measures of the complexities of* M *and* $\mathbf{u}$, *which will be specified in* §4). *Let* $\hat{}$ *be the homomorphism from* F_m *onto* $F_{m'}$ *defined by* $\hat{f} = f$ *for* f *in* $F_{m'}$ *and* $\hat{\zeta}_i = \Gamma(i, \mu)$, *for* $i > m'$. *Then for any s-tuple* $\mathbf{v}$ *of elements of* $F_{m'}$ *for which* $M(\hat{\mathbf{u}}, \mathbf{v})$ *holds, one can effectively calculate a sequence* $\check{\mathbf{v}}$ *of elements of* F_m *such that* $M(\mathbf{u}, \check{\mathbf{v}})$ *holds and such that* $\check{\mathbf{v}}\hat{} = \mathbf{v}$. *Moreover* $\check{\mathbf{v}}$ *is obtained by replacing certain subwords of elements of* $\mathbf{v}$ *on the letters* β *and* γ *by words of* F_m *involving the* ζ_i.

The proof of this lemma will be deferred to §4. First we apply it to obtain the Theorems A–E stated in the introduction.

2.

Theorem A. *Any* Π_3 *sentence in the language of* $F_{m'}$ *which holds in* F_m *under the standard embedding holds in* $F_{m'}$.

Proof. Let $(\forall x_1)(\exists x_2)(\forall x_3)M(c, x_1, x_2, x_3)$ hold in F_m where c is a tuple of (names for) elements of $F_{m'}$. Choose an arbitrary u_1 in $F_{m'}$ and the corresponding u_2 in F_m such that F_m satisfies the sentence $(\forall x_3)M(c, u_1, u_2, x_3)$. Let u be the sequence obtained by concatenating c, u_1 and u_2. If $\mu > \mathrm{BIG}(M, u)$, then $F_{m'}$ satisfies the sentence $(\forall x_3)M(c, u_1, \hat{u}_2, x_3)$; if there existed v in $F_{m'}$ such that the sentence $\sim M(c, u_1, \hat{u}_2, v)$ held in that group, then we could calculate $\check{v}$ in F_m such that $\sim M(c, u_1, u_2, \check{v})$ held in F_m. Thus $F_{m'}$ satisfies $(\exists x_2)(\forall x_3)M(c, u_1, x_2, x_3)$. But u_1 was an arbitrary choice of elements of $F_{m'}$. Consequently $(\forall x_1)(\exists x_2)(\forall x_3)M(c, x_1, x_2, x_3)$ holds in $F_{m'}$.

Theorem B. *Let Φ be any positive sentence in the language of $F_{m'}$. Φ holds in $F_{m'}$ if and only if an instance of Φ, obtained by replacing each existentially bound variable by a term involving the generators and the preceding universally bound variables and deleting the quantifiers, is valid in $F_{m'}$.*

Proof. If such an instance of Φ holds, it is clear that Φ must hold. The proof of the converse requires the principal lemma.

We shall define an increasing sequence of natural numbers $\mu_1, \mu_2, \cdots, \mu_n$ by induction and a finite sequence of free groups $H_1, \cdots, H_n$. Let the ith block of universally bound variables in the prefix have length t_i. Let $\xi_1, \xi_2, \cdots, \xi_t$ $(t = \Sigma\, t_i)$ be new letters. Let u_1 instantiate the first block of existentially bound variables. Let u_2 be the first t_1 ξ's. Let $\mu_1 = \mathrm{BIG}(M, J_1)$ where J_1 is concatenation of c and u_1. In general, if $i = 2k+1$, let u_i be a true instantation of the initial block of the existentially quantified variables in the formula $(\exists x_{2k+1}) \cdots M(c, u_1, \cdots, u_{2k}, x_{2k+1} \cdots)$ in the group $F_{m'} = \langle \beta, \gamma, \zeta_1, \cdots, \zeta_{m'}, u_2, u_4, \cdots, u_{2k}; \xi_i = \Gamma(i, \mu_j)$ for ξ_i in $u_j\rangle$. If $i = 2k+2$, let u_i be the first t_k ξ's whose subscripts exceed all the subscripts of ξ's appearing in u_{2k}. Let μ_{k+1} be any integer exceeding μ_k and $\mathrm{BIG}(M, J_i)$ where J_i is obtained by concatenating c, $u_1, \cdots, u_{2k+1}$ and replacing the ξ's which appear in the u_{2j} by the corresponding $\Gamma(i, \mu_j)$. When the above has been completed, define $H_i = F_{m'} * \langle \xi_j, \xi_j$ in u_{2n} or, $\cdots, u_{2(n-i+1)}\rangle$. In particular, $H_0 = F_{m'}$. Let $\Psi_0(c, u_1, \cdots, u_{2n+1})$ be the qunatifier-free formula so constructed. Ψ_0 is true in $F_{m'} = F_{m'} * \langle \xi_k; \xi_i = \Gamma(i, \mu_j), \xi_i \epsilon u_{2j}\rangle$. By the principal lemma therfore we can calculate $v_{(2n+1),1} = \check{u}_{2n+1}$ such that, in H_1, $M(c, u_1, \cdots, u_{2n}, v_{(2n+1),1})$ holds. (Call it Ψ_1.) Repeat this argument n times, at each stage concluding that since a formula holds in H_{i-1}, a related formula must hold in H_i, by considering H_{i-1} as a quotient of H_i by the rule $H_{i-1} = \langle H_i/(\xi_j = \Gamma(j, \mu_{n-i}), \xi_j$ in $u_{n-i})\rangle$. In this way calculate $v_{(2n+1),i} = \check{v}_{(2n+1),i-1}, \cdots, v_{2(n-i)+1,i+1} = \check{u}_{2(n-i)+1}$. It is immediate from the last sentence of the statement of the principal lemma that $\check{u}_{2k} = u_{2k}$ for each application of the lemma. At each stage a formula Ψ_i is constructed in the language of H_i which is true in that group because Ψ_{i-1} is true in H_{i-1}. Let Φ^* be Ψ_n; that is, Φ^* is $M(\mathrm{c}, \mathrm{v}_{1,n}, \mathrm{u}_2, \cdots, \mathrm{u}_{2n+1,n})$. Φ^* holds in H_n.

Obtain $\tilde{\Phi}$ from Φ^* by replacing the letters ξ_i by new variables z_i. $\tilde{\Phi}$ holds in $F_{m'}$, since given $w_1, \cdots, w_t$ elements of $F_{m'}$, the map $\xi_i \to w_i$ defines a homomorphism from H_n onto $F_{m'}$; thus the truth of Φ^* in H_n implies the truth of $\tilde{\Phi}(\mathrm{w})$ in $F_{m'}$.

Theorem C (Merzlyakov). *Let m and m' be integers with $m > m' \geq 2$, and let $\Phi(\mathrm{c})$ be a positive sentence in the language $L^{F_{m'}}$. $\Phi(\mathrm{c})$ holds in F_m if and only if it holds in $F_{m'}$.*

Proof. If the given sentence holds in F_m, it certainly holds in $F_{m'}$, since $F_{m'}$ is a quotient of F_m, and the truth of positive sentences is preserved under quotients.

Conversely, suppose that $\Phi(\mathrm{c})$ holds in $F_{m'}$. Let $\Phi^*(\mathrm{x}, \mathrm{c})$ be an instance of $\Phi(\mathrm{c})$, of the type specified in the statement of Theorem B, which is valid in F_m if and only if $\Phi(\mathrm{c})$ holds in F_m. Let x have n elements. It suffices to show that if $m - m' \geq n$, $\Phi^*(\mathrm{x}, \mathrm{c})$ is valid in F_m, for if $m - m' < n$, then F_m is a quotient of $F_{m'+n}$, the free group of rank $m' + n$, and, thus, $\Phi^*(\mathrm{x}, \mathrm{c})$ must be valid in F_m. Further, it suffices to show that $\Phi^*(\zeta_{m'+1}, \zeta_{m'+2}, \cdots, \zeta_{m'+n}, \mathrm{c})$ holds in F_m, for, given any n-tuple θ of elements of F_m, the endomorphism defined by $f \to f$ for f in $F_{m'}$, $\zeta_{m'+i} \to \theta_i$ for $1 \leq i \leq n$, and $\zeta_j \to \zeta_j$, for $j > m' + n$ must preserve the truth of $\Phi^*(\zeta_{m'+1}, \cdots, \zeta_{m'+n}, \mathrm{c})$. That is, $\Phi^*(\theta, \mathrm{c})$ must hold in F_m.

Choose $\mu > \mathrm{BIG}(\Phi^*, (\zeta_{m'+1}, \cdots, \zeta_{m'+n}, \mathrm{c}))$. Define the map $\hat{\ }: F_m \to F_{m'}$ by $\zeta_i \to \zeta_i$, for $i \leq m'$, and $\zeta_i \to \Gamma(i, \mu)$ for $i > m'$. Since $\Phi(\mathrm{c})$ holds in $F_{m'}$, $\Phi^*(\mathrm{x}, \mathrm{c})$ must be valid in $F_{m'}$. Hence $\Phi^*(\hat{\zeta}_{m'+1}, \cdots, \hat{\zeta}_{m'+n}, \mathrm{c})$ holds in $F_{m'}$. Therefore, by the principal lemma (where the vector u is $(\zeta_{m'+1}, \cdots, \zeta_{m'+n}, \mathrm{c})$ and the vector v is empty), F_m satisfies $\Phi^*(\zeta_{m'+1}, \cdots, \zeta_{m'+n}, \mathrm{c})$. Thus $\Phi(\mathrm{c})$ must hold in F_m.

Theorem D. *Let $\Phi(\mathrm{c})$ be a positive sentence in the language of F_m. Then there is an embedding of F_m into $F_{m'}$ such that $\Phi(\mathrm{c})$ holds in F_m if and only if it holds in $F_{m'}$.*

Proof. To avoid ambiguity, let the generators of F_m be renamed $\eta_1, \cdots, \eta_m$. If F_m satisfies $\Phi(\mathrm{c})$, then $K = F_{m'} * F_m$ satisfies it by Theorem C. Given any collection $w_1, \cdots, w_m$ of elements of $F_{m'}$, the group $\langle K/(\eta_i = w_i \ (i = 1, 2, \cdots, m))\rangle$ isomorphic to $F_{m'}$ satisfies $\Phi(\mathrm{c})$, because it is positive.

Conversely, suppose that a Σ_{2n+1} sentence, $\Phi(\mathrm{c})$, is given with constants c naming elements of F_m. Let M be the matrix of Φ. Choose $\mu_0 > \mathrm{BIG}(M, \varnothing)$. Embed F_m into $F_{m'}$ via the map which sends η_i to $\Gamma(i, \mu_0)$. Let $\hat{\mathrm{c}}$ be the embedded images of the constants c. We suppose now that $F_{m'}$ satisfies $\Phi(\hat{c})$. Let the ith block of universal quantifiers of Φ have t_i bound variables and suppose that there are t universally bound variables altogether. Let $\delta_1, \cdots, \delta_t$ be new letters. By Theorem C, since $F_{m'}$ satisfies $\Phi(\hat{c})$, then so does $K_1 = F_{m'} * \langle \delta_1, \cdots, \delta_t \rangle$. By Theorem B, K_1 satisfies a formula of the form $M(\hat{c}, u_1, u_2, \cdots, u_{n+1})$ where each u_{2i} is instantiated with the first t_i δ's not appearing in any preceding u_{2j}, and each u_{2i+1} is instantiated by a word in the generators of $F_{m'}$ and the δ's appearing in u_{2j}, for $j \leq i$. Therefore, by the principal lemma, $K_1 * F_m$ satisfies $M(c, \breve{u}_1, \breve{u}_2, \cdots, \breve{u}_{2n+1})$. But each $\breve{u}_{2i} = u_{2i}$ because u_{2i} does not involve the letters β and γ. Let $u^{\#}_{2i+1}$ be the image of $\breve{u}_{2i+1}$ under the map $F_{m'} = 1$, for each i. Then $\langle \delta_1, \cdots, \delta_t \rangle * F_m$ satisfies $M(c, u^{\#}_1, u_2, \cdots, u_{2n}, u^{\#}_{2n+1})$, where each $u^{\#}_{2i+1}$ is a word on the generators of F_m and those which appear in the preceding u_{2j}. Therefore $\langle \delta_1, \cdots, \delta_t \rangle * F_m$ satisfies $\Phi(c)$. Applying Theorem C once again shows that F_m satisfies $\Phi(c)$.

Theorem E. *F_m is not an elementary subgroup of $F_{m'}$.*

Proof. Let $w_1, \cdots, w_m$ be the embedded images of the generators of F_m under any embedding of F_m into $F_{m'}$. Let $W_1, \cdots, W_m$ be obtained from the corresponding w's by replacing β by the variable x_1, γ by the variable x_2, and ζ_i by x_i, $i = 3, 4, \cdots, m'$. The sentence $(\exists x_1)(\exists x_2) \cdots (\exists x_{m'})[w_1 = W_1 \;\&\; \cdots \;\&\; w_m = W_m]$ is true in $F_{m'}$ and false in F_m.

It is clear that the preceding argument is not restricted to the theory of groups. Let L be any first order language (with equality), and let T be any universal L-theory. Given a model M of T and a minimal finite set of generators $(a_1, \cdots, a_n)$ of M, then the elements of M are just terms involving the constants of L and the generators. Thus, one can mimic the proof of the preceding theorem to obtain

Theorem F. *Let $m > n$ be positive integers, and let M and N be models of a universal theory T where M has m generators in a generating set of minimal size, and N has n generators in such a generating set. Then M is not an elementary substructure of N.*

3. The following preliminaries concerning the graph theoretic techniques in small cancellation theory will be needed for the proof of the principal lemma. A *map* in the plane Π is determined by a finite set of points called *vertices* and simple arcs called *edges*. Both ends of an edge are to be vertices; it is assumed that one edge is incident to another only at a vertex. A *region of* M is a bounded component of $\Pi - M$. We consider only maps in which every region is simply connected. The *boundary* $M^{\cdot}$ of M is the topological boundary of the unbounded component of $\Pi - M$.

A *diagram* over a free group F consists of a map M together with a function assigning to each oriented edge E of M as *label* $\lambda(E)$ a nontrivial element of F and assigning $[\lambda(E)]^{-1}$ to the oppositely oriented edge E^{-1}. We shall associate a diagram M with each finite sequence $p_1, p_2, \cdots, p_n$ of nontrivial elements of F. Note that each p_i can be uniquely written without cancellation as $u_i r_i u_i^{-1}$ with r_i cyclically reduced.

A diagram M will be called a *diagram for the sequence* $p_1, \cdots, p_n$ if it satisfies the following two conditions: (1) The boundary $M^{\cdot}$ is connected and contains a vertex and has the following further property: if $E_1, \cdots, E_k$ are successive edges in a positive boundary cycle of M beginning at 0, then the product of the lables $\lambda(E_1)\lambda(E_2) \cdots \lambda(E_k)$ is reduced without cancellation and is the reduced form for the word $w = p_1 p_2 \cdots p_n$.

(2) If D is any region of M then its boundary $D^{\cdot}$ contains a vertex P such that if $E_1, \cdots, E_k$ are the successive edges traversed in a positive boundary cycle of D, the product of the labels $\lambda(E_1)\lambda(E_2) \cdots \lambda(E_k)$ is reduced without cancellation and is one of the r_i.

Lemma 3.1 (*van Kampen-Lyndon*). *There exists a diagram for every sequence; this diagram is connected and simply connected.*

Let R be a collection of cyclically reduced elements of F. We will call R *symmetrised* if R is closed under the operations of taking inverses and cyclic permutations. A sequence $p_1, \cdots, p_n$ of conjugates of elements of R will be called *minimal* if the product $p_1 p_2 \cdots p_n$ is not equal to another product $q_1 \cdots q_t$ of conjugates of elements of R with $t < n$.

Let M be a diagram over F. M is called *reduced* if for no pair of regions D_1 and D_2, with $D_1^{\cdot} \cap D_2^{\cdot} \neq \emptyset$, does $(\overline{D_1 \cup D_2})^{\cdot}$ have the product of the labels on a positive boundary cycle freely reduce to 1 in F.

Lemma 3.2 (*Schupp*). *If M is the diagram of a minimal sequence, then M is reduced.*

Lemma 3.3 (*Lyndon*). *Let M be a reduced diagram which contains at least one region. Then there is a region D of M such that $D^{\cdot} \cap M^{\cdot}$ is a connected simple arc.*

Call a simple arc in $M^{\cdot}$ of maximal length which contains no vertices of degree at least three a *segment*.

Lemma 3.4. *If M is a reduced map with $\nu > 0$ regions then the number of segments (with multiplicity) in $M^{\cdot}$ is at most $4\nu - 1$.*

Proof. If $\nu = 1$ then either M is a disc with 0 on its boundary or else M is a disc joined to the base point by a segment. In either case the number of segments does not exceed three.

In the general case, let D be a region for which $D^{\cdot} \cap M^{\cdot}$ is a connected simple arc A. A must be a segment for (i) all interior vertices of A must have degree two (otherwise $D^{\cdot} \cap M^{\cdot}$ is not a simple arc) and (ii) the end points of A must have degree at least three (otherwise A could be lengthened).

Case I. $D^{\cdot}$ contains no interior edges of M. Then there is a reduced map M' such that D is connected to M' by a vertex of D, P, or D is connected to M' by a segment attached to a vertex P of M'. M' has one less region, and, therefore, has at most $4(\nu - 1) - 1$ segments. If P has degree three in M', then the total number of segments of M is the sum of the number of segments in M' and the number of segments in D (and the attaching segment), which is at most $4(\nu - 1) - 1 + 3 \leq 4\nu - 1$. If P has degree two in M', then attaching D (and its attaching segment) divides a segment of M' into two segments. Thus the number of segments in M is at most $4(\nu - 1) - 1 + 4 = 4\nu - 1$.

Case II. $D^{\cdot}$ contains an interior edge of M. Let M' result from M by deleting A. M' is reduced, connected, and simply connected; also, M' has at most $\nu - 1$ regions. Let P and P' be the endpoints of A. If P and P' both have degree two, then M has at most two more segments than M'. If one of P and P' has degree two, then M has at most one more segment than M'. Otherwise, M has no more segments than M'. In any case, the number of segments of M is at most $4\nu - 1$.

It follows at once from its definition that a segment is either a maximal consecutive part of $D^{\cdot} \cap M^{\cdot}$ for some region D or else is a simple arc whose interior is not on the boundary of any region. Given any reduced map M, we can construct a map M^* in which all boundary edges are segments, simply by deleting boundary vertices of degree two and combining the incident edges.

4. In this section we prove the principal lemma. First we shall give numerous reductions of the problem and auxilliary lemmas. Recall that we are given an open formula $M(\mathbf{x}, \mathbf{y})$ of the basic language, a tuple $\mathbf{u}$ of elements from F_m, a sufficiently large value of the parameter μ, and a projection $\hat{}: F_m \twoheadrightarrow F_{m'}$ defined by $\hat{f} = f$ for f in $F_{m'}$ and $\hat{\zeta}_i = \Gamma(i, \mu)$ for $i > m'$. We seek an algorithm which, when given a tuple $\mathbf{v}$ of elements of $F_{m'}$ such that $M(\hat{\mathbf{u}}, \mathbf{v})$ holds, enables us to calculate pre-images $\check{\mathbf{v}}$ for the v's having the property that $M(\mathbf{u}, \check{\mathbf{v}})$ holds in F_m.

For any map $\hat{}$ for which $\check{\mathbf{v}}\hat{} = \mathbf{v}$, for any word $W(\mathbf{x}, \mathbf{y})$, if $W(\hat{\mathbf{u}}, \mathbf{v}) \neq 1$ in $F_{m'}$, then $W(\mathbf{u}, \check{\mathbf{v}}) \neq 1$ in F_m since positive sentences are preserved under quotients. Thus we need only ensure that the pre-image map $\check{}$ which we construct has the property that $W(\hat{\mathbf{u}}, \mathbf{v}) = 1$ in $F_{m'}$ implies that $W(\mathbf{u}, \check{\mathbf{v}}) = 1$ in F_m for each atomic subformula $W(\mathbf{x}, \mathbf{y}) = 1$ of $M(\mathbf{x}, \mathbf{y})$. We need only prove the lemma in the case that

M has precisely one atomic subformula $W_0(\mathrm{x}, \mathrm{y}) = 1$ for which $W_0(\hat{\mathrm{u}}, \mathrm{v}) = 1$. The case for more general M is handled as follows: Add a new letter d to both F_m and $F_{m'}$, obtaining the groups $\tilde{F}_m$ and $\tilde{F}_{m'}$. Suppose that $W_1(\hat{\mathrm{u}}, \mathrm{v}) = 1$, $W_2(\hat{\mathrm{u}}, \mathrm{v}) = 1$, and $\cdots$, and $W_\sigma(\hat{\mathrm{u}}, \mathrm{v}) = 1$ in $F_{m'}$. Then in $\tilde{F}_{m'}$ $\Pi d^i W_i(\hat{\mathrm{u}}, \mathrm{v}) d^{-i}$, $i = 1, 2, \cdots, \sigma$, equals 1. Therefore, by the special case, $\tilde{F}_m$ satisfies $\Pi\, d^i W_i(\mathrm{u}, \check{\mathrm{v}}) d^{-i}$, $i = 1, 2, \cdots, \sigma$. Thus F_m satisfies $W_1(\mathrm{u}, \check{\mathrm{v}}) = 1$, $W_2(\mathrm{u}, \check{\mathrm{v}}) = 1$, $\cdots$, and $W_\sigma(\mathrm{u}, \check{\mathrm{v}}) = 1$.

Let L be the length of the word $W(\mathrm{u}, \mathrm{y})$ as an element of the group $F_m * \langle \mathrm{y} \rangle$. Recall that s is the length of the sequence of variables y. Let s' be the number of distinct maximal subwords of elements of u on the generators of $F_{m'}$, and let ρ be the maximum length of such subwords. Let p be the number of occurrences of the letters ζ_i, $i > m'$, in $W(\mathrm{u}, \mathrm{y})$; let $\pi = L(s + s')(2s + 2s' + 1)t + 4p - 1$. Define $\mathrm{BIG}(M, u) = (\pi - 1)(\rho + 1) + p + 1$.

Let $T = \{2^i, i \text{ in } \mathrm{N}\}$. Let t be any integer; define $T + t = \{(a + t), a \text{ in } T\}$.

Lemma 4.1. *If $t \neq 0$, then $T \cap T + t$ has at most one element.*

Proof. Suppose $t > 0$. Let 2^a and 2^b be elements of $T + t \cap T$ and 2^c and 2^d be in T, where $2^a = 2^c + t$ and $2^b = 2^d + t$. Thus $t = 2^a - 2^c = 2^c + 2^{c+1} + \cdots + 2^{a-1} = 2^b - 2^d = 2^d + 2^{d+1} + \cdots + 2^{b-1}$. Therefore, $a = b$ and $c = d$. If $t < 0$, proceed as above with the roles of a and c, and b and d reversed.

Recall that $\alpha_i = \beta^i \gamma \beta^{-i}$. Let $\theta_{i,j} = \beta^i \zeta_j \beta^{-1}$, for $j = 3, 4, \cdots, m$ and i any integer. Let K be the subgroup of $F_{m'}$ generated by the α_i and the $\theta_{i,j}$ for $i \leq m'$ and let J be the subgroup of F_m generated by all of the α_i and the $\theta_{i,j}$. Let $\rho_1, \rho_2 \cdots$ be variables ranging over the generators of J and $\eta_1, \eta_2 \cdots$ be variables ranging over the generators of K. Let $\Upsilon_1, \Upsilon_2, \cdots$ be variables ranging over words on the ρ_i, and $\chi_1, \chi_2, \cdots$ be variables ranging over words in the η_i.

It is clear that every element of J has exponent sum zero on β. The following procedure writes all words in the generators of F_m with exponent sum zero on β as a word on the generators of J. First let $\alpha_i^{(t)} = \alpha_{i+t}$ and $\theta_{i,j}^{(t)} = \theta_{i+t,j}$ and $\rho_k^{(t)} = \alpha_i^{(t)}$ or $\theta_{i,j}^{(t)}$ according as ρ_k is α_i or $\theta_{i,j}$, where t may be any integer. If $\Upsilon = \rho_{i_1} \rho_{i_2} \cdots \rho_{i_k}$, let $\Upsilon^{(t)} = \rho_{i_1}^{(t)} \rho_{i_2}^{(t)} \cdots \rho_{i_k}^{(t)}$. If $a = \Pi \Upsilon_i \beta^{\delta_i}$ where $\Sigma \delta_i = 0$, then $a = \Pi \Upsilon_i^{(q_i)}$ where $q_1 = 0$ and $q_{i+1} = q_i + \delta_i$. For example, if $a = \alpha_1 \beta^{\delta_1} \alpha_2 \beta^{\delta_2} \theta_{1,3} \beta^{\delta_3}$, then

$$a = \alpha_1 (\beta^{\delta_1} \alpha_2 \beta^{-\delta_1})(\beta^{\delta_1 + \delta_2} \theta_{1,3} \beta^{-(\delta_1 + \delta_2)}) = \alpha_1 \alpha_{2+\delta_1} \theta_{(1+\delta_1+\delta_2),3}.$$

Consequently if b is an element of J, b can be uniquely written in the form $\Upsilon \beta^\delta$ where δ is the exponent sum on β in b. Since $K = J \cap F_{m'}$, the corresponding statements apply where J, F_m, and Υ are replaced by K, $F_{m'}$ and χ, respectively. Let $\Lambda = \{\alpha_i, i \text{ in } T\}$ and $\Lambda^{(t)} = \{\alpha_i^{(t)}, \alpha_i \text{ in } \Lambda\}$. If $t \neq 0$, then, by Lemma 4.1, the set $\Lambda \cap \Lambda^{(t)}$ has at most one member. These facts are summarized in the following lemma.

Lemma 4.2. *Let a and c be elements of F_m and $F_{m'}$ respectively.*

(i) *a is an element of J if and only if a has exponent sum zero on β.*

(i′) *c is an element of K if and only if c has exponent sum zero on β.*

(ii) *a can be uniquely written in the form $\Upsilon\beta^\delta$ where Υ is in J.*

(ii′) *c can be uniquely written as $\chi\beta^\delta$ where χ is in K.*

(iii) *If $t \neq 0$, then $\Lambda \cap \Lambda^{(t)}$ has at most one element.*

Let A be a free group. Let $a = a_1 a_2 \cdots a_m$ and $b = b_1 b_2 \cdots b_n$ be normal forms for elements of A. If $a_m \neq b_1^{-1}$, then there is *no cancellation* in the product ab. This situation is denoted $ab = a \cdot b$. If $a = a' \cdot c$ and $b = c^{-1} \cdot b'$, then c and c^{-1} will be called *cancelled parts* in the product ab. An *equation over A with variables* y is a freely reduced word of $A^*\langle \mathrm{y}\rangle$. If W is an equation over A with variables y, a *solution* to W is a homomorphism b such that $ba = a$ for a in A, each by is an element of A and $bW = 1$. A solution can be given by specifying the images of the elements of y. In this terminology our problem can be stated as follows: given an equation $W_0(\hat{\mathrm{u}}, \mathrm{y})$ which has a solution $\check{\mathrm{v}}$ over $F_{m'}$, calculate a solution $\check{\mathrm{v}}$ to $W_0(\hat{\mathrm{u}}, \mathrm{y})$ in F_m such that $\check{\mathrm{v}}\hat{} = \mathrm{v}$.

If x is a variable, the expression $x^{(t)}$ is called a *modified variable.* A *modified equation* over F_m (or $F_{m'}$) with variables x is an equation over F_m in which the variables are chosen from the set $\{x^{(t)}, x \text{ in } \mathrm{x}, t \text{ in } \mathbf{Z}\}$ ($x^{(t)}$ and $x^{(t^*)}$ are to be considered as distinct symbols unless $t = t^*$). If W is a modified equation over $F_{m'}$, W is just an abbreviation for the unmodified equation obtained from W by replacing each occurrence of $x^{(t)}$ by $\beta^t x \beta^{-t}$ for each variable x and each value of t. In what follows, it will be convenient to treat modified equations instead of the equations which they abbreviate. A solution **b** to a modified equation is simply a solution to the corresponding unmodified equation.

Our equation $W_0(\hat{\mathrm{u}}, \mathrm{y})$ having a solution v in $F_{m'}$ can easily be converted to an equivalent modified equation having a solution χ in K; this is seen immediately when one notes that $W_0(\hat{\mathrm{u}}, \mathrm{v})$ must have exponent sum zero on β. For example, suppose that $W_0(\mathrm{x}, \mathrm{y})$ is $y_1 x y_2$, that **u** is simply ζ_1, and that an appropriate choice for μ is 3. Then $W_0(\hat{\mathrm{u}}, \mathrm{y})$ is $y_1\Gamma(1, 3)y_2$. One solution to this equation is $y_1 = \alpha_1\beta^2$ and $y_2 = [\Gamma(1, 3)^{-1}]^{(-2)}\alpha_{-1}^{-1}\beta^{-2}$. The corresponding modified equation over K, $W_1(\hat{\mathrm{u}}^*, \mathrm{y})$, is $y_1[\Gamma(1, 3)]^{(2)}y_2^{(2)}$ and its solution $\chi_1 = \alpha_1$ and $\chi_2 = \Gamma(1, 3)^{-1}\alpha_{-1}^{-1}$. The problem has now been reduced to the one of converting this solution χ (in K) to this modified equation to a solution χ (in J) to the equation $W_1(\mathbf{u}^*, \mathrm{y};) = y_1\theta_{2,3}y_2^{(2)}$ with the added property that $\check{\chi}\hat{} = \chi$.

A couple H consisting of a modified equation over F_m, $W_1(\mathbf{u}^*, \mathbf{y})$ and a solution χ to $W_1(\hat{\mathbf{u}}^*, \mathbf{y})$ is said to be reduced if $W_1(\mathbf{u}^*, \chi)$ is freely reduced and nontrivial, and if no element of χ is trivial. The following inductive procedure converts an arbitrary couple to a reduced couple. Let $W_0(\mathbf{u}, \mathbf{y})$ be our original equation with $\mathbf{v}$ a solution to $W_0(\hat{\mathbf{u}}, \mathbf{y})$; let $z_1, z_2, \cdots, z_{s'}$ be new variables. Obtain $U_0(\mathbf{u}_0, \mathbf{y}_0)$ by replacing distinct maximal subwords of elements of $\mathbf{u}^*$ on the generators of F_m, by distinct variables z_i which we will call restricted variables. (Recall that there were s' distinct such subwords.) Let $\mathbf{v}_0$ be the sequence obtained from $\mathbf{v}$ by appending the subwords for which the z's were inserted. Thus $\mathbf{v}_0$ is a solution to $U_0(\mathbf{u}_0, \mathbf{y}_0)$. Let $U_1(\mathbf{u}_1, \mathbf{y}_1)$ be the equivalent modified equation and χ_1 a solution to $U_1(\mathbf{u}_1, \mathbf{y}_1)$. Let H_1 consist of U_1 and χ_1. Suppose H_n has been defined but is not yet a reduced couple. If there exists an adjacent pair of modified elements of $\mathbf{y}_n$ in $U_n(\mathbf{u}_n, \mathbf{y}_n)$, $[y^\epsilon]^{(t)}[y^{*\epsilon^*}]^{(t^*)}$, such that $\chi^{\epsilon^{(t)}} \chi^{*\epsilon^{*(t^*)}}$ has a nontrivial cancelled part, say

$$\chi^{\epsilon^{(t)}} = \Psi^{\epsilon^{(t)}} \cdot c \quad \text{and} \quad [\chi^{*\epsilon^*}]^{(t^*)} = c^{-1} \cdot \Psi^{*\epsilon^{*(t^*)}},$$

where c is the maximal cancelled part, proceed as follows: (1) Let $\tilde{y}$ be a new variable. (2) Replace y^ϵ at all occurrences in U_n by $y^\epsilon[\tilde{y}^\epsilon]^{(-t)}$ and $y^{*\epsilon^*}$ by $[\tilde{y}^{*-\epsilon^*}]^{(-t^*)}y^{\epsilon^*}$ and append $\tilde{y}$ to $\mathbf{y}_n$; if either y or y^* is restricted then $\tilde{y}^*$ is restricted. (3) Replace χ by Ψ, χ^* by Ψ^*, and append c to χ_n. (4) Delete all trivial elements from the resulting sequence of solution elements, and delete the corresponding elements from the variable sequence and from U_n as modified in step (2). Call the resulting variable and solution sequences $\mathbf{y}_{n+1}$ and χ_{n+1}. (5) Freely reduce the expression obtained from $U_n(\mathbf{u}_n, \mathbf{y}_n)$ in step (4) to obtain $U_{n+1}(\mathbf{u}_{n+1}, \mathbf{y}_{n+1})$. If there is no such adjacent pair, then reducedness must be violated by the existence of a trivial element of χ_n. Obtain H_{n+1} from H_n by applying steps (4) and (5) of the preceding instructions.

The convergence of the above algorithm is clear when one notes that once it has been applied for a product of a pair of (modified) variables $y^\epsilon y^{*\epsilon^*}$, the products of χ's corresponding to all of the following expressions (each of the variables may also be modified) which actually occur in one of our subsequent couples are freely reduced: $y^\epsilon \tilde{y}^\epsilon$, $y^\epsilon y^{*\epsilon^*}$, $\tilde{y}^{\epsilon^*} y^{*\epsilon^*}$. Consequently, at most one new variable is introduced for each possible pair $y^\epsilon y^{*\epsilon}$ in $\mathbf{y}_1$. There are $2(s + s')^2$ distinct such pairs. Consequently, when the procedure terminates, we have an equation with at most $(s + s')(2s + 2s' + 1)$ variables, of which at most $s'(4s + 2s' + 1)$ are restricted variables. Note that restricted χ's in χ_n have length at most ρ because each is a subword of a translate of a restricted element of χ_1.

Our final reduction of the problem has now been obtained. Given a reduced couple with equation $U_n(\mathbf{u}_n, \mathbf{y}_n)$ and solution χ_n in K to $U_n(\hat{\mathbf{u}}_n, \mathbf{y}_n)$, calculate a solution to the former equation χ_n with the properties that $\check{\hat{\chi}}_n = \chi_n$ and if y is a restricted variable, and χ is the corresponding element of χ_n, then $\check{\chi} = \chi$. The rest of this paper is devoted to solving this problem.

We will consider maps and diagrams over the free group J with the symmetrised set R of relations determined by $\theta_{i,j} = [\Gamma(j, \mu)]^{(i)}$, i an integer, $m' < j \leq m$. An immediate consequence of Lemma 4.2 (iii) is that cancelled parts in products of elements of R have length at most 1. Observe that K is simply the quotient of J by the normal subgroup generated by R. The diagrams we wish to consider will be the diagrams for sequences of conjugates of elements of R.

Let M be a reduced diagram. The label on an internal edge of M must be a cancelled part in the product of two elements of R since the label on an internal edge is cancelled in the product of the two elements of R which label the boundaries of the two regions (reading from one fixed end of the edge in question) on either side of that edge. Consequently, in reduced diagrams of the types which we consider, the labels on internal edges have length one; furthermore no two regions can share two or more edges, each with label of length 1 by Lemma 4.2 (iii).

Since each region D has $D^{\cdot}$ labelled by a member of R and no $\theta_{i,j}$ can be a cancelled part in a product of two distinct members of R, each region D has $D^{\cdot} \cap M^{\cdot}$ including at least one edge.

Let $c_1, c_2, \cdots, c_p$ be a sequence of conjugates of elements of R. The minimal diagram for such a sequence will have at most p regions since the cyclically reduced part of each c_k contains exactly one $\theta_{i,j}^{\pm 1}$ and these letters can not be shared by the labels on distinct regions. Furthermore, each region D has the sum of the lengths of the labels on $D^{\cdot}$ equal to $\mu + 1$. At most $p - 1$ edges on $D^{\cdot}$ are shared with other regions, and consequently, the sum of the lengths of the labels on $D^{\cdot} \cap M^{\cdot}$ is at least $\mu + 2 - p$.

Let $U_n(\mathbf{u}_n, \mathbf{y}_n)$ and χ_n be the reduced couple in question. $U_n(\mathbf{u}_n, \chi_n)$ is freely reduced, contains at most p occurrences of letters $\theta_{i,j}$ for $j > m'$ (since the original equation $W_0(\mathbf{u}, \mathbf{y})$ had p occurrences of ζ_j for $j > m'$) and $U_n(\hat{\mathbf{u}}_n, \chi_n) = 1$ in K. Therefore $U_n(\mathbf{u}_n, \chi_n)$ is equal in J to a product of a sequence of at most p conjugates of elements of R. Let M_0 be the reduced diagram corresponding to a minimal such sequence, and let M be the corresponding segment diagram. The label on $M^{\cdot}$ is $U_n(\mathbf{u}_n, \chi_n)$. The boundary vertices of M give one partition of this word into at most $4p - 1$ cells, and the spelling of $U_n(\mathbf{u}_n, \mathbf{y}_n)$ gives another partition of this word, in which the cells either contain (a translate of) a member of $\mathbf{u}_n$, or (a translate of) a member of χ_n corresponding to an occurrence of a particular variable. Let Π be the coarsest common refinement of these two partitions. Call the cells of Π *constant cells*, *restricted cells* or *unrestricted cells* according as these cells contain subwords of constants or members of χ_n corresponding to restricted or unrestricted variables. Π has at most $\pi = L(s + s')(2s + 2s' + 1) + 4p - 1$ cells. (M has at most $4p - 1$ segments; L is the length of $W_0(\mathbf{u}, \mathrm{y})$; for the sake of an estimate we suppose that each term in this expression is split into a part for each variable in y_n.)

Let N be the map which arises from M by adding vertices of degree two to reflect this refinement Π. The boundary edges of N are labelled by the contents of the corresponding cells of Π. For each region D of N, $D^{\cdot} \cap N^{\cdot}$ has total label length at least $\mu + 2 - p$. Further, the edge of N which is labelled with the $\theta_{i,j}$ $(j > m')$ for this region contains that letter alone. Therefore, the remaining $\mu + 1 - p$ letters on $D^{\cdot}$ are divided among at most $\pi - 1$ cells. By the pigeonhole principal, one of these cells must contain at least $(\mu + 1 - p)/(\pi - 1)$ letters. This particular cell must be an unrestricted cell, since restricted cells can contain at most ρ letters. Let the label on this cell be Δ. If Δ is replaced by Δr, where r is the relator in R with the initial segment Δ^{-1}, in both χ_n and on the boundary of N, the regions with boundary edges labelled by Δ become regions with a boundary which freely reduces to 1 in J. Therefore, if the word is freely reduced and the corresponding reduced diagram $\tilde{M}$ is constructed, $\tilde{M}$ has fewer regions. If this replacement procedure is carried out at most p times, the resulting diagram will be the trivial diagram with no regions. That is, we will have replaced the sequence χ_n by a sequence $\check{\chi}_n$ having the property that $U_n(\mathrm{u}_n, \check{\chi}_n) = 1$ in J. Moreover, since the replacements are only made in unrestricted cells, if χ is a restricted element of χ_n, $\check{\chi} = \chi$. Thus we have described the desired algorithm and have proved

Lemma 4.3 (*the principal lemma*). *Suppose that* $\mu > \mathrm{BIG}(M, \mu)$. *Let* $\hat{}$ *be a homomorphism from* F_m *onto* $F_{m'}$, *defined by* $\hat{f} = f$ *in* $F_{m'}$, *and* $\hat{\zeta}_i = \Gamma(i, \mu)$, *for* $i > m'$. *Then for any s-tuple* v *of elements of* $F_{m'}$, *for which* $M(\hat{\mathbf{u}}, \mathrm{v})$ *holds, one can effectively calculate a sequence* $\check{\mathrm{v}}$ *of elements of* F_m *such that* $M(\mathbf{u}, \check{\mathrm{v}})$ *holds and such that* $\check{v} = \hat{\check{\mathrm{v}}}$. *Moreover* $\check{\mathrm{v}}$ *is obtained by replacing certain subwords of elements of* v *on the letters* β *and* γ *by words* F_m *involving the* ζ_i.

BIBLIOGRAPHY

1. R. C. Lyndon, *On Dehn's algorithm*, Math. Ann. 166 (1966), 208–228. MR 35 #5499.

2. Ju. I. Merzljakov, *Positive formulae on free groups*, Algebra i Logika Sem. 5 (1966), no. 4, 25–42. (Russian) MR 36 # 5201.

3. P. E. Schupp, *On Dehn's algorithm and the conjugacy problem*, Math. Ann. **178** (1968), 119–130. MR 38 #5901.

MATHEMATICAL INSTITUTE, OXFORD UNIVERSITY, OXFORD OX1 3LB, ENGLAND

Current address: Institute for Advanced Study, Princeton, New Jersey 08540