EQUATIONS IN FREE GROUPS[1]

BY

R. C. LYNDON

1. **Introduction and summary.** If $w(x)=w(x, a_1, \cdots, a_r)$ is any element of the free group on generators $x, a_1, \cdots, a_r$, one may ask what elements $u=u(a_1, \cdots, a_r)$ of the free subgroup on generators $a_1, \cdots, a_r$ satisfy the equation $w(u)=1$. As a trivial example, if $w(x)=xa_1a^{-1}a_1^{-1}$, the solutions u are all elements a_1^{ν} where ν is an integer. This example suggests already that the answer to the general problem should be sought in terms of "parametric words," that is, of group theoretic expressions in the generators $a_1, \cdots, a_r$ that contain certain integer-valued parameters $\nu_1, \cdots, \nu_d$ as exponents. In fact, we succeed in giving an effective method of associating with any $w(x)$, except $w(x)=1$ identically, a finite set of such parametric words with the property that the set of group elements represented by them under all substitutions of integers for the parameters is precisely the set of all elements u such that $w(u)=1$.

The establishment of this result falls into two parts. The key to the first part is a familiar cancellation argument that seems to originate with Nielsen [3] (see also, for example, Nielsen [4] and Kurosh [1, vol. 2, p. 17]) saying, roughly, that if, in a product of words representing elements of a free group, no word cancels entirely into the two adjacent words, then the product can not reduce to the empty word. This, or even a weaker argument, when applied to a given solution u of the equation $w(u)=1$ provides a transformation of $w(x)$ into $w'(x)$ with u going into corresponding u' that is shorter than u, and hence, after a finite number of iterations, yields $w''(x)$ with corresponding $u''=1$, from which u can be recovered. The crucial step is to specify these transformations in such a way that the nature of the transformations, as well as a bound on their number, depends only on $w(x)$ and not upon u. This proves possible if one admits parametric words, and enables us to associate with $w(x)$ a finite set of parametric words whose values *include* all solutions u of $w(u)=1$.

The second part of the argument is devoted to replacing this set of parametric words by a new set whose values are precisely all solutions. For this we require the theory of free X-groups, where X is the polynomial ring $Z[\nu_1, \cdots, \nu_d]$, and, although we try to make clear here all the concepts and results required, we must refer to an earlier paper [2] for a basic algorithm.

2. **A class representing all solutions.** We begin by reviewing some familiar considerations in the theory of free groups. Let G be the free group on a speci-

Received by the editors January 26, 1960.

(1) This work was supported in part by National Science Foundation Grants and by Contract Nonr 2631(00) with the Office of Naval Research.

fied set of generators. A *letter* is a generator or the inverse of a generator. A *word* is a finite sequence, possibly empty, of letters, and *represents* that group element which is the product of its letters, in order. A word is *reduced* if no two successive letters are inverses of each other. Every group element is represented by exactly one reduced word. We write $w=w_1\cdot w_2\cdot\ \cdots\ \cdot w_n$ to express that w is the product of $w_1, w_2, \cdots, w_n$ "without cancellation": that is, the reduced word representing w is the result of juxtaposing, in order, the reduced words for $w_1, w_2, \cdots, w_n$. Commonly, in a product uv some part ending u will cancel against some part beginning v; precisely, for all u and v there exist unique u', v' and p such that $u=u'\cdot p$, $v=p^{-1}\cdot v'$ and $uv=u'\cdot v'$. It is useful to note that a relation $u\cdot v=u'\cdot v'$ implies either $u=u'\cdot p$, $v'=p\cdot v$ for some p, or else $u'=u\cdot p'$ and $v=p'\cdot v'$ for some p'. Further, each u can be written uniquely as $u=p^{-1}\cdot v\cdot p$ where v is *cyclically reduced*, that is, $vv=v\cdot v$.

To state the key result mentioned above, define a triple of group elements, (u, v, w), to be *singular* if v cancels entirely in forming the product uvw: precisely, if there exist u', w', p and q such that $u=u'\cdot p$, $w=q\cdot w'$ and $v=p^{-1}\cdot q^{-1}$, whence $uvw=u'w'$.

PROPOSITION 1. *If* $w_1w_2\cdot\ \cdots\ \cdot w_n=1$, $n\geqq 1$, *then at least one of the triples* $(1, w_1, w_2)$, (w_1, w_2, w_3), $\cdots$, (w_{n-2}, w_{n-1}, w_n), $(w_{n-1}, w_n, 1)$ *is singular.*

To prove this, suppose that $w_1, w_2, \cdots, w_n$, $n\geqq 1$, are elements such that none of the triples listed is singular. Elements p_i, for $1\leqq i<n$ are uniquely determined by the conditions $w_i=w_i'\cdot p_i$, $w_{i+1}=p^{-1}\cdot w_{i+2}''$, $w_iw_{i+1}=w_i'\cdot w_{i+1}''$, and it follows from the hypothesis that

$$w_1 = v_1\cdot p_1,\quad w_2 = p_1^{-1}\cdot v_2\cdot p_2,\ \cdots,\ w_{n-1} = p_{n-2}^{-1}\cdot v_{n-1}\cdot p_{n-1},\quad w_n = p_{n-1}^{-1}\cdot v_n$$

for elements $v_1, v_2, \cdots, v_n\neq 1$ such that $v_iv_{i+1}=v_i\cdot v_{i+1}$. It follows that $w_1w_2\cdot\ \cdots\ \cdot w_n$ has the nonempty reduced form $v_1\cdot v_2\cdot\ \cdots\ \cdot v_n$, whence the product is not 1.

We want now to apply this proposition to the situation that $w(x)$ and u are given such that $w(u)=1$. The reduced representation of $w(x)$ yields a unique expression of $w(x)$ in the form

$$w(x) = a\cdot x^{e_1}\cdot c_2\cdot x^{e_2}\cdot c_3\cdot\ \cdots\ \cdot c_t\cdot x^{e_t}\cdot b,$$

for some $t\geqq 0$, $e_1, e_2, \cdots, e_t=\pm 1$, and $a, c_2, \cdots, c_t, b$ elements of the free group F_0 on generators $a_1, \cdots, a_r$. The *degree* of $w(x)$ is t. If $w(x)=1$ identically, all elements u of F_0 are solutions, and since it is evident that, for $r>1$, there is no finite set of parametric words representing all u in F_0, we have no choice but to exclude this case from consideration. Otherwise, if $w(x)$ has degree $t=0$, $w(u)$ assumes the same value $w\neq 1$ for all u, the set of solutions is empty, and the conclusion that we are seeking holds vacuously. It is easy

to check that, if we begin with some $w(x)$ of degree $t>0$, all new $w'(x)$ introduced in the course of the reasoning that follows will also have positive degree, so that we are justified in tacitly excluding the case $t=0$ from further consideration.

It is convenient to define $c_{t+1}=c_1=ba$ and $e_{t+1}=e_1$. With any $w(x)$ as above, and any element u in F_0, we now define the set $A(w, u)$ to consist of all consecutive triples in the sequence obtained from

$$u^{e_t}, c_1, u^{e_1}, c_2, u^{e_2}, c_3, \cdots, c_t, u^{e_t}, c_1, u^{e_1}$$

by deleting any terms $c_i=1$. Then Proposition 1 gives us immediately the following result.

PROPOSITION 2. *If $w(x)$ and u are such that $w(u)=1$, then $A(w, u)$ contains at least one singular triple.*

Under the supposition that a triple of the type (c_i, u, c_{i+1}) is singular, the element u is determined, within a finite number of possibilities, from the knowledge of $w(x)$ alone. For this supposition requires that there exist p, q, r, and s such that $c_i=p\cdot q$, $c_{i+1}=r\cdot s$ and that $u=q^{-1}r^{-1}$, and it is clear that there are only finitely many such "factorizations" of the given c_i, c_{i+1}, hence only finitely many such elements u. It is hardly necessary to emphasize that not all elements u obtained in this fashion need satisfy the equation $w(u)=1$.

In the same vein, suppose a triple (u, u, c_i) is singular. Write $u=p^{-1}\cdot v\cdot p$ with v cyclically reduced. Since $uu=p^{-1}\cdot v\cdot v\cdot p$, the supposition requires that $v\cdot p$ cancel entirely into c_i, hence that c_i have the form $c_i=p^{-1}\cdot v^{-1}\cdot q$ for some q. Since given c_i has only finitely many factorizations of this sort, there are only finitely many possibilities for u.

Similar reasoning applies to singular triples of the type (u, c_i, u), under an additional hypothesis. Singularity implies that we have both $u=p\cdot q$ and $u=r\cdot s$ where $c_i=q^{-1}\cdot r^{-1}$. We make here the further hypothesis that the parts q and r together include all of u, hence, for some v, y, z that $u=v\cdot y\cdot z$ with $q=y\cdot z$, $r=v\cdot y$, and therefore $c_i=z^{-1}\cdot y^{-1}\cdot y^{-1}\cdot v^{-1}$. It then follows as before that there are only finitely many possibilities for u.

A further case is that of a singular triple (u, u, u). Writing $u=p^{-1}\cdot v\cdot p$, with v cyclically reduced, we see that $uuu=p^{-1}\cdot v\cdot v\cdot v\cdot p$, and singularity implies that $v=1$ and hence $u=1$.

Triples (c_i, u^{-1}, c_{i+1}) can be treated in a manner symmetrical to that for (c_i, u, c_{i+1}). Triples (u^{-1}, u^{-1}, c_i), (c_i, u, u) and (c_i, u^{-1}, u^{-1}) are symmetrical with (u, u, c). Triples (u^{-1}, c_i, u^{-1}) are symmetrical with (u, c_i, u); and (u^{-1}, u^{-1}, u^{-1}) with (u, u, u).

The remaining possibilities we term *critical triples*; these are singular triples of the types $(u^e, c, u^{e'})$, for $e, e'=\pm 1$, where, if $e=e'$, we require that $u^e=p\cdot q\cdot r$ and $c_i=r^{-1}\cdot p^{-1}$ for some $q\neq 1$ and p, r.

With each $w(x)$ we associate the finite set $B(w)$ of all elements of the following forms:

(i) $q^{-1}r^{-1}$ *where some* $c_i^{\pm 1} = p \cdot q$, $c_j^{\pm 1} = r \cdot s$;

(ii) $p^{-1}vp$ *where some* $c_i^{\pm 1} = p^{-1} \cdot v_j^{\pm 1} \cdot r$, $v \neq 1$;

(iii) pqr *where some* $c_i^{\pm 1} = p \cdot q \cdot q \cdot r$, $q \neq 1$.

Note that 1 is in $B(w)$ by virtue of (i), and that $B(w)$ includes all values for u arising from a noncritical singular triple. This establishes the following.

PROPOSITION 3. *If* $w(u) = 1$, *then either* u *is in* $B(w)$ *or else* $A(w, u)$ *contains some critical triple.*

Our next aim is to show that if $A(w, u)$ contains a critical triple, it is possible to replace $w(x)$ and u by a pair $w'(x)$ and u', equivalent for the purpose at hand, such that $A(w', u')$ contains fewer critical triples than $A(w, u)$. More specifically, with each critical triple $\tau = (u^e, c, u^{e'})$, $e, e' = \pm 1$, we shall associate an element $d(x) = axb$, where a and b are in F_0, such that $w'(x) = w(axb)$ and $u' = a^{-1}ub^{-1}$ have the desired property. In view of the symmetry defined by the antiautomorphism $v \to v^{-1}$, it will suffice to treat only the two types of critical triples, (u, c, u) and (u, c, u^{-1}).

CASE 1. *Critical* $\tau = (u, c, u)$. By hypothesis we have $u = p \cdot q \cdot r$ and $c = r^{-1} \cdot p^{-1}$ for some $q \neq 1$, p, and r. It may happen that either $r^{-1} = p \cdot z$ or $p^{-1} = z \cdot r$ for some z; by left-right symmetry it suffices to treat only the former case. *Case* 1a. $r^{-1} = p \cdot z$. Then $u = p \cdot q \cdot z^{-1} \cdot p^{-1}$, $c = p \cdot z \cdot p^{-1}$, and, since $c \neq 1$, $z \neq 1$. Therefore we can write $u = p \cdot z^m \cdot u' \cdot z^{-n} \cdot p^{-1}$ where, first, $n > 0$ is maximal, and then (for this n), $m \geqq 0$ is maximal. In this case we define $d(x) = pz^m xz^{-n}p^{-1}$. *In Case* 1b, where neither $r^{-1} = p \cdot z$ nor $p^{-1} = z \cdot r$, we define $d(x) = pxr$.

CASE 2. *Critical* $\tau = (u, c, u^{-1})$. Write $c = p \cdot z \cdot p^{-1}$ with $z \neq 1$ cyclically reduced. Singularity requires first that $u = v \cdot p^{-1}$ for some v, and hence $ucu^{-1} = vzv^{-1}$. Moreover, cyclically reduced z can not cancel both left against v and right against v^{-1}, so that singularity requires that it cancel wholly to one side, and by symmetry we may suppose that $v = r \cdot z^{-1}$ for some r. *In Case* 2a, where $r = p \cdot q$ for some q, we have that $u = v \cdot p^{-1} = r \cdot z^{-1} \cdot p^{-1} = p \cdot q \cdot z^{-1} \cdot p^{-1}$, and we may write $u = p \cdot z^m \cdot u' \cdot z^{-n} \cdot p^{-1}$ with first $n > 0$ and then $m \geqq 0$ maximal, and define $d(x) = pz^m xz^{-n}p^{-1}$, exactly as in Case 1a. *In Case* 2b, we have $u = r \cdot z^{-1} \cdot p^{-1}$ where $r = p \cdot q$ for no q. We write $u = u' \cdot z^{-n} \cdot p^{-1}$ with $n > 0$ maximal, and define $d(x) = xz^{-n}p^{-1}$.

PROPOSITION 4. *Let* $d(x) = axb$ *be associated with a critical triple in* $A(w, u)$. *If* $w'(x) = w(axb)$ *and* $u' = a^{-1}ub^{-1}$, *then* $A(w', u')$ *contains fewer critical triples than* $A(w, u)$.

The proof of Proposition 4 depends on three lemmas. To state these, consider all the consecutive triples of the form $\tau = (u^e, c, u^{e'})$, $e, e' = \pm 1$ in the sequence

$$u^{e_t}, c_1, u^{e_1}, c_2, u^{e_2}, c_3, \cdots, c_t, u^{e_t}, c_1, u^{e_1},$$

where we no longer exclude triples with $c=1$, although by definition such triples are not counted as critical. Clearly the sequence associated with $w'(x)$ and u' will have exactly the same number, $t+1$, of triples of this sort as for $w(x)$, u; and the triple τ' corresponding to τ is easily calculated from τ. Proposition 4 will evidently be a consequence of the following three lemmas.

LEMMA 4.1. *If τ is a critical triple in $A(w, u)$, and $w'(x)$, u' are defined by means of $d(x)$ associated with τ, then the corresponding triple τ' is no longer critical.*

LEMMA 4.2. *If $c_{i+1} \neq 1$, but the triple $\tau = (u^{e_i}, c_{i+1}, u^{e_{i+1}})$ is not critical, then the corresponding triple τ' is not critical.*

LEMMA 4.3. *If $c_{i+1}=1$, so that $\tau = (u^{e_i}, c_{i+1}, u^{e_{i+1}})$ is by definition not critical, then also τ' is not critical.*

The proof of Lemma 4.1 falls into four cases, corresponding to the four cases that, using symmetry, were considered in defining the $d(x)$ associated with a critical triple.

CASE 1a. $\tau = (u, c, u) = (p \cdot z^m \cdot u' \cdot z^{-n} \cdot p^{-1}, p \cdot z \cdot p^{-1}, p \cdot z^m \cdot u' \cdot z^{-n} \cdot p^{-1})$ whence evidently $\tau' = (u', z^{m-n+1}, u')$. If $s = m-n+1 = 0$, τ' is by definition not a critical triple and we are done. Suppose $s>0$; since $n \geqq 1$, $m-n+1>0$ implies that $m>0$. The expression for u, with $m>0$, insures that there is no cancellation in the product $zu' = z \cdot u'$, hence none in the product $z^s u' = z^s \cdot u'$. Singularity of τ' would therefore require that z^s cancel entirely to the left into u', implying that $u' = v \cdot z^{-s}$ for some v, which contradicts the maximality of n. Suppose $s<0$; then $u'z^{-n} = u' \cdot z^{-n}$, $n>0$, implies that $u'z^s = u' \cdot z^s$. Singularity of τ' would require that z^s cancel entirely to the right into u', hence $u' = z^{-s} \cdot v$ for some v, which, since $s<0$, contradicts the maximality of m.

CASE 1b. $\tau = (u, c, u) = (r^{-1} \cdot u' \cdot q^{-1}, q \cdot r, r^{-1} \cdot u' \cdot q^{-1})$, whence $\tau' = (u', 1, u')$, by definition not critical. *Cases* 2a *and* 2b both give $\tau' = (u', z, u'^{-1})$. The expression for u gives $u'z^{-n} = u' \cdot z^{-n}$, $n \geqq 1$, hence $zu'^{-1} = z \cdot u'^{-1}$ so that singularity would require that z cancel entirely to the left into u', hence that $u' = v \cdot z^{-1}$ for some v, which contradicts the maximality of n.

To prove Lemma 4.2 we establish a slightly stronger result: if $w'(x) = w(axb)$ and $u = a \cdot u' \cdot b$, for arbitrary a and b in F_0, and τ is not critical, then corresponding τ' is not critical. By symmetry it suffices to treat the cases that $\tau = (u, c, u)$ or $\tau = (u, c, u^{-1})$. By induction on the sum of the lengths of a and b it suffices to treat the two cases that $u = a \cdot u'$ and $u = u' \cdot b$, where a and b are single letters. *First*, if $\tau = (u, c, u)$ there is symmetry between the cases $u = a \cdot u'$ and $u = u' \cdot b$, and we treat only the case $u = u' \cdot b$. Then $\tau' = (u', bc, u')$. Suppose that $bc = b \cdot c$. Then $u = u' \cdot b$ implies that bc does not cancel at all to the left, whence singularity of τ' would require that bc cancel entirely to the right, and that $u' = c^{-1} \cdot b^{-1} \cdot v$ for some v, and for τ' to be criti-

cal we would have $v=1$. But this contradicts the assumption that $u=u'\cdot b$. Supposing on the other hand that $bc\neq b\cdot c$, since b is a single letter we would have $c=b^{-1}\cdot f$ for some f, with $\tau'=(u', f, u')$. For τ' to be critical we would have to have $u'=p\cdot q\cdot r$ with $f=r^{-1}\cdot p^{-1}$ and $q\neq 1$. But this would imply that $u=p\cdot q\cdot r\cdot b$ with $c=b^{-1}\cdot r^{-1}\cdot p^{-1}$ and hence that τ was critical.

Second, let $\tau=(u, c, u^{-1})$, $c\neq 1$. If $u=a\cdot u'$, then $\tau'=(u', c, u'^{-1})$, and τ is not singular, so that c does not cancel entirely in the product ucu^{-1} and it will, a fortiori, not cancel entirely in $u'cu'^{-1}$. Suppose then that $u=u'\cdot b$, hence $\tau'=(u', bcb^{-1}, u'^{-1})$. If $bc=b\cdot c$, because $u'b=u'\cdot b$ and hence also $b^{-1}u'^{-1}$, singularity of τ' would require that bcb^{-1} not end in b^{-1}, hence that $c=f\cdot b$ for some f. It follows that $bcb^{-1}=b\cdot f$, and that this must cancel entirely to the right, into $u'^{-1}=f^{-1}\cdot b^{-1}\cdot v$ for some v. But this would give $u^{-1}=b^{-1}\cdot u'^{-1}=b^{-1}\cdot f^{-1}\cdot b^{-1}\cdot v=c^{-1}\cdot b^{-1}\cdot v$, implying that τ was singular. The case that $cb^{-1}=c\cdot b^{-1}$ follows by symmetry. There remains only the case that $c=b^{-1}\cdot f\cdot b$ for some f, where singularity of $\tau'=(u', f, u'^{-1})$ clearly implies that of $\tau=(u'b, b^{-1}fb, b^{-1}u'^{-1})$.

To prove Lemma 4.3 it suffices by symmetry to treat only the first of the two cases $\tau=(u, 1, u)$ and $\tau=(u^{-1}, 1, u^{-1})$. We proceed again according to the four cases under the definition of $d(x)$.

In Cases 1a *and* 2a, $\tau=(p\cdot z^m\cdot u'\cdot z^{-n}\cdot p^{-1}, 1, p\cdot z^m\cdot u'\cdot z^{-n}\cdot p^{-1})$, whence $\tau'=(u', z^{m-n}, u')$, and, taking $s=m-n$, the argument used for Case 1a of Lemma 4.1 shows that τ' can not be critical.

In Case 1b, $\tau=(p\cdot u'\cdot r, 1, p\cdot u'\cdot r)$ whence $\tau'=(u', rp, u')$. The hypothesis of this case ensures that neither factor of $c=rp$ cancels entirely into the other, whence c begins with the first letter of r and ends with the last letter of p, and from the expression $u=p\cdot u'\cdot r$ it follows that $u'cu'=u'\cdot c\cdot u'$.

In Case 2b, $\tau=(u'\cdot z^{-n}\cdot p^{-1}, 1, u'\cdot z^{-n}\cdot p^{-1})$ whence $\tau'=(u', z^{-n}\cdot p^{-1}, u')$. The expression $u=u'\cdot z^{-n}\cdot p^{-1}$ precludes any cancellation to the left. Singularity of τ' would therefore require that $z^{-n}\cdot p^{-1}$ cancel entirely to the right, into u', hence a fortiori into $u=u'\cdot z^{-n}\cdot p^{-1}$, $n\geqq 1$. But this contradicts the hypothesis for this case, that $u=r\cdot z^{-1}\cdot p^{-1}$ where $r=p\cdot q$ for no q.

The proof of Proposition 4 is complete. We now associate with each $w(x)$ a set $C(w)$ of elements that will include all $d(x)$ associated with any critical triple in $A(w, u)$, for any u. We define $C(w)$ to consist of all elements of the following forms:

(i) $pz^mxz^{-n}p^{-1}$, $xz^{-n}p^{-1}$, *or* pz^mx, *where some* $c_i^{\pm 1}=p\cdot z\cdot p^{-1}$, $z\neq 1$, *and* m *and* n *are integers*;

(ii) pxr *where some* $c_i^{\pm 1}=p\cdot r$.

Consider three finite sequences: $w_0(x)$, $w_1(x)$, $\cdots$, $w_k(x)$; $d_0(x)$, $d_1(x)$, $\cdots$, $d_{k-1}(x)$; and u_0, u_1, $\cdots$, u_k; and suppose that, for all i, $1\leqq i\leqq k$, we have $d_{i-1}(x)\in C(w_{i-1})$, $w_i(x)=w_{i-1}(d_{i-1}(x))$, and $u_{i-1}=d_{i-1}(u_i)$. If also $w_0(u_0)=1$, it follows that $w_i(u_i)=1$, $1\leqq i\leqq k$. We note also that $u_0=d_0(d_1(\cdots(d_{k-1}(u_k))\cdots))$.

By Proposition 4, if $w(x)=w_0(x)$ and $u_0=u$ are given satisfying $w(u)=1$,

there exists a chain of the sort described above such that the numbers of critical triples in $A(w_0, u_0)$, $A(w_1, u_1)$, $\cdots$ decrease strictly until some $A(w_k, u_k)$ is reached that contains no critical triples. Since $A(w_0, u_0)$ contains at most $t+1$ critical triples, where t is the degree of $w(x)$, we shall have $k \leqq t+1$. Since $w_k(u_k)=1$, while $A(w_k, u_k)$ contains no critical triples, it follows by Proposition 3 that w_k is in $B(w_k)$.

Associate with each $w(x)$ the set $D(w)$ of all elements u such that, for some $k \leqq t+1$, there exist $w_0(x)=w(x), \cdots, w_k(x)$ and $d_0(x), \cdots, d_{k-1}(x)$, related as above, together with an element u_k in $B(w_k)$ such that $u=d_0(d_1(\cdots(d_{k-1}(u_k))\cdots))$. Then the argument just given establishes the following.

PROPOSITION 5. *If $w(u)=1$, then u is in $D(w)$.*

The set $U(w)$ of all u in F_0 such that $w(u)=1$ is, in general, infinite; since $U(w) \subseteq D(w)$, the set $D(w)$ must inevitably also be infinite in general. However, $B(w)$ is finite, and the elements of $C(w)$ are among the values of a finite set of parametric words, obtained by replacing the integers m, n appearing in the definition of $C(w)$ by parameters μ and ν. By this device we shall define a finite set $D'(w)$ of parametric words whose values include all u such that $w(u)=1$.

There is only one obstacle to be surmounted. If we define $w_1(x)=w(d(x))$ where now $d(x)$ contains parameters, say $d(x)=pz^{\mu}xz^{-\nu}p^{-1}$, we find that the coefficients c_i of $w_1(x)$ now contain parameters, and in order to continue with the definition of a set $C'(w_1)$ of appropriate $d_1(x)$, we are required to find some substitute for the conditions, such as $c_i^{\pm 1}=p\cdot z\cdot p^{-1}$, that appear in the definition of $C(w)$.

For this purpose we need a precise concept of *parametric word*. Recursively, we define a parametric word of *height* 0 to be any ordinary reduced word (containing no parameters), while, for $t>0$, we define a parametric word of *height* t to be a formal expression

$$\omega = \omega_1^{\alpha_1}\omega_2^{\alpha_2}\cdots\omega_n^{\alpha_n}$$

where the $\omega_1, \cdots, \omega_n$ are parametric words of height $t-1$ and the elements $\alpha_1, \cdots, \alpha_n$ are polynomials in $X=Z[\nu_1, \cdots, \nu_d]$ for some $\nu_1, \cdots, \nu_d$. For our purposes it is not important to specify in detail what is meant by ω^{-1}, by a word $\omega(x)$ with coefficients γ_i, nor how the coefficients of $\omega_1(x)=\omega(\delta(x))$ are specified, where $\delta(x)=\alpha x\beta$ and α, β are parametric words not containing x.

A *factorization* relation, $\omega \sim \phi:\psi$ for parametric words will now be defined recursively. If ω is of height 0 we require that ϕ and ψ be of height 0, and that $u=v\cdot z$, where u, v, z are the elements of F_0 represented by ω, ϕ, ψ. For ω, as above, of height $t>0$, we require that

$$\phi = \omega_1^{\alpha_1}\omega_2^{\alpha_2}\cdots\omega_h^{\beta}\eta, \qquad \psi = \zeta\omega_h^{\gamma}\omega_{h+1}^{\alpha_{h+1}}\cdots\omega_n^{\alpha_n},$$

where $1 \leqq h \leqq n$, where β, γ are parameters, and η, ζ are parametric words of height $t-1$ such that $\omega \sim \eta : \zeta$. We define $\omega \sim \omega_1 : \omega_2 : \cdots : \omega_n$ to mean that $\omega \sim \omega_1 : \eta_1$, $\eta_1 \sim \omega_2 : \eta_2$, $\cdots$, $\eta_{n-2} = \eta_{n-1} \sim \omega_{n-1} : \omega_n$ for some $\eta_1, \cdots, \eta_{n-1}$.

It is routine to verify that if a parametric word ω represents an element u of F_0 under a certain assignment of values to the parameters, and if $u = u_1 \cdot u_2 \cdot \cdots \cdot u_n$, then there exist $\omega_1, \omega_2, \cdots, \omega_n$ such that $\omega \sim \omega_1 : \omega_2 : \cdots : \omega_n$ and that each ω_i represents corresponding u_i under the same assignment of values.

We can now paraphrase the definitions of $D(w)$, $C(w)$, and $D(w)$ for $\omega(x)$ that contain parameters. We define $B'(\omega)$ to consist of all elements of the following forms:

(i) $\phi^{-1}\psi^{-1}$ *where some* $\gamma_i^{\pm 1} \sim \eta : \phi$ *and* $\gamma_j^{\pm 1} \sim \psi : \zeta$ (γ_i, γ_j *coefficients of* $\omega(x)$);

(ii) $\phi^{-1}\psi\phi$ *where some* $\gamma_i^{\pm 1} \sim \phi_1^{-1} : \psi^{\pm 1} : \chi$;

(iii) $\phi\psi$ *where some* $\gamma_i^{\pm 1} \sim \phi : \chi : \psi$.

(We note that, to avoid certain ambiguities, we have made the set $B'(\omega)$ somewhat larger than necessary.) We define $C'(\omega)$ to consist of all parametric words of the following form:

(i) $\phi\psi^{\mu}x\psi^{\nu}\chi$ *where some* $\gamma_i^{\pm 1} \sim \phi : \psi : \chi$ *and* μ, ν *are parameters.*

The definition of $D'(\omega)$ now parallels exactly that of $D(w)$ in terms of the $B(w)$ and $C(w)$.

It is clear from the manner of definition of $D'(\omega)$ that, in the case that $\omega(x) = w(x)$ contains no parameters, $U(w)$ is included in the set of values of the elements of $D'(w)$. As defined, $D'(w)$ is not finite, since we have imposed no restriction on the new parameters introduced in the factorization process, or, explicitly, in the definition of $C'(\omega)$. Consequently we modify the definition by supposing the set of all parameters ordered, and requiring that in an element of $D'(w)$ these parameters be all distinct, and constitute an initial set of the totality of parameters. With this requirement, $D'(w)$ is finite, and we have established the following.

PROPOSITION 6. *There is an effective process associating with each* $w(x)$ *a finite set* $D'(w)$ *of parametric words such that the set of their values includes all* u *in* F_0 *satisfying* $w(u) = 1$.

3. **A class constituting all solutions.** Proposition 6 effectively associates with each nontrivial $w(x) = w(x, a_1, \cdots, a_r)$ a finite set of parametric words $\phi_1, \cdots, \phi_n$ in the generators $a_1, \cdots, a_r$, and containing certain parameters $\nu_1, \cdots, \nu_d$, such that each element u in the free group F_0 on generators $a_1, \cdots, a_r$ that satisfies $w(u) = 1$ is the value of some ϕ_i, $1 \leqq i \leqq n$, under a suitable substitution of integers for the parameters $\nu_1, \cdots, \nu_d$. Our ultimate goal is to replace these ϕ_i, effectively, by a finite set of parametric words $\psi_1, \cdots, \psi_m$, such that the union of the sets $V(\psi_j)$ of their values is precisely the set $U(w)$ of all u in F_0 that satisfy $w(u) = 1$. To accomplish this it will

clearly suffice to show that given $w(x)$ and ϕ effectively determine $\psi_1, \cdots, \psi_s$ such that

$$U(w) \cap V(\phi) \subseteq V(\psi_1) \cup \cdots \cup V(\psi_s) \subseteq U(w).$$

For this we use the main concepts and results of [2], which we will summarize as required. A *word* henceforth will be a pair (ω, C), where ω is the sort of formal expression that was called a "parametric word" previously, and C is a finite set of formal conditions $\rho\alpha = \rho\beta$ or $\rho\alpha < \rho\beta$, where α and β are elements of $X = Z[\nu_1, \cdots, \nu_d]$, $d \geqq 0$. If ρ is any retraction of X onto Z, that is, any assignment of values in Z to the parameters, we denote by $\rho\omega$ the element of F_0 represented by ω under this substitution. For the set of all values $\rho\omega$ of ω under ρ satisfying the conditions C we write $V(\omega, C)$.

The *roots* of ω are those expressions ξ such that ω contains a part ξ^α, with α not a constant; the *exponents* of ω are the α thus occurring. A word (η, C) is *primitive* if $(\eta, C) \equiv (\zeta^\alpha, C)$ only for $\alpha = \pm 1$; that is, the X-group axioms together with equations $\beta = \gamma$ whenever C contains the condition $\rho\beta = \rho\gamma$, do not suffice to imply any equation $\eta = \zeta^\alpha$ except for $\alpha = \pm 1$. Those properties of a *normal word* (ω, C), as defined in [2], that are essential here are the following: all its roots are primitive, that is, (ξ, C) is primitive for every root ξ of ω; all its exponents are positive, that is, C contains $\rho\alpha > 0$ for every exponent α of ω; and 1 does not belong to $V(\omega, C)$ unless $\omega = 1$ identically. It is a trivial matter to see that none of the results of [2] is affected if we impose on normal words the additional condition that for any linear α in X, if the set of values $\rho\alpha$ for ρ satisfying C is finite, then it consists of only a single integer.

Let $w(x)$ be fixed henceforth. A *reduction chain* for an expression ϕ is defined to be a sequence $(\omega_1, C_1), \cdots, (\omega_n, C_n)$, for some $n \geqq 1$, with the following properties:

(1) $\omega_1 = w(\phi)$; *and* C_1 *implies no nontrivial equation, that is, implies* $\rho\alpha = \rho\beta$ *only for* $\alpha = \beta$;

(2) (ω_n, C_n) *is normal; and, for each root* ξ *of* ϕ, (ξ, C_n) *is primitive*;

(3) *for each* i, $1 \leqq i < n$, (ω_i, C_i) *and* (ω_{i+1}, C_{i+1}) *are related in one of the following ways*:

(3a) $\omega_{i+1} = \omega_i$ *and* C_{i+1} *is equivalent to* C_i;

(3b) $C_{i+1} = C_i$ *and* ω_{i+1} *results from* ω_i *by replacing some occurrence of* α *by* β *where* C_i *contains* $\rho\alpha = \rho\beta$;

(3c) $C_{i+1} = C_i$ *and* ω_{i+1} *results from* ω_i *by an application of one of the* X*-group axioms, with the proviso that the axiom* $u^\alpha u^\beta = u^{\alpha+\beta}$ *is never used to introduce an exponent of higher degree than those already present*;

(3d) $\omega_{i+1} = \omega_i$ *and* C_{i+1} *is obtained by adjoining to* C_i *a condition* $\rho\alpha > 0$ *or* $\rho\alpha = 0$, *where* α *is a linear combination of the exponents of* ω_i.

We observe immediately that $V(w(\phi), C_n) = V(\omega_n, C_n)$.

LEMMA 1. *If* $(\omega_1, C_1), \cdots, (\omega_n, C_n)$ *is a reduction chain for* ϕ, *where all*

exponents of ϕ are linear, then there exists (ψ, D) such that $V(\phi, C_n) \subseteq V(\psi, D)$, that $(w(\psi), D)$ has a normal form (χ, D), and that D implies no nontrivial equation.

Proof. If C_n implies no nontrivial equation, we can take $\psi = \phi$ and $D = C_n$. This is the case, in particular, if the number d of parameters is 0. For an induction, we assume that $d > 0$, and that the lemma holds for all $d' < d$. In view of our opening remark, it suffices to treat the case that some C_k implies a nontrivial equation. Our main task is to show that the first such C_k then implies a linear equation.

We shall establish by induction that, for $1 \leqq i < k$, each (ω_i, C_i) has the following property:

(P) *if ξ is a root of ω_i, then $(\xi, C_i) \equiv (\eta^m, C_i)$, where m is an integer and η is a conjugate of some root ζ of ϕ; every exponent α of ω_i is linear; and C_i implies no nontrivial equation.*

Now (ω_1, C_1) has the property P. For the roots of $\omega_1 = w(\phi)$ are evidently powers of the roots of ϕ; every exponent of ω_1 is a linear combination of those of ϕ, which are linear by the hypothesis of the lemma; and C_1 implies no nontrivial equation because of condition (1) in the definition of a reduction chain.

Assume now that, for some i, (ω_i, C_i) has the property P, and examine the circumstances under which (ω_{i+1}, C_{i+1}) will have the same property. *Cases* 3a *and* 3b are immediate. *In Case* 3c, application of the axiom $u^1 = u$ or the axiom $u^\alpha u^\beta = u^{\alpha+\beta}$, subject to the stated proviso, introduces no new roots and no nonlinear exponents. Application of the axiom $u(vu)^\alpha = (uv)^\alpha u$ introduces no new exponents, and only roots that are conjugates of roots of ω_i. Application of the remaining axiom, $(u^\alpha)^\beta = u^{\alpha\beta}$, preserves P provided either α or β is a constant; we shall show that the case of α, β both nonconstant can not arise. Since $\alpha\beta$ is nonlinear, the hypothesis that (ω_i, C_i) satisfies P precludes that ω_i should have any part $\xi^{\alpha\beta}$. For the other possibility, suppose that ω_i contained a part $(\xi^\alpha)^\beta$ with β nonconstant. Then $(\xi^\alpha, C_i) \equiv (\eta^m, C_i)$ for some integer m and η conjugate to a root ζ of ϕ, and, for some conjugate θ of ξ we should have $(\theta^\alpha, C_i) \equiv (\zeta^m, C_i)$, whence, a fortiori, $(\theta^\alpha, C_n) \equiv (\zeta^m, C_n)$. By condition (2), (ζ, C_n) is primitive, whence it follows easily that α divides m, hence α is a constant.

Under Case 3d, as long as C_{i+1} implies no nontrivial equation, P is preserved. In particular, if C_k is the first that implies a nontrivial equation, then $(\omega_1, C_1), \cdots, (\omega_{k-1}, C_{k-1})$ all satisfy P, and (ω_k, C_k) must be obtained, under Case 3d, by adjoining to C_{k-1} a relation $\rho\alpha > 0$ or $\rho\alpha = 0$. Since all exponents of ω_i are linear, α must be linear. A new condition $\rho\alpha > 0$ can imply an equation only if C_{k-1} already implies a condition $\rho\alpha \leqq h$ for some integer h, so that C_k implies that $\rho\alpha$ be one of the integers $1, 2, \cdots, h$. In any case, C_k and therefore C_n implies that $\rho\alpha$ assume one of a finite set of values, and hence, in view of the additional condition that has been imposed on normal words,

C_n must imply that $\rho\alpha = h'$ for some integer h'. Restating this, we have that C_n implies some $\rho\alpha' = 0$ where α' is linear and nonconstant.

A nonsingular linear, possibly nonhomogeneous, transformation on the parameters $\nu_1, \cdots, \nu_d$ does not invalidate any of the foregoing considerations, and permits us to suppose that C_n implies the equation $\rho\nu_d = 0$. We now form ϕ' and a chain $(\omega_1', C_1'), \cdots, (\omega_n', C_n')$ by everywhere replacing ν_d by 0. Then all exponents of ϕ' are surely linear. To verify that the new chain is a reduction chain, conditions (1) and (3) are immediate, while (2) follows from the observation that C_n contained the condition $\rho\nu_d = 0$.

The inductively assumed case of the lemma for $d-1$ then gives us (ψ, D) such that $V(\phi', C_n') \subseteq V(\psi, D)$, that $(w(\psi), D)$ has a normal form (χ, D), and that D implies no nontrivial equation. Using again the fact that C_n implies $\rho\nu_d = 0$, we see that $V(\phi, C_n) = V(\phi', C_n')$, whence (ψ, D) satisfies the conclusion of the lemma.

LEMMA 2. *If, for all roots ξ of ϕ, the word $(\xi, 0)$ is primitive, and if all exponents of ϕ are linear, then there exist $\phi_1, \cdots, \phi_n$, for some $n \geqq 0$, such that*

$$U(w) \cap V(\phi, 0) \subseteq V(\phi_1, 0) \cup \cdots \cup V(\phi_n, 0) \subseteq U(w).$$

Proof. We shall use the following two basic properties of the reduction to normal form: if some (γ, C) has a normal form consisting of the words $(\gamma_1, C_1), \cdots, (\gamma_n, C_n)$, $n \geqq 0$, then

(i) a retraction ρ satisfies C if and only if ρ satisfies one of $C_1, \cdots, C_n$;

(ii) $V(\gamma, C) = V(\gamma_1, C_1) \cup \cdots \cup V(\gamma_n, C_n)$.

Let $(w(\phi), 0)$ have a normal form $(\sigma_1, S_1), \cdots, (\sigma_m, S_m)$. Write $I = \{1, 2, \cdots, m\}$. From (i) it follows that $V(\phi, 0) = V(\phi, S_1) \cup \cdots \cup V(\phi, S_m)$, whence

(iii) $U \cap V(\phi, 0) = \bigcup_{i \in I} [U \cap V(\phi, S_i)]$.

Let I_1 be the subset of I consisting of those i such that (ξ, S_i) is not primitive, for some root ξ of ϕ. Then $(\xi, S_i) \equiv (\eta^\beta, S_i)$ for some η with (η, S_i) primitive, and some $\beta \neq \pm 1$. Now ϕ contains a part ξ^α for some α, and, if we form ϕ_i' by replacing this part by η^ν, where ν is a new indeterminate, then ϕ_i' is, in an obvious sense, shorter than ϕ. Since the only root of ϕ_i' that is possibly not a root of ϕ is η, and (η, S_i) and therefore $(\eta, 0)$ is primitive, and the only exponent of ϕ_i' that is not an exponent of ϕ is ν, which is linear, ϕ_i' as well as ϕ satisfies the hypotheses of the lemma. By an induction on length, we may suppose that ϕ_i', shorter than ϕ, also satisfies the conclusion of the lemma. Thus there exist $\phi_{i1}, \cdots, \phi_{in_i}$, for some $n_i \geqq 0$, such that

$$U \cap V(\phi_i', 0) \subseteq \bigcup_{1 \leq j \leq n_i} V(\phi_{ij}, 0) \subseteq U.$$

Clearly $V(\phi, S_i) \subseteq V(\phi_i', S_i) \subseteq V(\phi_i', 0)$, whence it follows that

$$\text{(iv)} \qquad \bigcup_{i \in I_1} [U \cap V(\phi, S_i)] \subseteq \bigcup_{i \in I_1} \bigcup_{1 \leq j \leq n_i} V(\phi_{ij}, 0) \subseteq U.$$

Next, let i belong to $I-I_1$, that is, suppose that, for each root ξ of ϕ, the word (ξ, S_i) is primitive.

We assert that the process of reduction to normal form, as set forth in [2], when applied to $(w(\phi), 0)$, yields a reduction chain for ϕ with last term $(\omega_n, C_n)=(\omega_i, S_i)$. Condition (1) is trivial, since $C_1=0$, and condition (2) holds by hypothesis. All the parts of condition (3) are contained in the definition of the reduction process, excepting the proviso attached to the use of the axiom $u^\alpha u^\beta = u^{\alpha+\beta}$, and the condition under (3d) that α be a linear combination of the exponents of ω_j. But it can be seen by inspection that the algorithm given in [2] for reduction to normal form in fact conforms to these additional requirements. Therefore Lemma 1 provides us with a word (ψ_i, T_i) such that $V(\phi, S_i)\subseteq V(\psi_i, T_i)$, that $(w(\psi_i), T_i)$ has a normal form (χ_i, T_i), and that T_i implies no nontrivial equation.

Define I_2 to be the subset of $I-I_1$ consisting of all i for which $\chi_i\neq 1$. By (ii), since $(w(\psi_i), T_i)$ has normal form consisting of (χ_i, T_i) alone, $V(w(\psi_i), T_i) = V(\chi_i, T_i)$. By a property of normal words stated earlier, $\chi_i\neq 1$ implies that 1 does not belong to $V(\chi_i, T_i)$, and therefore not to $V(w(\psi_i), T_i)$. This means that, for all ρ satisfying T_i, $w(\rho\psi_i)=\rho w(\psi_i)\neq 1$, or, in other words, $U\cap V(\psi_i, T_i)=0$. Since $V(\phi, S_i)\subseteq V(\psi_i, T_i)$, this implies that

$$\text{(v)} \qquad \bigcup_{i\in I_2} [U\cap V(\phi, S_i)] = 0.$$

Finally, for i in the remaining set $I_3=I-I_1-I_2$, $\chi_i=1$. It follows that $(w(\psi_i), T_i)\equiv(1, T_i)$, that is, that $w(\psi_i)$ reduces to 1 by use only of the axioms for X-groups, together with equations $\alpha=\beta$ where T_i contains the equation $\rho\alpha=\rho\beta$. Since T_i contains no nontrivial equations, this means that $w(\psi_i)$ reduces to 1 by use of the axioms alone, which implies that $w(\rho\psi_i)=\rho w(\psi_i)=1$ for all ρ, that is, that $V(\psi_i, 0)\subseteq U$. Since $V(\phi, S_i)\subseteq V(\psi_i, T_i)\subseteq V(\psi_i, 0)$, it follows that

$$\text{(vi)} \qquad \bigcup_{i\in I_3} [U\cap V(\phi, S_i)] \subseteq \bigcup_{i\in I_3} V(\psi_i, 0) \subseteq U.$$

The conclusion of the lemma now follows by splitting the union over I in the right member of (iii) into unions over I_1, I_2, I_3, and then applying (iv), (v), and (vi).

LEMMA 3. *For all ϕ, there exist $\phi_1, \cdots, \phi_n$, for some $n\geqq 0$, such that*

$$U(w)\cap V(\phi, 0)\subseteq V(\phi_1, 0)\cup\cdots\cup V(\phi_n, 0)\subseteq U(w).$$

Proof. Let $(\phi, 0)$ have a normal form $(\phi_1, C_1), \cdots, (\phi_m, C_m)$. From (ii) it follows that

$$\text{(vii)} \qquad V(\phi, 0) = \bigcup_{1\leqq i\leqq m} V(\phi_i, C_i) \subseteq \bigcup_{1\leqq i\leqq m} V(\phi_i, 0).$$

Since each (ϕ_i, C_i) is normal, for each root ξ of ϕ_i, the word (ξ, C_i) is primitive, and, a fortiori, $(\xi, 0)$ is primitive. Form ϕ_i' from ϕ_i by replacing all exponents of ϕ_i by distinct indeterminates. The roots of ϕ_i' are the same as those of ϕ_i, with $(\xi, 0)$ primitive; and, by construction, the exponents of ϕ_i' are linear. Therefore Lemma 2 applies to ϕ_i' to yield $\phi_{i1}, \cdots, \phi_{in_i}$, for some $n_i \geqq 0$, such that

$$U \cap V(\phi_i', 0) \subseteq \bigcup_{1 \leqq j \leqq n_i} V(\phi_{ij}, 0) \subseteq U.$$

Since clearly $V(\phi_i, 0) \subseteq V(\phi_i', 0)$, this gives

$$U \cap V(\phi_i, 0) \subseteq \bigcup_{1 \leqq j \leqq n_i} V(\phi_{ij}, 0) \subseteq U.$$

Taking the union over all i, $1 \leqq i \leqq m$, and using (vii), we obtain

$$U \cap V(\phi, 0) \subseteq \bigcup_{1 \leqq i \leqq m} [U \cap V(\phi_i, 0)] \subseteq \bigcup_{1 \leqq i \leqq m} \bigcup_{1 \leqq j \leqq n_i} V(\phi_{ij}, 0) \subseteq U,$$

which completes the proof of the lemma.

It was noted at the beginning of this section that this lemma, together with Proposition 6, suffice to establish our main result.

THEOREM. *There exists an effective procedure that associates with each element $w(x) \neq 1$ in the free group on generators $x, a_1, \cdots, a_r$, a finite set of parametric expressions in the generators $a_1, \cdots, a_r$, with the property that the set of elements u in the free group on generators $a_1, \cdots, a_r$ that satisfy $w(u) = 1$ is exactly the set of elements represented by one of the parametric words under some substitution of integer values for the parameters.*

BIBLIOGRAPHY

1. A. G. Kurosh, *The theory of groups*, New York, Chelsea, 1956.

2. R. C. Lyndon, *Groups with parametric exponents*, Trans. Amer. Math. Soc. vol. 96 (1960) pp. 445–457.

3. J. Nielsen, *Über die Isomorphismen unendlicher Gruppen ohne Relation*, Math. Ann. vol. 79 (1918) p. 269.

4. ———, *A basis for subgroups of free groups*, Math. Scand. vol. 3 (1955) p. 31.

UNIVERSITY OF MICHIGAN,
ANN ARBOR, MICHIGAN
INSTITUTE FOR DEFENSE ANALYSES,
PRINCETON, NEW JERSEY