ON TWO VARIABLE EQUATIONS IN FREE GROUPS

K. I. APPEL¹

1. Introduction. In [3], Lyndon defined parametric words in groups as group theoretic expressions in the generators $a_1, \dots, a_r$ that contain certain integer valued parameters $\nu_1, \dots, \nu_d$ as exponents. The main theorem of his paper was that with any nontrivial equation in one variable in a free group can be associated a finite collection of parametric words such that any substitution of integers for parameters yields a solution, and all solutions are thus obtainable. (This result was refined in [1] to show that each parametric word need have only one parameter occurrence.)

The main result of this paper is to show that no comparable statement can be made for equations in two variables. In particular, it will be shown that even with a somewhat more general type of parametric word the equation

$$(1) \quad axbaya^{-1}x^{-1}b^{-1}a^{-1}y^{-1} = 1$$

has a collection² of solutions which cannot be described by any finite number of generalized parametric words.

2. Notation, definitions and primitivity lemmas. Let G be the free group on free generators $a, b, d, d_2, d_3, \dots$. Let $w(x, y)$ be any freely reduced word in $G^*\{x, y\}$. We say that $(U(a, b, d, \dots), V(a, b, d, \dots))$ is a solution of $w=1$ if $w(U, V)$ is the identity of G . Let a generalized parametric word over G be a group theoretic expression in the generators of G and variables $v_1, v_2, \dots$ that contains certain integer valued parameters $\nu_1, \nu_2, \dots$ as exponents. A pair (U, V) of such parametric words is called a solution pair for the equation $w(x, y)=1$ in G if every substitution of words in the generators of G for variables and integers for parameters occurring in (U, V) yields a solution of $w=1$. The need for the generalization arises from the fact that while Lyndon was able to simply exclude the trivial equation (which in our notation has the solution v_1 in one variable equations), the two variable analogue of this seems impossible. For exam-

Received by the editors May 9, 1968.

¹ This work has been supported by National Science Foundation Contract NSF GP 7421 while the author was at University of Bristol.

² The solutions described will not be all the solutions of (1). A larger collection (and possibly all) of the solutions can be described as the set of all paths beginning at a particular distinguished vertex of a directed graph with 112 vertices and over 500 edges. This collection employs only 12 of the vertices and 15 edges of the graph.

ple, among the solutions of the equation $b^{-1}x^{-1}ybx y^{-1}=1$ are the parametric set $(b^\lambda, b^\star)$ as well as the set (b^{-1}, v_1) , (i.e. if b^{-1} is substituted for x the resulting equation in y is trivial).

The following question, if it had an affirmative answer, would provide a natural analogue to Lyndon's result. The fact that the answer is negative seems to imply that no such analogue is possible.

Question. Can each equation in two variables in the free group G be associated with a finite set of solution pairs of generalized parametric words such that each solution of the equation is an instance of one of the solution pairs (i.e. results by substitution for variables and parameters)?

A very useful tool employed in the argument is the concept of primitivity of words in a free group (or semigroup) as employed by Lyndon and Schützenberger in [5]. A word w on the generators of G is called primitive if it is cyclically reduced and is not a proper power (i.e., w is not a formal m -fold repetition of one of its subwords for $m > 1$). We use $|w|$ to denote the length of w as a freely reduced word on the generators of G . We write $uv = u \cdot v$ if uv is freely reduced, that is, if the final letter of u is not the inverse of the initial letter of v . The following lemma states some results of Lyndon and Schützenberger [5].

LEMMA 1(a). *If a and b are cyclically reduced and have powers a^p and b^q with a common segment of length $|a| + |b|$ then each is a power of a primitive element of length at most g.c.d. $(|a|, |b|)$.*

(b) *If $ab = ba$ in G then a and b are powers of a common element, hence if c is primitive it is not nontrivially of the form $c = a \cdot b$ where $ab = ba$.*

A second technical lemma is

LEMMA 2(a). *Let p be primitive, $|p| > |q| > 0$ and $j > 4$. If $p^{j+1}q$ is cyclically reduced, then it is primitive.* (b) *Any cyclic permutation of a primitive word is primitive.*

PROOF. 2(b) is immediate so we shall only prove 2(a). Suppose 2(a) is false. Let r be primitive with $p^{j+1}q = r^k$, $k > 1$. We may write $p^{j+1}q = p^j \cdot (pq)$ since p is primitive and hence cyclically reduced and q is shorter than p . Suppose $|r| \leq |p|$. Then $p = r^h \cdot r_1$ where $r_1 \cdot r_2 = r$. But since $j > 4$ we must also have $p = r_2 \cdot r^h \cdot r_3$ where $r_3 \cdot r_4 = r$. But by Lemma 1(b) this implies that r_1 or r_2 is 1 and $p = r^h$, whence $h = 1$ and $p = r$. This means q is a power of r , contradiction. If $|r| > |p|$ we can similarly use Lemma 1(b) to show that p is not primitive.

3. **Proof of the main result.** We shall, for each integer $m \geq 1$ define a $3m$ parameter, variable free solution pair for equation (1). Let

$$(2) \quad \begin{aligned} C_1 &= b^{-1}, & B_1 &= b^{-1} C_1^{-(\gamma_1+1)} a^{-2}, \\ A_{n+1} &= b a^{-2} B_{n+1}^{-(\beta_{n+1}+1)} b^{-1} C_{n+1}^{-1} a^2 & \text{for } 0 \leq n < m, \\ C_{n+1} &= a^2 A_n^{(\alpha_n-1)} b a^{-2} B_n^{-1} b^{-1} & \text{for } 1 \leq n < m, \\ B_{n+1} &= b^{-1} C_{n+1}^{(\gamma_{n+1}+1)} a^2 A_n^{-1} b a^{-2} \end{aligned}$$

and

$$U_m = b^{-1} A_m^{\alpha_m} b a^{-2} B_m^{-1} b^{-1}, \quad V_m = a b^{-1} A_m a^{-1}.$$

To check that (U_m, V_m) are solution pairs one need only note that upon substitution of U_m for x and V_m for y in (1) we obtain

$$(i)_m: b a^{-2} B_m^{-1} a^2 b^{-1} A_m a^{-2} b B_m a^2 b^{-1} A_m^{-1} = 1.$$

Now substitution for A_m yields

$$(ii)_m: B_m^{-1} b^{-1} C_m^{-1} b B_m a^2 b^{-1} a^{-2} C_m b = 1.$$

Next, substitution for B_m yields

$$(iii)_m: a^2 b^{-1} A_{m-1} a^{-2} C_{m-1}^{-1} a^2 A_{m-1}^{-1} a^{-2} C_m b = 1.$$

Now substitution for C_m in $(iii)_m$ yields $(i)_{m-1}$, so we need only verify that the words resulting from substitution for A_1, B_1 , and C_1 is the identity. This is quite simple and hence all instances of the parametric words are solutions.

First, we will show that no generalized parametric solution pair for (1) contains nontrivial variables. Suppose that (U, V) is such a pair at least one of which contains a nontrivial variable occurrence. Without loss of generality we may assume that the variables $v_1, v_2, \dots, v_n$ occur nontrivially in (U, V) . Set $v_1 = d, v_2 = d_2, \dots, v_n = d_n$ to obtain a parametric solution $(\bar{U}, \bar{V})$ without variables. Since v_1 occurs nontrivially, some instance $(\bar{U}, \bar{V})$ of (U, V) must, when freely reduced, contain occurrences of d . Write $\bar{U} = W_1 d^{e_1} W_2 \dots W_n d^{e_n} W_{n+1}$, $\bar{V} = T_1 d^{f_1} T_2 \dots T_m d^{f_m} T_{m+1}$ where all W_i, T_i are d -free and e_i, f_i are ± 1 and $\bar{U}$ and $\bar{V}$ are freely reduced. Then (1) becomes

$$(3) \quad \begin{aligned} a W_1 d^{e_1} \dots d^{e_n} W_{n+1} b a T_1 d^{f_1} \dots d^{f_m} T_{m+1} a^{-1} W_{n+1}^{-1} d^{-e_n} \dots \\ \cdot d^{-e_1} W_1^{-1} b^{-1} a^{-1} T_{m+1}^{-1} d^{-f_m} \dots d^{-f_1} T_1^{-1} = 1. \end{aligned}$$

Now if $W_{n+1} b a T_1 = T_{m+1} a^{-1} W_{n+1}^{-1} = W_1^{-1} b^{-1} a^{-1} T_{m+1}^{-1} = T_1^{-1} a W_1 = 1$, then

$$\begin{aligned} (W_{n+1} b a T_1) (T_1^{-1} a W_1) (W_1^{-1} b^{-1} a^{-1} T_{m+1}^{-1}) (T_{m+1} a^{-1} W_{n+1}^{-1}) \\ = W_{n+1} b a^2 b^{-1} a^{-2} W_{n+1}^{-1} = 1, \end{aligned}$$

whence $ba^2b^{-1}a^{-2}=1$ contradicting the fact that b and a are free generators of G .

Suppose $W_{n+1}baT_1 \neq 1$. From (3) we obtain

$$(4) \quad \begin{aligned} aW_1d^{e_1} \cdots d^{e_n}W_{n+1}baT_1d^{f_1} \cdots d^{f_m}T_{m+1} \\ = T_1d^{f_1} \cdots d^{f_m}T_{m+1}abW_1d^{e_1} \cdots d^{e_n}W_{n+1}a. \end{aligned}$$

Our supposition implies that the free reduction of the left side cannot delete any d occurrence, hence no d occurrences may be lost on the right. By equating corresponding segments we obtain

$$(5) \quad T_1^{-1}aW_1 = 1 \quad \text{and} \quad W_{n+1}aT_{m+1}^{-1} = 1.$$

By symmetry we may assume $n \geq m$. If $n > m$ we obtain $W_{m+1} = T_{m+1}abW_1$ and $W_{n-m+1} = W_{n+1}baT_1$. But for $1 < i \leq m$, $W_i = T_i$; for $0 \leq i < m-1$, $W_{n-i} = T_{m-i}$; and for $1 < i \leq n-m$, $W_i = W_{i+m}$. Hence we have $W_i = W_{km+j(n-m)+i}$ whenever the two subscripts lie between 1 and $n+1$. Thus $W_{m+1} = W_{n-m+1}$ and

$$(6) \quad T_{m+1}^{-1}W_{n+1}baT_1W_1^{-1}b^{-1}a^{-1} = 1.$$

If $n = m$ we obtain (6) directly. But using (5) to substitute in (6) we again obtain $a^{-2}b^{-1}a^2b = 1$. The assumption $T_1^{-1}aW_1 \neq 1$ leads to a similar contradiction, so variables are eliminated.

Now it will be shown that no finite number of variable free parametric solution pairs can have as instances all solutions of (1). First we will show that if an integer k greater than 6 is chosen for $\alpha_i, \beta_i, \gamma_i$, $1 \leq i \leq m$ then the free reductions of A_i, B_i and C_i are all primitive. We claim that each A_i , when freely reduced is a word containing occurrences of only a and b^{-1} and ending in a^2 . Similarly, each B_i contains only a^{-1} and b and begins with b and ends with ba^{-2} and each C_i is a word in a and b^{-1} and ends with b^{-1} . This is certainly enough to show cyclic reduction. The proof is by induction. For $i=1$, $C_1 = b^{-1}$, $B_1 = b^ka^{-2}$ and $A_1 = b^{1-k}(a^2b^{-k})^ka^2$. For the inductive step we note that the equations (2) can be written

$$(7) \quad \begin{aligned} C_2 &= a^2 A_1^{(\alpha_1-2)} [ba^{-2} B_1^{-\beta_1}] a^2 C_1^{\gamma_1} a^2 [ba^{-2} B_1^{-1}] b^{-1} \\ C_{i+1} &= a^2 A_i^{\alpha_i-2} [ba^{-2} B_i^{-\beta_i}] a^2 b^{-1} [A_{i-1} a^{-2}] C_i^{\gamma_i} a^2 [ba^{-2} B_i^{-1}] b^{-1} \end{aligned}$$

for $i \geq 2$, and for $i \geq 1$,

$$\begin{aligned} B_{i+1} &= [B_i a^2 b^{-1}] A_i^{1-\alpha_i} a^{-2} C_{i+1}^{-(\gamma_{i+1}-1)} b [B_i a^2 b^{-1}] A_i^{-\alpha_i} b a^{-2} \\ A_{i+1} &= [A_i a^{-2}] [C_{i+1}^{(\gamma_{i+1}+1)} b] B_{i+1}^{-(\beta_{i+1}-1)} a^2 b^{-1} [A_i a^{-2}] C_{i+1}^{\gamma_{i+1}} a^2. \end{aligned}$$

Now note that (by induction) each factor of the right hand sides

of equations (7) is of the proper type where by factor we mean either the free reduction of a bracketed expression or a segment not contained in brackets. Hence the cyclic reduction is proved. It is immediate from inspection of (2) that with $\alpha_i = \beta_i = \gamma_i = k \geq 6$ in each of the definitions of A_i , B_i and C_i , $i > 1$, that the term with parametric exponent is longer than the remainder of the word (e.g. in the definition of A_i , B_i is longer than $|ba^{-2}b^{-1}C_i^{-1}a^2|$). But A_1 , B_1 and C_1 are clearly primitive, so Lemma 2 may be applied to show that all are primitive.

Let W be a parametric word written so that all nonparametric exponents are ± 1 . The number of generator occurrences in W in this form is called the width of W . The number of occurrences of parameters is called its height. Call a (nonparametric) word P a (q, r) nest if: (i) P contains a proper primitive subword, P_1 , of length greater than q and (ii) For $1 \leq i < r-1$, P contains a primitive proper subword P_{i+1} which has P_i^q as a proper subword.

LEMMA 3. For $q > 6w$ and $r > h$ no (q, r) nest can be an instance of a parametric word of width less than w and height less than h .

PROOF. By induction on h . For $h=0$ it is immediate by definition of height. For reductio ad absurdum assume that the conclusion is false for h and let P be a nest and E a corresponding parametric word which serves as a minimal counterexample. Let $E = c_1 E_1^{\alpha_1} c_2 E_2^{\alpha_2} \cdots c_f E_f^{\alpha_f} c_{f+1}$ where the c_i are parameter free and the E_i are parametric words. [Note that $\text{width}(E) = \sum (|c_i| + \text{width}(E_i))$.] Now let integers be substituted for the parameters of E to obtain P , i.e. $P = c_1 \bar{E}_1^{\alpha_1} \cdots c_f \bar{E}_f^{\alpha_f} c_{f+1}$. Now $P = S \cdot P_r^q \cdot T$ with P_r a primitive $(q, r-1)$ nest. Let $\bar{E}_j$ be such that P_r^q contains a longer power of $\bar{E}_j$ than of any other $\bar{E}_i$. Let $\bar{E}_j^s$ be the power. Now $E_j = QR^m Q^{-1}$ with R primitive and hence $\bar{E}_j^s = QR^{ms} Q^{-1}$. If Q is longer than P_r , then P_r would be a cyclic permutation of its own inverse which is impossible. Hence $|R^{ms}| > |\bar{E}_j^s| - 2|P_r|$. But $|\bar{E}_j^s| > (1/w)|P_r^q|$ by definition of width. Hence $|R^{ms}| > 4|P_r|$. If $|R| < |P_r|$ the primitivity of P_r is contradicted by Lemma 1(a). Hence $|R| > |P_r|$ and $E_j = M \cdot P_r \cdot N$ for some M, N . But E_j has width less than w and height at most $h-1$ and P_r is a $(q, r-1)$ nest so the lemma is proved.

Suppose that $(U_1, V_1), \dots, (U_d, V_d)$ were a set of parametric solution pairs for (1). Let w be the maximum of the widths of the V_i and h be the maximum of their heights. Let m be such that $3m > h$ and choose all parameters $= q = 6hw$. Then by Lemma 3 the $\bar{V}$ thus obtained cannot be an instance of the set of pairs and the result is proved.

REFERENCES

1. K. I. Appel, *One variable equations in free groups*, Proc. Amer. Math. Soc. **19** (1968), 912-918.
2. A. A. Lorenc, *The solution of systems of equations in one unknown in free groups*, Dokl. Akad. Nauk SSSR **148** (1963), 1253-56 = Soviet Math. Dokl. **4** (1963), 262-266.
3. R. C. Lyndon, *Equations in free groups*, Trans. Amer. Math. Soc. **96** (1960), 445-457.
4. ———, *Groups with parametric exponents*, Trans. Amer. Math. Soc. **96** (1960), 518-533.
5. R. C. Lyndon and M. P. Schützenberger, *The equation $a^M = b^N c^P$ in a free group*, Michigan Math. J. **9** (1962), 289-298.

UNIVERSITY OF ILLINOIS