ON THE EQUATION $z_1^n z_2^n \cdots z_k^n = y^n$ IN A FREE SEMIGROUP

BY

K. I. APPEL AND F. M. DJORUP(1)

1. **Introduction.** Stallings [6] generalized a result of Lyndon [3] by showing that if elements $x_1, x_2, \ldots, x_m$ of a free group F satisfy a relation $x_1^n x_2^n \cdots x_m^n = 1$ where $n \geqq 2$, then they generate a free subgroup F_0 of rank $\leqq m/2$. This bound is best possible: if $m=2k$ taking $x_{2i} = x_{2i-1}^{-1}$ for $1 \leqq i \leqq k$ gives a solution in the free group generated by $x_1, x_3, \ldots, x_{2k-1}$.

Stallings' Theorem implies a corresponding result for free semigroups. If $x_1, x_2, \ldots, x_m$ are elements of a free semigroup F that satisfy a relation $x_1^n x_2^n \cdots x_m^n = x_{m+1}^n$ where $n \geqq 2$ then $x_1, x_2, \ldots, x_m$ are contained in a free subsemigroup F_0 of rank $r \leqq (m+1)/2$. However, one may ask whether, in free semigroups, this bound remains the best possible. The principal result in this paper shows that this is so only for $n=2$. We make the following conjecture:

CONJECTURE. If $a_1, a_2, \ldots, a_k$ and b are elements of a free semigroup F such that $a_1^n a_2^n \cdots a_k^n = b^n$, where $n \geqq 1$, then they are contained in a free subsemigroup F_0 of rank $r \leqq (k+n-1)/n$.

This is trivial for $n=1$ and follows from Stallings' result for $n=2$. We establish it for $k \leqq n$ and also for $n \geqq 6$ and $k \leqq 2n-2$. We note that the conjectured bound cannot be lowered for general n and k. If n and q are given, let $k=nq+1$, and hence $[(k+n-1)/n]=q+1$. In the free semigroup F of rank $q+1$ on generators $x, y_1, y_2, \ldots, y_q$, the elements $a_1, a_2, \ldots, a_k$, and b appearing in the relation

$$x^n(y_1x^{n-1})^n(y_2x^{n-1})^n \cdots (y_qx^{n-1})^n(xy_1x^{n-2})^n \cdots (xy_qx^{n-2})^n \cdots (x^{n-1}y_1)^n \cdots (x^{n-1}y_q)^n = (x^n(y_1x^{n-1})^n \cdots (y_{q-1}x^{n-1})^n y_q)^n$$

are not contained in any proper free subsemigroup.

In the two sections which follow we prove the following two theorems.

THEOREM 1. *If $a_1^n \cdots a_k^n = b^n$ in a free semigroup F and $k \leqq n$, then $a_1, \ldots, a_k$ and b lie in a free semigroup of rank* 1.

THEOREM 2. *If $a_1^n \cdots a_k^n = b^n$ in a free semigroup F with $k \leqq n$ or $n \geqq 6$ and $k \leqq 2n-2$ then $a_1, \ldots, a_k$ and b are contained in a free semigroup of rank $[(k+n-1)/n]$.*

Received by the editors August 16, 1966 and, in revised form, July 24, 1967.

(1) The authors would like to thank Professor R. C. Lyndon for reading a first draft of this paper and making many suggestions to improve the exposition. They would also like to thank Professor Richard Brown for his aid in employing the CSX-1 computer at the University of Illinois in a search for potential counterexamples which led to the discovery of several techniques of proof.

The arguments are organized as follows. In §2, after stating a lemma of Lyndon and Schützenberger, we define a canonical solution of $z_1^n z_2^n \cdots z_k^n = y^n$ and note that we may proceed in terms of canonical solutions. Next, we define an inductive condition in terms of which most of our later results are phrased. Roughly, the proofs of Theorems 1 and 2 consist in showing that under the hypotheses of these theorems the inductive condition is satisfied. The section concludes with two lemmas giving hypotheses under which the inductive condition is satisfied and a proof of Theorem 1. §3 consists of four further lemmas giving hypotheses under which the inductive condition is satisfied. Theorem 2 is an immediate consequence of Theorem 1 plus the last two of these lemmas.

2. Our arguments use a lemma of Lyndon and Schützenberger [4].

LEMMA 1. *Let F be a free semigroup.*

(a) *If $ab=bc \in F$, $a \neq 1$, then $a=uv$, $b=(uv)^k u$, $c=vu$ for some $u, v \in F$.*

(b) *If $ab=ba \in F$ then a and b are powers of a common element.*

(c) *If a and b have powers a^p and b^q with common segment of length $|a|+|b|$ (where $|a|$ denotes the length of a as a word on the generators of F), then a and b both admit periods of length the greatest common divisor of $|a|$ and $|b|$. If the segment is initial to both a^p and b^q then a and b are powers of common element.*

We now proceed with a sequence of definitions. Let n be fixed. The rank of a solution $S=\langle a_1, a_2, \ldots, a_k; b\rangle$ of $z_1^n z_2^n \cdots z_k^n = y^n$ is the minimum rank of a free subsemigroup F_0 containing $a_1, a_2, \ldots, a_n$ and b. The element b^n of F is given by a word $w=x_1 x_2 \cdots x_t$ in the $x_i \in X$, the basis of F, where $t=\sum n|a_i|$. The fact that $b^n=w$ admits a period of length n imposes certain identifications on the x_i. Let I be the set of indices $1, 2, \ldots, t$. Let $i \approx j$ be the smallest equivalence relation on the index set such that

(i) $i \approx j$ if $i \equiv j$ modulo $|b|$,

(ii) $i \approx j$ if $|a_1^n \cdots a_{l-1}^n| < i, j \leqq |a_1^n \cdots a_l^n|$ for some l and $i \equiv j$ modulo $|a_l|$.

We say that the type of S is the k-tuple $\langle |a_1|, |a_2|, \ldots, |a_k|\rangle$. For any solution with the same type as S, whenever $i \approx j$ we must have $x_i = x_j$. A canonical solution $\tilde{S}$ is obtained by choosing $x_i = x_j$ if and only if $i \approx j$. Then the general solution S is obtained from canonical $\tilde{S}$ by an endomorphism of F identifying certain generators, whence it follows (since a subsemigroup of free F generated by r elements is always contained in a free subsemigroup of rank $\leqq r$) that $r(\tilde{S}) \geqq r(S)$. Hence it will suffice to establish our bound on the ranks of canonical solutions.

Let S be a canonical solution. Let L be the set of left letters, that is, those beginning with some a_j and R the set of right letters, ending some a_j. Define H to be the set of subwords of w beginning with a letter from L and ending with a letter from R, and containing no other letters from either L or R.

LEMMA 2. *If S is canonical then H is a basis for a free subsemigroup F_0 of F containing $a_1, a_2, \ldots, a_k$ and b and these elements are contained in no free subsemigroup of smaller rank.*

If we construct the relation $i \approx j$ by first imposing condition (ii) and then (i), we note that it is the case that if x_i is followed by x_{i+1} in some h_k and $x_i = x_j$ where x_j appears in some h_k then $x_{i+1} = x_{j+1}$. This may be seen by a routine induction. Similarly if $x_{i+1} = x_{j+1}$ and x_i is followed by x_{i+1} in some h_k, $x_i = x_j$. By iteration, it follows that if h_j and h_k have any letter in common then $h_j = h_k$. Thus the set H of segments h_j is a basis for a free subsemigroup F_0 of F containing $a_1, \ldots, a_k$, and b, and has equal cardinal with each of L and R.

To prove that F_0 has minimal rank, suppose $a_1, \ldots, a_k$ and b contained in some F_0' free on basis Z. Since each x_i in L begins some a_j, each x_i in L must begin some $z \in Z$. Therefore Z must have at least as many elements as L. But this is precisely the number of elements of H.

In the lemmas which follow, we will show that under certain hypotheses on S if all solutions S' with smaller k' and all those with equal k' and smaller $|b'|$ satisfy the conclusion of our conjecture then so does S. We will abbreviate this by writing "S satisfies the inductive condition."

Henceforth, we suppose n fixed, $n \geqq 3$. We first argue by induction on k, and, second, for fixed k we argue by induction on $|b|$. An element c of F is primitive if it is not a proper power $c = d^m$, $m > 1$. Every element $a \neq 1$ of F is uniquely a power of a primitive element $a = c^m$, $m \geqq 1$. We adopt the notation $a_i = c_i^{m_i}$ and $b = d^m$, c_i and d primitive. Then we have $c_1^{m_1 n} \cdots c_k^{m_k n} = d^{mn}$. Suppose $|c_1| + |d| \leqq |a_1^n|$. Then $a_1^n = c_1^{m_1 n}$ and $b^n = d^{mn}$ have a common initial segment of length at least $|c_1| + |d|$, so by Lemma 1, c_1 and d are powers of a common element, and since both are primitive $c_1 = d$. Therefore, we may cancel a_1^n from both sides of the equation and obtain

$$a_2^n \cdots a_k^n = (d^{m - m_1})^n.$$

It is easy to see that the rank of the solution of the original equation is no greater than that for this equation, whence S satisfies the inductive condition.

If some $|c_i| + |d| \leqq |a_i|^n$ for $i \neq 1$ we pass to the equation $a_i^n \cdots a_k^n a_1^n \cdots a_{i-1}^n = (b')^n$ where b' is a conjugate of b (we will write $b' \sim b$); that is, for some u, v, $b = uv$, $b' = vu$. This equation has the same H as the original, hence the same rank, and the argument for the case $i = 1$ applies.

Henceforth, we may assume, inductively, that the result has been shown for all solutions S' with $k' < k$ and those with $k' = k$ and $|b'| < |b|$. Furthermore, we may assume, by the above primitivity argument, that for all i, $m_i n |c_i| = |a_i^n| < |c_i| + |d|$, whence $(m_i n_i - 1)|c_i| < |d|$, $(n-1)|a_i| < |b|$, and by a simple counting argument $k \geqq n$. Similar considerations permit us to assume that $c_i \neq c_{i+1}$ (subscripts modulo k).

The word $w = b^n$ is invariant under a shift by b places $x_i \to x_{i+|b|}$. If under some iteration of this shift the translate of a_i^n can be brought to overlap a_j^n by as much as $|c_i| + |c_j|$, then it follows from Lemma 1 that $c_i \sim c_j$. This must happen if $|a_i^n|$ and $|a_j^n|$ are large enough, and under these circumstances we find that $m_i = m_j$ whence $a_i \sim a_j$.

LEMMA 3. (i) *If* $|b| \leqq |a_i^n|$ *then* $m=1$ *and* nm_i *is the least integer greater than or equal to* $|b|/|c_i|$.

(ii) *If* $|b| \leqq |a_i^n|$ *and* $|b| \leqq |a_j^n|$ *then* $a_i \sim a_j$.

Proof. (i) If $|b| \leqq |a_i^n|$, $(nm_i-1)|c_i| < d$ and $b=m|d| \leqq nm_i|c_i|$ then $m(nm_i-1) < nm_i$ and $m=1$. Now

(ii) Let $|b| < |a_i^n|$, $|b| < |a_j^n|$. We may suppose that $i \neq j$ and $|c_i| \leqq |c_j|$.

Let $(0, 1, \ldots, t-1)$ be the integers modulo t, in their natural cyclical order. For h and k from this set, we denote by $[h, k]$ the interval $(h, h+1, \ldots, k)$, and we write $[h, k]+f=[h+f, k+f]$. Each interval $I=[h, k]$ determines a word $W(I) = x_h x_{h+1} \cdots x_k$. From the fact that $w=b^n$ it follows that w has period $|b|$, that is, for every interval I we have $W(I+|b|)=W(I)$. We define $I_j=[n|a_{j-1}|+1, n|a_j|]$, $[h, l]+f=[h+f, l+f]$ (mod t) and $W[h, l]=x_h \cdots x_l$. From $w=b^n$ we have $W([h, l]+f|b|)=W[h, l]$, whence $W(I_k)=a_k^n$.

If any translate $P=I_i+f|b|$ meets I_j in an interval $P \cap I_j$ of length at least $|c_i|+|c_j|$, by Lemma 1 we have $c_i \sim c_j$ and since $m_i=m_j$ by (i) $a_i \sim a_j$. In particular, if any translate $P=I_i+f|b|$ is contained entirely in I_j, then the conclusion follows, since $|P|=|a_i^n| > |b| > (m_j n-1)|c_j| \geqq 2|c_j| \geqq |c_i|+|c_j|$. Otherwise, choose a translate P_0 to contain a maximal initial segment $Q_0=P_0 \cap I_j$ of I_j. Since $|b| \leqq |P|$, $P_1 = P_0+|b|$ begins at the latest with the first number following P_0, and, since $P_1 \nsubseteq I_j$, it ends after the end of I_j. Thus $Q_1=P_1 \cap I_j$ is a terminal segment of I_j and $I_j = Q_0 \cup Q_1$. Let $Q_0'=Q_0+|c_j|$. Then $|Q_0' \cap Q_1| \geqq |c_j| \geqq |c_i|$ and $W(Q_0')=W(Q_0)$ since they are both contained in $W(I_j)$ and are translated by $|c_j|$; and $W(Q_1)$ and $W(Q_0)$ as parts of translates of a_i^n admit period $|c_i|$ it follows that $Q_0' \cup Q_1$ admits period $|c_i|$ and, as a subinterval of I_j admits period $|c_j|$. But $|Q_0 \cup Q_1| \geqq |I_j|-|c_j| \geqq 2|c_j| \geqq |c_i|+|c_j|$. By Lemma 1, $c_i \sim c_j$ and $a_i \sim a_j$ as above.

LEMMA 4. *If* $|b| \leqq |a_i^n|$ *for* $1 \leqq i \leqq n-1$ *then S satisfies the inductive condition.*

Proof. By Lemma 3, $|a_1|=|a_2|=\cdots|a_{n-1}|$. If $|b|=|a_1^n|$, then $a_1=a_2$, a case already considered. Assume that $|b| < |a_1^n|$, hence that $a_1^n=bu$ with $u \neq 1$. On each of the segments $P_1=I_1, P_2=I_2-|b|, \ldots, P_{n-1}=I_{n-1}-(n-2)|b|$, W has period $|c_1|$. For $1 \leqq i < n-1$, P_i and P_{i+1} overlap by the same amount as I_i and $I_{i+1}-|b|$, that is by $|b| > 2|c_1|$, so by Lemma 1, $W(P_i \cup P_{i+1})$ has period $|c_1|$. It follows that $y=W(P_1 \cup P_2 \cup \cdots P_{n-1})$ has period $|c_1|$. But $|y|=|a_1^n|+(n-2)|u|$, and unless $|y| < |c_1|+|b|$ we can apply Lemma 1 to obtain our conclusion; hence $|y| < |c_1|+|b| \leqq |a_1|+|b|$ and so $n|a_1|+(n-2)|u| < (n+1)|a_1|-|u|$, and $(n-1)|u| < |a_1|$.

Since W begins with b^2 and a_1^n with bu, b begins with u. Since W begins with b and with a_1 and $(n-1)|u| < |a_1|$, a_1 begins with u. Suppose inductively that a_1 begins with u^h, $h < n-1$. Since $y=a_1^n e$, where $|e|=(n-2)|u|$, and y has period $|c_1|$ and since a_1 begins with u^h, e begins with u^h. Thus W begins with $a_1^n u^h = bu^{h+1}$, with $|u^{h+1}| < |b|$, whence b begins with u^{h+1} and hence a_1 begins with u^{h+1}. By induction we conclude that $a_1=u^{n-1}v$ and $y=a_1^n u^{n-2}$. Moreover, we have $a_i^n u = u a_{i+1}^n$,

hence $a_i u = u a_{i+1}$ for $1 \leqq i < n-1$, whence $a_1 = u^{n-1}v$, $a_2 = u^{n-2}vu$, ..., $a_i = u^{n-i}vu^{i-1}$, ..., $a_{n-1} = uvu^{n-2}$. Now, also since $a_1^n = bu$, a_1 ends in u, and $a_1 = u^{n-2}zu$ with $zu = uv$. From $bu = a_1^n = (u^{n-1}v)^n = (u^{n-1}v)^{n-2}u^{n-2}zu$ we have $b = (u^{n-1}v)^{n-1}u^{n-2}z$. But

$$a_i^n = u^{n-i}v(u^{n-1}v)^{n-2}u^{n-1}vu^{i-1} = u^{n-i}v(u^{n-1}v)^{n-2}u^{n-2}zu^i,$$

and hence

$$a_1^n \cdots a_{n-1}^n = ((u^{n-1}v)^{n-1}u^{n-2}zu)(u^{n-2}v(u^{n-1}v)^{n-2}u^{n-2}zu^2)\cdots \cdots(uv(u^{n-1}v)^{n-2}u^{n-2}zu^{n-1})$$

$$= ((u^{n-1}v)^{n-1}u^{n-2}z)^{n-1}u^{n-1} = b^{n-1}u^{n-1}.$$

Cancelling this factor from the equation $a_1^n a_2^n \cdots a_k^n = b^n = b^{n-1}(u^{n-1}v)^{n-1}u^{n-2}z$ gives $a_n^n \cdots a_k^n = v(u^{n-1}v)^{n-2}u^{n-2}z$. Thus

$$a_n^n \cdots a_k^n u^n = v(u^{n-1}v)^{n-2}u^{n-2}zu^n = (vu^{n-1})^{n-2}vu^{n-1}vu^{n-1} = ((vu)^{n-1})^n.$$

But this equation has $k' = k+2-n < k$ and since F_0' containing $a_n, \ldots, a_k$, u and vu^{n-1} must also contain $a_1, a_2, \ldots, a_{n-1}$ and b, the lemma is proved.

Proof of Theorem 1. As previously noted, if $k < n$ the conclusion follows, hence we may assume $k = n$. Since $\sum |a_i| = |b|$ if all $|a_i^n| \leqq |b|$ then all $|a_i^n| = |b|$, whence $a_1 = a_2$ and the conclusion follows. Therefore we may suppose some $|a_i^n| > |b|$, say $|a_1^n| > |b|$ where $|a_1| = \max |a_i|$. Suppose $|a_i^n| < |b|$ implies that $(n-1)|a_i| \leqq a_1$, and hence, since $(n-1)|a_1| < |b|$, that $|a_i| < |b|/(n-1)^2$. Let p be the number of i such that $|a_i^n| \geqq |b|$; by Lemma 4 we can suppose that $p \leqq n-2$. For these a_i we have the bound $|a_i| < |b|/(n-1)$. Summing gives

$$|b| = \sum |a_i| < p\frac{|b|}{n-1} + (n-p)\frac{|b|}{(n-1)^2}$$

$$\leqq \left(\frac{n-2}{n-1} + \frac{2}{(n-1)^2}\right)|b| = \frac{n^2-3n+4}{n^2-2n+1}|b|$$

whence $n^2-3n+4 > n^2-2n+1$, $3 > n$, a contradiction. We conclude that there exists some i such that $|a_i^n| < |b|$ and yet $(n-1)|a_i| > |a_1|$. Now consider the positions $P = 2|a_1|, P+|b|, \ldots, P+f|b|$. If two of these are contained in the same I_l then $|a_i^n| > |b|$ and for some j, $|(I_l - j|b|) \cap I_1| \geqq 2|a_1| = |a_1| + |a_l|$ and

$$|(I_l - j|b|) \cup I_1| > |b| + |a_1|,$$

so the conclusion holds by Lemma 1. If each $P+f|b|$ is in a distinct I_l then we claim that $|c_i| = |c_1|$. For if $n = 3$ we may assume that $i = 3$ (if necessary by writing W in reverse order), and, since we assumed that $(n-1)|a_i| > |a_1|$, we have by Lemma 1 that $|c_1| = |c_i|$. If $n \geqq 4$, since I_i contains some $p+f|b|$, we have $|I_i \cap (I_1 + f|b|)| \geqq \min(2|a_1|, a_i^n) \geqq |a_1| + |a_i|$ and again $|c_i| = |c_1|$ by Lemma 1. Now since $|c_i| = |c_1|$ and $|a_i| < |a_1|$ we have $m_1 > 1$, and $(m_1 n - 1)|c_1| < |b|$. If each $|a_j|$ satisfied $(n-1)|a_j|$

$\geqq a_1$ then all $|c_j|$ and $|d|$ would be equal and the conclusion would hold. If not, then

$$\sum_{i=1}^{n} |a_i| - |b| < p\frac{m_1|b|}{m_1 n - 1} + (n-p-1)\frac{|b|}{n} + \frac{|b|}{(n-1)(m_1 n-1)} - |b|$$

$$\leqq \left(\frac{(n-2)^2}{2n-1} + \frac{1}{n} + \frac{1}{(2n-1)(n-1)} - 1\right)|b| < 0, \quad \text{a contradiction.}$$

3. We next prove a sequence of lemmas culminating in the proof of Theorem 2. Before proceeding with the proof, it seems worthwhile to sketch the ideas involved in the remaining rather technical lemmas and give some idea why the techniques we are about to present do not yield a stronger theorem. An analysis of the proof of Theorem 1 shows that the principal techniques involved showing coperiodicity of long and short words and invoking special properties of those a_i satisfying $n|a_i| > |b|$. For $k > n$, such a_i's need not exist but for $k < 2n-2$ and $n \geqq 6$ one of the following happens:

(i) We can find a_i satisfying $n|a_i| > |b|$ and obtain counting arguments basically similar to those used in the proof of Theorem 1 (Lemmas 5 and 7);

(ii) An initial segment of each $[j|b|+1, (j+1)|b|]$ intersects a distinct a_i of period $|c_1|$, and we can inductively decrease $|b|$ (Lemma 6).

It is apparent that these arguments are not applicable to large k, although it might be hoped that analogous arguments could be obtained.

We first describe a rather special method of replacing S with a solution S' whose rank is at least that of S. Although we do not claim that the subsemigroup determined by S' contains all the factors in S, certainly if the conclusion is true for S' it is true for S. Suppose that j and l are such that for some q, p, h, g, $I_q = [h, j]$, $I_{q+p} = [g, l]$ and $W[j, l]$ has period $|a_{q+p}|$. Then if S' is obtained from S by replacing $a_{q+1}^n \cdots a_{q+p}^n$ by $\hat{a}^n a_{q+1}^n \cdots a_{q+p-1}^n$ where $\hat{a} = W[j+1, j+1+|a_{qp}|]$, the periodicity of $W[h, j]$ insures that the number of right letters has not been decreased since the rank of S' is at least the number of its right letters. Now, since S is canonical, its rank is the number of its right letters and our claim is proved. In such a situation we will say that S' is obtained from S by an a_{p+q} left shift.

LEMMA 5. *If $|a_i^n| > |b|$ for $n-1$ values of i then S satisfies the inductive condition.*

Proof. We may assume that $n|a_1| > |b|$ and if $n|a_i| > b$ then, by Lemma 3, $|a_i| = |a_1|$. Let j be the smallest number such that $n|a_j| < |b|$. If $j < n-1$, then the conclusion holds by Lemma 4. We note that each interval $[1, |a_1|]+f|b|$, $0 \leqq f \leqq n-2$ contains exactly one initial point of an I_l such that $|a_l^n| > |b|$. Hence, if i is the smallest integer greater than j such that $|a_i^n| > |b|$, we have $\bigcup_{m=j}^{i-1} I_m \subset [1, |a_1|] + (j-1)|b|$. Therefore, we may use an a_i left shift to obtain a solution S' with $a_1', \ldots, a_j'$ all satisfying $n|a_i'| > |b|$, and the lemma follows by induction.

LEMMA 6. *Let a_1 be the largest power of any primitive of length $|c_1|$ which appears among the a_i and let $|a_1^n| < |b|$. If for each j, $0 \leqq j < n$ there exists a distinct integer $h(j)$*

such that $|c_{h(j)}| = |c_1|$ *and* $I_{h(j)} - j|b|$ *intersects* I_1 *in an interval of length at least* $|c_1|$, *then* S *satisfies the inductive condition.*

Proof. If $i = h(j)$ for some j we call a_i a special word. We may assume that the longest word v of period $|c_1|$ containing a_1 has length less than $|b| + |c_1|$ by Lemma 1. Let $v = W[r+1, p]$ (where, of course, $(n-1)|b| < r \leqq t$) and $|a_1^n| \leqq p < |b| + |c_1|$. Now delete the initial $|c_1^n|$ letters from b. The effect of this operation is just to delete a segment of length $|c_1^n|$ from each special word. Hence, S is replaced by a solution $S' = \langle a_1', \ldots, a_k', b' \rangle$ where $a_q' = a_q$ if a_q is not special and $a_q' = c_q^{m_q - 1}$ if a_q is special (note that if $m_q = 1$ then a_q' is empty). Since S' is obtained from S by deletion and S is canonical, the set R' of right letters of S' is contained in the set R of right letters of S. We claim that $R = R' \cup x_{r+|c_1|}$ (where we interpret the subscript modulo t). For suppose y is an element of R not contained in R'. Then y is the terminal letter of some $a_{h(j)}$. Let i be the smallest such $h(j)$. Then the final letter z of a_{i-1} is not y and the segment za_i^n of W does not have period $|c_1|$. But a_i^n has period $|c_1|$ so $z = x_r$ and $y = x_{r+|c_1|}$.

If $R' = R$ then we have not deleted any h_i from H. Hence the free subsemigroup generated by H' contains $a_1, \ldots, a_k, b$. If exactly n of the a_i are deleted, that is, if for every special a_i we had $m_i = 1$, then the generators of the subsemigroup generated by H' along with c_1 would generate a free subsemigroup containing $a_1, \ldots, a_k, b$. We shall show that these are the only two possibilities and hence the inductive condition is satisfied and the lemma is proved. Assume $R' \neq R$ and some $m_i > 1$ for a special word. By the hypothesis of the lemma this implies that $m_1 > 1$ and $t + p - r \geqq 2n|c_1|$, for $|v| \geqq |c_1^{2n}|$. But now apply the same argument to L, the set of left letters and note that $L \neq L'$ and $R \neq R'$ imply $m_1 = 1$.

LEMMA 7. *Suppose that* $n \geqq 6$ *and* $k \leqq 2n-2$. *If* $|a_i^n| > |b|$ *for some* $i < k$, *then* S *satisfies the inductive condition.*

Proof. We may assume that S does not satisfy the inductive condition, that $n|a_i| > |b|$, that $|c_1| = |c_i|$ and if $|c_1| = |c_j|$ then for some unique f, $P_j = I_j - f|b| \subseteq [1, |b| + |c_1|]$. Let $P = [1, q]$ be the union of these P_j (such that $|c_j| = |c_1|$). By Lemma 1, P has period $|c_1|$ and $q - |b| < |c_1|$. For any integer j, let $\hat{j}$ be the least positive residue of j modulo $|b|$.

We first observe that if $|c_u| < |c_1|$ and if for some f, $I_u - f|b| \subseteq [1, q]$ we must have $|a_u| < |c_1|/(n-1)$ by Lemma 1. If $|c_u| < |c_1|$ and the above condition holds for no f, (i.e., in the case of an interval containing some $h|b|$ and $h|b| + \hat{q} + 1$), then Lemma 1 may have to be applied to initial and terminal segments. In such a case, if $I_u = [y, z]$, $(l-1)|b| < y < l|b|$, then $|c_1| + |a_u| > l|b| + \hat{q} - y$ (condition on period at end of $[1, q]$) and $|c_1| + |a_u| > z - l|b|$ (condition on period at beginning of $[1, q]$). Hence $2|c_1| + 2|a_u| > z - y + \hat{q} = n|a_u| + \hat{q}$, or equivalently $(n-2)|a_u| < 2|c_1| - \hat{q}$. Since $n \geqq 6$ this implies that $|a_u| < |c_1|/2$ and $|a_u^n| < 3|c_1| - \hat{q}$.

Let r be such that $(n-1)|b| \in I_r = [e, g]$. We consider two cases.

Case 1. $|c_r|=|c_1|$. Then $(n-1)|b|\leqq g\leqq(n-1)|b|+\hat{q}$ and $m_in|c_1|>|b|-\hat{g}>|b|-|c_1|\geqq(m_in-1)|c_1|-\hat{q}>(m_in-2)|c_1|$. Also since c_1 is primitive, $a_r^n\cdots a_k^n$ has length $|b|-\hat{g}$ and period $|c_1|$ and has no smaller period. Hence for $r+1\leqq j\leqq k$ either $|a_j|=m_j|c_1|$ with $m_j<m_i$ or $(n-1)|a_j|<|c_1|$ by Lemma 1; and $m_in|c_1|>n\sum_{j=r+1}^{k}|a_j|>(m_in-2)|c_1|$. Thus the total length of those I_j, $r+1\leqq j\leqq k$ such that $|c_j|=|c_1|$ is greater than $(n-2)|c_1|$ and $k-r>(n-2)|c_1|/(n|c_1|/(n-1))=(n-2)(n-1)/n>n-3$, hence $k-r\geqq n-2$.

Now we will show that $r\geqq n+1$ and hence $k\geqq n+1+(n-2)=2n-1$. Let $L=\{j\mid |a_j|=|a_i|\}$, and let l be the cardinal of L. By Lemma 5, $l\leqq n-2$. If $m_i=1$, since $|a_j|=|a_i|\Rightarrow I_j\subseteq[1,q]+f|b|$ for some f, we must have $n-1-l$ numbers h, less than $n-1$ such that $Q_h=[3|c_1|/2,\ |b|+\hat{q}-3|c_1|/2+h|b|]$ intersects no I_j of period $|c_1|$. For each such h, since $|Q_h|=|b|+\hat{q}-3|c_1|\geqq 6|c_1|-3|c_1|=3|c_1|$, and if I_j intersects Q_h, $|I_j|<6|c_1|/5$ and $I_j\subseteq[h|b|,\ (h+1)|b|]$, by Lemma 1, we know that Q_h intersects more than 15/6 distinct I_j. Hence Q_h intersects at least 3 distinct I_j and $r\geqq l+3(n-l-1)$ with $h\geqq 1$ and hence $r>n+1$.

If, however, $m_i>1$, and $|c_1|=|c_2|=\cdots=|c_r|$ since $|a_i^n|>|b|$ the argument in the proof of Lemma 4 shows that S satisfies the inductive condition. Hence, for some u, $|c_u|<|c_1|$ and $|a_u^n|<3|c_1|-\hat{q}$.

If $j\in L$ and $I_j=[j_1,j_2]$ then $j_1<\hat{q}$ and $j_2\leqq\hat{q}$. Since $l\leqq n-2$, for some $n-1-l\geqq 1$ values of h we must have $Q_h=[\hat{q},\ |b|]+h|b|$ such that Q_h intersects no I_j with $j\in L$. Now, $|b|-\hat{q}\geqq(m_in-2)|c_j|>((m_i-1)n+3)|c_1|$, so such an interval must intersect I_j for at least two values of j with $|c_j|=|c_1|$ and $m_j<m_1$ and at least three distinct I_j if one of these satisfies $|c_j|<|c_1|$. By calculation as above $r>n+1$.

Case 2. $|c_r|<|c_1|$. Let v be such that $(n-2)|b|\in I_v=[y,z]$. Now if $|c_v|=|c_1|$ then $\hat{z}<\hat{q}<|c_1|$ and if $|c_v|<|c_1|$, then $\hat{z}<3|c_1|/2$ by our observation. Hence $\hat{z}<3|c_1|/2$. Also, since $|c_r|<|c_1|$ and both $[1,\hat{e}]$ and $[\hat{g},b]$ are less than $m_in|c_1|$, if $J=\{j\mid v<j<k;\ j\neq r,\ (n-1)|a_j|<|c_1|\}$ then $n\sum_{j\in J}|a_j|+n|a_r|>2[n|c_1|-\hat{q}]-3|c_1|/2$. But $n|a_r|<3|c_1|-\hat{q}$ and hence $n\sum_{j\in J}|a_j|>(4n-9)|c_1|/2-\hat{q}>(4n-11)|c_1|/2$. But $n\geqq 6$ so $n\sum_{j\in J}|a_j|>n|c_1|$, hence $|J|\geqq|n|$. But $u\geqq n-2$ and $k\geqq u+|J|+1\geqq 2n-1$.

Thus, we have shown that if the inductive condition is not satisfied then $k\geqq 2n-1$ and the lemma is proved.

LEMMA 8. *If $n\geqq 6$, $|a_i^n|<|b|$ for $1\leqq i\leqq k$ and $k\leqq 2n-2$ then the inductive condition is satisfied.*

Proof. Let $|c_1|$ be the largest of the $|c_i|$ and a_1 be a longest word of period $|c_1|$. Let $Q=[r+1,p]\supseteq I_1$ be the longest segment of period $|c_1|$ containing I_1. We may assume $|Q|<|b|+|c_1|$ by Lemma 1. First suppose $|Q|<|b|$. Let e be the greatest integer in $3/2|c_1|$, and consider the set of numbers $r+f|b|$ and $e+f|b|$, $0\leqq f\leqq n-1$. We claim that no two members of this set appear in the same I_i. First, if for any g, g and $g+|b|$ appear in I_i then I_i has period $|c_1|$ and properly contains Q, a contradiction. But if $r+f|b|$ and $e+f|b|$ appear in I_i, again I_i must have period $|c_1|$ by Lemma 1 and Q is extended to the left. Similarly, if $e+f|b|$ and $r+(f+1)|b|$ are in

I_i, Q is extended to the right. Hence if $|Q| < |b|$ we have $k \geqq 2n$, and we may assume $|b| \leqq |Q| < |b| + |c_1|$.

Let $P = [|c_1| + 1, m_1 n|c_1|]$ and $R = [1, (m_1 n - 1)|c_1|]$. We will call f special if for every a_i such that $I_i = [d, e]$ and $(d - f|b|) \in P$ or $(e - f|b|) \in R$ we have $|c_i| < |c_1|$. By Lemma 6, if S does not satisfy the inductive condition, there is at least one special f. Suppose f is special. Let g and h be such that $f|b| \in I_g = [g_1, g_2]$ $(f|b| + m_1 n|c_1|) \in I_{h+1} = [h_1, h_2]$. If $g_2 > f|b| + |c_1|$ then since f is special $|c_g| < |c_1|$ and hence $\hat{g}_2 < |c_1| + |c_g|$. However, since $[g_1, g_2]$ is contained in the union of two segments of period $|c_1|$, by Lemma 1, $|c_g| < 2|c_1|/(n-2)$, and $\hat{g}_2 < n|c_1|/(n-2)$. Similarly, $\hat{h}_1 \geqq m_1 n|c_1|/(n-2)$, and $n \sum_{i=g+1}^{h} |a_i| = \hat{h}_1 - \hat{g}_2 > (m_1 n - 3)|c_1|$. But, since f is special for $g < i < h$, $(n-1)|a_i| < |c_1|$, we have $h - g \geqq m_1 n - 3$. If F is the number of special numbers f, then since $n|a_i| < |b|$ for all i by hypothesis, $k \geqq (n - F + 1) + F(m_1 n - 3) = n(1 + m_1 F) - 4F + 1$. If $m_1 > 1$ then $k \geqq n(1 + 2F) - 4F + 1 > 2n$ since $n \geqq 6$. If $F > 1$ then $k \geqq n(1+2) - 4(2) + 1 = 3n - 7 \geqq 2n - 1$. Therefore we may assume $m_1 = F = 1$.

Let the function δ be defined by $I_i = [\delta(i-1) + 1, \delta(i)]$, and we write $\hat{\delta}(i)$ for the operation $\hat{}$ applied to $\delta(i)$. First we claim that if for any j, $|a_j| > |a_1|$ then $k \geqq 2n$. Since by hypothesis $|c_j| < |c_1|$, we must have $\hat{\delta}(j-1) > (n-1)|c_1| - |c_j|$ and either $\hat{\delta}(j) > \hat{\delta}(j-1)$ or $\hat{\delta}(j) < |c_1| + |c_j|$. Hence, by the primitivity of c_1 and c_j, each of the $2n$ integers $3|c_1| + h|b|$, $\hat{\delta}(j-1) + |c_2| + h|b|$, $1 \leqq h \leqq n$ must belong to distinct I_j.

Next, if $|c_1| = |c_i|$ then for some u, $\delta(i-1) < (n-1)|c_1|$ or $|c_1| < \delta(i)$. Suppose not. Then $|b| > (2n-2)|c_1|$ and for each j, $|a_j| \leqq |c_1|$. Hence $k \geqq 2n - 1$. Now, let f be the unique special number, and if $f \neq n-1$, let i be the smallest integer such that $I_i = [i_1 + 1, i_2]$, $\delta(i-1) \geqq f|b| + |c_1|$ and $|c_1| = |c_i|$. Replace S by

$$\langle a_i, a_{i+1}, a_k, a_1, \ldots, a_{i-1}, b' \rangle.$$

We will now prove the lemma for this new S which clearly has the same H as the old one; and in addition, either the conclusion holds by Lemma 6 or the unique special number is now $n-1$. Let j satisfy $(n-1)|b| \in I_j$. Suppose $|c_j| = |c_1|$. Then we have $[1, |b|]$ of period $|c_1|$ and for $j < i \leqq k$, $(n-1)|a_i| < |c_1|$. But $n|b| - \delta(j) > (n-1)|c_1|$, hence $k - j \geqq n - 1$. But $j \geqq n$ so $k \geqq 2n - 1$. Suppose $|c_j| < |c_1|$. By previous arguments, $(k-1) - j \geqq n - 3$, hence $k - (j-1) \geqq n - 1$. Hence if $k < 2n - 1$ since only $(n-1)$ is special we must have $|c_i| = |c_1|$ if $1 \leqq i < n - 1$.

If $|b| \geqq (n+1)|c_1|$, counting arguments of the above type show that $k \geqq 2n - 1$. Hence we have $|b| < \delta(1) + |c_1|$, and $\delta(1) > \delta(2) - |b| > \delta(3) - 2|b| > \cdots > \delta(n-1) - (n-2)|b|$. Now we may assume that $\delta(i) - (i-1)|b| > \delta(1) - |c_1|$ for $1 \leqq i \leqq n-2$. For if $\delta(i) - (i-1)|b| \leqq \delta(1) + |c_1|$ and $\delta(i+1) - i|b| \geqq \delta(1) + |c_1|$ we have $|a_1| = |a_2|$ by periodicity considerations and the inductive condition is satisfied.

Now $b = a_1^n z$. Also, since $\delta(n-2) - (n-3)|b| > \delta(1) - |c_1|$ we must have $\delta(n-3) - (n-4)|b| > |b| - |c_1|$. Hence $(n-3)|b| - |c_1| < (n-3)|c_1|$ so $(n-3)(n|c_1| + |z|) < n(n-3)|c_1| + |c_1|$ and $(n-3)|z| < |c_1|$. We claim that for $1 \leqq i \leqq n-2$, $W[\delta(i) + 1, \delta(i-1) + |b|] = z$. First, $a_2 = zx$ for some x. But $a_1 = xy$ since x is initial to b and $|y| = |z|$. But since $n \geqq 2$, using the periodicity of a_2 we have $z = y$. Inductively, if

$q<n-3$ and the claim is valid for $1\leqq i\leqq q$ we have $a_{q+1}=z^{q+1}x'$ (since we have shown that $(n-3)|z|<|c_1|$). But then $a_1=x'z^{q+1}$.

Now we have $a_1=xz^{n-3}$, $b=(xz^{n-3})^n z$ and $a_n^n a_{n+1}^n\cdots a_k^n=z^{n-2}(xz^{n-3})^n z$. Either a_k is coperiodic with z or $(n-1)|a_k|<|z|$ or $|a_k|+|z|>(n-2)|z|$ since the terminal segment of b is z^{n-2}. We will show that each of these possibilities implies that $(n-2)|a_k|<|c_1|$.

If $z=y^r$, $a_k=y^q$, y primitive, we know that x cannot be a power of y or a_1 and b would be coperiodic. Let v be the longest terminal segment of b of period $|y|$. We know $|v|<|yxz^{n-2}|$. Thus $n|a_k|=nq|y|<|y|+|x|+r(n-2)|y|$, and $(n-1)|a_k|<|x|+r(n-2)|y|=|c_1|+|z|\leqq c_1+|a_k|$ and so $(n-2)|a_k|<|c_1|$.

If $(n-1)|a_k|<|z|$ then $(n-2)|a_k|<|z|<|c_1|$.

If $|a_k|+|z|>(n-2)|z|$ then $|a_k|>(n-3)|z|$ and in order that a_1 and a_k not be periodic we must have $|a_k|+|c_1|>(n-1-1/(n-3))|a_k|>(n-2)|a_k|$.

By symmetry, the same argument applies to $|a_n|$. Now either $(n-1)|a_i|<|c_1|$ for $n<i<k$ or $n|a_k|<|z|$ and $n|a_n|<|z|$. The nontrivial case is the former and here, if $k-n\leqq n-2$ we have

$$n\sum_{i=n}^{k}|a_i| < 2n|c_1|/(n-2)+n(n-3)|c_1|/(n-1) = |c_1|n(n-3)/(n-2) < |b_1|$$

contradiction, and Lemma 8 is proved.

References

1. G. Baumslag, *On a problem of Lyndon*, J. London Math. Soc. **35** (1960), 30–32.

2. A. Lentin, *Sur l'équation $a^M=b^Nc^Pd^Q$ dans un monoïde libre*, C. R. Acad. Sci. Paris **260** (1965), 3242–3244.

3. R. C. Lyndon, *The equation $a^2b^2=c^2$ in free groups*, Michigan Math. J. **6** (1956), 89–95.

4. R. C. Lyndon and M. Schützenberger, *The equation $a^M=b^Nc^P$ in a free group*, Michigan Math. J. **9** (1962), 289–295.

5. E. Schenkman, *The equation $a^nb^n=c^n$ in a free group*, Ann. of Math. **70** (1959), 562–564.

6. J. Stallings, *On certain relations in free groups*, Abstract 559–166, Notices Amer. Math. Soc. **6** (1959), 532.

Institute For Defense Analyses,
Princeton, New Jersey
The University of Illinois,
Urbana, Illinois