Can. J. Math., Vol. XXVII, No. 6, 1975, pp. 1329–1335

PRODUCTS OF COMMUTATORS AS PRODUCTS OF SQUARES

CHARLES C. EDMUNDS

1. Introduction. In any group G, the commutator subgroup G' is contained in G^2, the subgroup of G generated by the squares in G. Thus any product of commutators can be written as a product of squares in G. For instance, the commutator $[x, y]$ $(= xyx^{-1}y^{-1})$ can be expressed as the product of three squares: $[x, y] = x^2(x^{-1}y)^2(y^{-1})^2$. Roger Lyndon and Morris Newman have made the interesting observation [**4**, Theorem 1] that, in this case, the number three is minimal in the sense that there are groups which contain commutators not expressible as the product of fewer than three squares. In particular, if G is the free group of rank two $\langle x_1, x_2; \emptyset\rangle$, no endomorphism of G sends $x_1^2x_2^2$ to $[x_1, x_2]$(i.e. there are no words U and V in G for which $U^2V^2 = [x_1, x_2]$).

Let F be the countably generated free group $\langle x_1, x_2, \ldots ; \emptyset\rangle$ and let $S(n)$ and $C(n)$ denote the words $x_1^2x_2^2 \ldots x_n^2$ and $[x_1, x_2][x_3, x_4] \ldots [x_{2n-1}, x_{2n}]$ respectively, with $S(0) = C(0) = 1$ (the empty word). We generalize the result of Lyndon and Newman to products of commutators as follows.

THEOREM 1. *There is an endomorphism of F sending $S(2n + 1)$ to $C(n)$, for $n \geqq 0$.*

THEOREM 2. *No endomorphism of F sends $S(2n)$ to $C(n)$, for $n > 0$.*

As an immediate consequence we obtain the following:

COROLLARY. *If g is the product of n (>0) commutators in a group G, then g can be written as the product of $2n + 1$ squares but, in general, g is not expressible as a product of fewer squares.*

A word W in F is said to be *quadratic* if each generator occurring in W appears, with exponent $+1$ or -1, exactly twice. As an application of our results we will give a new solution to the endomorphism problem (see **2**) for quadratic words. The proof of Theorem 1 is straightforward. The proof of Theorem 2 is based on certain previous results [**2**; **3**] of the author; these will be summarized briefly just prior to their use. A completely different proof of Theorem 2 due to R. C. Lyndon will appear in the forthcoming book by Lyndon and Schupp.

Received July 29, 1974 and in revised form, March 5, 1975.

The author wishes to thank the University of Manitoba and the Canadian Mathematical Congress, Summer Research Institute (University of Calgary, 1974) for financial support of this research.

The author wishes to thank the referee whose comments have led to considerable improvement in the exposition of this paper.

2. Proof of Theorem 1. If an automorphism of F sends U to V we say that the words U and V are *automorphic* and write $U \cong V$.

LEMMA 1. *If x, y, and z are three distinct x_i's, then there is a sequence of Nielsen automorphisms (induced by free substitutions* [**5**, p. 120]) *sending $x^2y^2z^2$ to $x^2[y, z]$.*

Proof. The following sequence of free substitutions sends $x^2y^2z^2$ to $x^2[y, z]$: (1) $y \to x^{-1}y$, x and z fixed; (2) $y \to yx$, x and z fixed; (3) $z \to x^{-1}z$, x and y fixed; (4) $y \to yz^{-1}$, x and z fixed; (5) $y \to yx$, x and z fixed; (6) $x \to xy^{-1}$, y and z fixed; (7) $x \to x$, $y \to y^{-1}$, $z \to z^{-1}$.

Let $C'(n)$ denote the word $[x_2, x_3][x_4, x_5] \ldots [x_{2n}, x_{2n+1}]$.

LEMMA 2. *For any $n > 0$, there is an automorphism of F sending $S(2n + 1)$ to $x_1^2C'(n)$ and fixing each x_i for $i > 2n + 1$.*

Proof. The result follows from Lemma 1 by induction on n.

Proof of Theorem 1. By Lemma 2, there is an automorphism α of F sending $S(2n + 1)$ to $x_1^2C'(n)$. Define an endomorphism β and an automorphism γ as follows: $\beta : x_1 \to 1$, $x_i \to x_i$ otherwise; $\gamma : x_{i+1} \to x_i$ for $1 \leqq i \leqq 2n + 1$, $x_1 \to x_{2n+1}$, $x_j \to x_j$ otherwise. The composition $\alpha\beta\gamma$ (writing mappings on the right) is an endomorphism of F sending $S(2n + 1)$ to $C(n)$.

Remarks. (1) Lemmas 1 and 2 are implicit in the work of Dehn [**1**]. (2) Using the proof of Theorem 1, $C(n)$ can be written as a product of squares explicitly. For instance $C(2) = [x_1, x_2][x_3, x_4]$ can be written as

$$x_1^2(x_1^{-1}x_2x_1)^2(x_1^{-1}x_2^{-1}x_3)^2(x_3^{-1}x_2x_1x_3^{-1}x_1^{-1}x_2^{-1}x_3x_4x_1^{-1}x_2^{-1}x_3)^2 \times (x_3^{-1}x_2x_1x_4^{-1})^2.$$

3. Lemmas. We begin this section with an explicit discussion of the notational conventions to be used for the remainder of the paper; the reader is referred to Magnus, Karrass, and Solitar [**5**] for any unexplained notation. This is followed by a sequence of lemmas concerning the interplay between the application of automorphisms and trivializations (defined below) to quadratic words. The key lemma is Lemma 5 which will be used in the next section to prove Theorem 2.

Given the free group F, we call $X = \{x_1, x_2, \ldots\}$ the set of *generators* of F and $L = \{x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots\}$ the set of *letters* of F. A *reduced* word is a finite string of letters in which no letter occurs next to its inverse. We will view F as the set of reduced words where the product of two words U and V, denoted $U \cdot V$, is formed by juxtaposition followed by reduction (i.e. deletion of all subwords of the form xx^{-1} for $x \in L$). Furthermore, a dot will be used

to indicate a point at which some cancellation (i.e. reduction) might occur in a product; thus if there is no cancellation between U and V in forming their product, we write $U \cdot V = UV$. If $W \in F$ and φ is an endomorphism of F, the word $W\varphi$ is obtained by replacing each letter of W by its image under φ and reducing the result. The length of a word W will be denoted $|W|$. For $S \subseteq L$, we define the endomorphism τ_S, *trivialization* of S, by

$$\tau_S\colon x \to 1 \text{ if } x \in S \text{ or } x^{-1} \in S,\ y \to y \text{ otherwise.}$$

Henceforth, lower case letters occurring as parts of words will denote elements of L.

LEMMA 3. *If* $U\tau_S = V$ *where* $U = A_1xA_2yA_3x^{-1}A_4$ *is quadratic,* $A_2 \neq 1$, y^{-1} *occurs in* A_1 *or* A_4, *and* τ_S *fixes* x *and* y, *then:*

(i) $V = B_1xB_2yB_3x^{-1}B_4$, *where* $A_i\tau_S = B_i$ $(1 \leqq i \leqq 4)$, *and*

(ii) *there are quadratic words* U' *and* V', *automorphic to* U *and* V *respectively, such that* $U'\tau_S = V'$, $U' = A_1xA_2'yA_3'x^{-1}A_4$, $V' = B_1xB_2'yB_3'x^{-1}B_4$, *and* $|A_2'| < |A_2|$.

Proof. Denote τ_S by τ.

(i) Since τ fixes x and y,

$$V = U\tau = (A_1\tau) \cdot x \cdot (A_2\tau) \cdot y \cdot (A_3\tau) \cdot x^{-1} \cdot (A_4\tau).$$

U is quadratic, thus neither x nor x^{-1} occurs in $A_i (1 \leqq i \leqq 4)$. As a result, there is no x or x^{-1} in any $A_i\tau$. In particular, $A_1\tau$ does not end with x^{-1}, $A_2\tau$ does not begin with x^{-1}, $A_3\tau$ does not end with x, and $A_4\tau$ does not begin with x. Therefore the dots surrounding x and x^{-1} can be omitted from the expression above. Since y^{-1} occurs in A_1 or A_4, y^{-1} is in either $A_1\tau$ or $A_4\tau$; thus $A_2\tau$ does not end with y^{-1} and $A_3\tau$ does not begin with y^{-1}. As a result, the dots surrounding y can be omitted. We now have

$$V = (A_1\tau)x(A_2\tau)y(A_3\tau)x^{-1}(A_4\tau)$$

as desired.

(ii) Since $A_2 \neq 1$, we can write

$$A_2 = aA_2' \text{ and } U = A_1xaA_2'yA_3x^{-1}A_4.$$

Note that $|A_2'| < |A_2|$. Let α be the automorphism defined by $\alpha\colon x \to xa^{-1}$, $y \to y$ for $y \neq x^{\pm 1}$, and let $U' = U\alpha$. There are two cases: (1) $a\tau = 1$ and (2) $a\tau \neq 1$.

Case 1. Let $V' = V$. Clearly,

$$U' = U\alpha = A_1xA_2'y(A_3 \cdot a)x^{-1}A_4.$$

By part (i) $A_i\tau = B_i$ $(1 \leqq i \leqq 4)$, therefore letting $A_3' = A_3 \cdot a$, $B_2' = B_2$, and $B_3' = B_3$ it remains to show that $A_2'\tau = B_2$ and $(A_3 \cdot a)\tau = B_3$.

Since $a\tau = 1$,

$$A_2'\tau = (a^{-1} \cdot aA_2')\tau = (a^{-1}\tau) \cdot (A_2\tau) = 1 \cdot B_2 = B_2, \text{ and}$$
$$(A_3 \cdot a)\tau = (A_3\tau) \cdot (a\tau) = B_3 \cdot 1 = B_3.$$

Case 2. Let $V' = V\alpha$. It is easy to see that

$$U' = A_1xA_2'y(A_3 \cdot a)x^{-1}A_4 \quad \text{and} \quad V' = B_1x(a^{-1} \cdot B_2)y(B_3 \cdot a)x^{-1}B_4.$$

Again by part (i), $A_i\tau = B_i (1 \leqq i \leqq 4)$; therefore, letting $A_3' = A_3 \cdot a$, $B_2' = a^{-1} \cdot B_2$, and $B_3' = B_3 \cdot a$, it remains to show that $A_2'\tau = a^{-1} \cdot B_2$ and $(A_3 \cdot a)\tau = B_3 \cdot a$.

Since $a\tau \neq 1$, $a\tau = a$; therefore,

$$A_2'\tau = (a^{-1} \cdot aA_2')\tau = (a^{-1}\tau) \cdot (A_2\tau) = a^{-1} \cdot B_2, \text{ and}$$
$$(A_3 \cdot a)\tau = (A_3\tau) \cdot (a\tau) = B_3 \cdot a.$$

LEMMA 4. *If V is a non-trivial quadratic word in F', then there are letters x and y such that $V = B_1xB_2yB_3x^{-1}B_4y^{-1}B_5$ (where any of the B_i's may be empty).*

Proof. Since $V \in F'$, the exponent sum [**5**, p. 76] on each generator occurring in V is zero. Furthermore V is quadratic; hence for each letter appearing in V, its inverse appears exactly once in V. Suppose that x and x^{-1} are letters in V with a minimal number of letters between them. (This number is positive since V is assumed to be reduced.) Let y be any letter between x and x^{-1}. By the minimality assumption, y^{-1} does not occur between x and x^{-1} in V; therefore, $V = A_1xA_2yA_3x^{-1}A_4$ with y^{-1} occurring in either A_1 or A_4. Relabeling "x" by "y" and "y" by "x^{-1}", if necessary, we write $V = B_1xB_2yB_3x^{-1}B_4y^{-1}B_5$.

LEMMA 5. *If $U\tau_S = V(\neq 1)$ where U is quadratic and $V \in F'$, then there are quadratic words U_1 and V_1, automorphic to U and V respectively, such that $U_1\tau_S = V_1$, and for some letters x and y, $U_1 = [x, y]U_2$ and $V_1 = [x, y]V_2$.*

Proof. Denote τ_S by τ. Clearly V is quadratic, thus by Lemma 4 there are letters x and y such that $V = B_1xB_2yB_3x^{-1}B_4y^{-1}B_5$. Since $V = U\tau$, it is clear that τ fixes x and y and that $U = A_1xA_2yA_3x^{-1}A_4y^{-1}A_5$ (i.e. that x, y, x^{-1}, and y^{-1} occur in the same order in U as they do in V). By Lemma 3(i), $A_i\tau = B_i (1 \leqq i \leqq 3)$ and $(A_4y^{-1}A_5)\tau = B_4y^{-1}B_5$. Again by Lemma 3(i), $(A_1xA_2)\tau = B_1xB_2$ and $A_j\tau = B_j (3 \leqq j \leqq 5)$. Thus $A_i\tau = B_i$ $(1 \leqq i \leqq 5)$.

If $A_2 \neq 1$, then by Lemma 3(ii) there exist quadratic words U' and V' such that $U'\tau = V'$,

$U \cong U' = A_1xA_2'yA_3'x^{-1}A_4y^{-1}A_5$, and $V \cong V' = B_1xB_2'yB_3'x^{-1}B_4y^{-1}B_5$, where $|A_2'| < |A_2|$. By successive applications of this reduction, we arrive at words U'' and V'' such that $U''\tau = V''$,

$$U \cong U'' = A_1xyA_3''x^{-1}A_4y^{-1}A_5, \text{ and } V \cong V'' = B_1xyB_3''x^{-1}B_4y^{-1}B_5.$$

We apply the same technique, using y and y^{-1} in place of x and x^{-1}, to reduce A_3'' to the empty word. Thus there are quadratic words $U^{(3)}$ and $V^{(3)}$

such that $U^{(3)}\tau = V^{(3)}$,

$$U \cong U^{(3)} = A_1xyx^{-1}A_4'y^{-1}A_5, \text{ and } V \cong V^{(3)} = B_1xyx^{-1}B_4'y^{-1}B_5.$$

Next we apply the inner automorphisms $W \to y^{-1}x^{-1}A_1^{-1} \cdot W \cdot A_1xy$ and $W \to y^{-1}x^{-1}B_1^{-1} \cdot W \cdot B_1xy$ to $U^{(3)}$ and $V^{(3)}$ respectively. By repeating the procedure above, we reduce A_4' to 1 and arrive at quadratic words $U^{(4)}$ and $V^{(4)}$ such that $U^{(4)}\tau = V^{(4)}$,

$$U \cong U^{(4)} = x^{-1}y^{-1}(A_5 \cdot A_1)'xy, \text{ and } V \cong V^{(4)} = x^{-1}y^{-1}(B_5 \cdot B_1)'xy.$$

Finally we apply the inner automorphism $W \to xy \cdot W \cdot y^{-1}x^{-1}$ to both $U^{(4)}$ and $V^{(4)}$, to obtain quadratic words U_1 and V_1 such that $U_1\tau = V_1$,

$$U \cong U_1 = [x, y]U_2, \text{ and } V \cong V_1 = [x, y]V_2.$$

4. Proof of Theorem 2. We begin this section by quoting some results which will be used in the proof of Theorem 2. The necessary facts are listed as lemmas in order to facilitate their use later.

LEMMA 6. *Given any non-trivial quadratic word W, there is a unique word $U \in \{S(n), C(n) : n \geqq 1\}$ such that $W \cong U$. Furthermore, for any given W, there is an effective procedure for finding U.*

Proof. In [**1**] Max Dehn observed that any non-trivial quadratic word is automorphic to either $S(n)$ or $C(n)$ for some $n > 0$. In order to prove uniqueness, it suffices to show that no two words of the form $S(n)$ or $C(n)$ $(m, n > 0)$ are automorphic. Since F' is a characteristic subgroup of F, no automorphism of F sends $C(m)$ $(\in F')$ to $S(n)(\notin F')$. By Lemma 1 of [**3**] (which is Theorem 2 of [**4**]), $S(n) \cong S(n')$ implies that $n = n'$. And by Lemma 2 of [**3**], if $C(m) \cong C(m')$, then $m = m'$. The effectiveness of the procedure for finding U is immediate from the proof of Dehn's observation [**1**].

LEMMA 7. *If U is an endomorphic image of W, there exists a sequence of words $W = W_0, W_1, \ldots, W_m$ and a sequence of endomorphisms $\varphi_1, \varphi_2, \ldots, \varphi_m$ such that:*

(i) $W_{i-1}\varphi_i = W_i$ $(1 \leqq i \leqq m)$.

(ii) *Each φ_i is either a trivialization or a special type of automorphism. (In the terminology of* [**2**, p. 5 and p. 8], *each φ_i is either a trivialization, a level substitution, or a $\rho(s, g, i)$ where s is a square or $i = 1$).*

(iii) *There is an endomorphism γ such that $W_m\gamma = U$ and no cancellation occurs in forming this endomorphic image (i.e. when the letters of W_m are replaced by their images under γ, no reduction applies to the result).*

(iv) *If W is quadratic, each W_i is quadratic* $(1 \leqq i \leqq m)$.

Proof. Parts (i), (ii), and (iii) are the main import of Lemma B.2 of [**2**]. Part (iv) follows from parts (i) and (ii) by the fact that trivializations, level substitutions, and $\rho(s, g, i)$'s preserve the property of being quadratic.

https://doi.org/10.4153/CJM-1975-135-6 Published online by Cambridge University Press

Proof of Theorem 2. Having quoted these results, we are ready to prove Theorem 2. Suppose that $C(n)$ is an endomorphic image of $S(2n)$ for some $n > 0$. By Lemma 7, there is a sequence of quadratic words $W_0 = S(2n)$, $W_1, \ldots, W_m$, a sequence of trivializations and automorphisms $\varphi_1, \varphi_2, \ldots, \varphi_m$, with $W_{i-1}\varphi_i = W_i$, and an endomorphism γ such that $W_m\gamma = C(n)$ and no cancellation occurs when γ is applied to W_m.

First we observe that $W_m \in F'$, as follows. Since W_m is quadratic and γ allows no cancellation, if any letter of W_m is sent by γ to a word of length greater than one, the word $W_m\gamma$ contains two separate occurrences of this word, or its inverse. By inspection, $C(n)$ $(= W_m\gamma)$ contains no such subwords; therefore γ sends each letter of W_m to a letter of $C(n)$. Since each letter of $C(n)$ occurs with exponent sum zero, the same is true for W_m; therefore $W_m \in F'$.

Since $W_0 \notin F'$, $W_m \in F'$, and F' is a fully invariant subgroup of F, there is a number k $(0 \leqq k \leqq m)$ such that $W_i \notin F'$ for $i \leqq k$ and $W_j \in F'$ for $j > k$. In particular, $W_k \notin F'$ and $W_{k+1} \in F'$; thus the endomorphism φ_{k+1} is not an automorphism. By Lemma 7(ii), φ_{k+1} is a trivialization, call it τ.

By Lemma 5 there are quadratic words U_1 and V_1, automorphic to W_k and W_{k+1} respectively, such that $U_1\tau = V_1$, $U_1 = [x, y]U_2$, and $V_1 = [x, y]V_2$. Clearly $U_2\tau = V_2$, and by repeated use of Lemma 5 we arrive at quadratic words U and V, automorphic to W_k and W_{k+1} respectively, such that $U\tau = V$, $U = C(q)U'$, and $V = C(q)$ (for some $q > 0$).

Now $C(n)$ is an endomorphic image of $C(q)$, since $C(q) = V \cong W_{k+1}$ and $\varphi_{k+2}\varphi_{k+3} \ldots \varphi_m\gamma$ sends W_{k+1} to $C(n)$. Thus by Lemma 2 of [**3**], $q \geqq n$. Since $C(q)U' = U \cong W_k \notin F'$, U' is a quadratic word not in F'. Therefore by Lemma 6, $U' \cong S(p)$ for some $p > 0$. By repeated applications of Lemma 1, $C(q)U' \cong S(p + 2q)$. Thus $W_k \cong S(p + 2q)$. However, W_k is an endomorphic image of $W_0 = S(2n)$; hence, by Lemma 1 of [**3**], $p + 2q \leqq 2n$. Therefore we have $2n \leqq 2q < p + 2q \leqq 2n$; a contradiction. This completes the proof of Theorem 2.

5. An application. In this section Theorems 1 and 2 are used to solve the endomorphism problem (see [**2**]) for any quadratic word W. The problem is: Given a quadratic word W, to decide whether or not a given word U (not necessarily quadratic) is an endomorphic image of W.

If we suppose that U is an endomorphic image of W, Lemma 7 implies the existence of a quadratic word W_m, which is an endomorphic image of W, and an endomorphism γ such that no cancellation occurs in forming $W_m\gamma (= U)$. It is clear that such a W_m and γ exist if and only if U is an endomorphic image of W. Starting with a given U, it is easy to find all possible candidates for W_m: list all quadratic words of length no greater than U and determine which of these can be sent to U by a substitution admitting no cancellation. The problem is therefore reduced to deciding whether or not a given non-trivial quadratic word V is an endomorphic image of W.

By Lemma 6, there are two cases: (1) $W \cong C(n)$ for some $n > 0$, or (2) $W \cong S(n)$ for some $n > 0$.

Case 1. If $V \cong S(m)$ for some $m > 0$, there is no endomorphism sending W to V since this would yield an endomorphism sending $C(n)$ to $S(m)$. If $V \cong C(m)$ for some $m > 0$, then, by Lemma 2 of [**3**], V is an endomorphic image of W if and only if $m \leqq n$.

Case 2. If $V \cong S(m)$ for some $m > 0$, Lemma 1 of [**3**] implies that V is an endomorphic image of W if and only if $m \leqq n$. If $V \cong C(m)$ for some $m > 0$, Theorems 1 and 2 say that V is an endomorphic image of W if and only if $m \leqq [(n - 1)/2]$, where $[x]$ denotes the greatest integer less than or equal to x.

References

1. M. Dehn, *Über unendliche diskontinuierliche Gruppen*, Math. Ann. *71* (1912), 116–144.
2. C. Edmunds, *On the endomorphism problem for free groups*, Comm. Algebra *3* (1975), 1–20.
3. ——— *Some properties of quadratic words in free groups* (to appear in Proc. Amer. Math. Soc.).
4. R. Lyndon and M. Newman, *Commutators as products of squares*, Proc. Amer. Math. Soc. *39* (1973), 267–272.
5. W. Magnus, A. Karrass, and D. Solitar, *Combinatorial group theory* (Interscience, New York, 1966).

University of Manitoba,
Winnipeg, Manitoba