Canad. Math. Bull. Vol. **24** (1), 1981

COMMUTATORS IN FREE GROUPS

BY
R. C. LYNDON AND M. J. WICKS

1. Introduction and summary. We study the representations of an element of a free group as a commutator. For a given element g of a free group F, we are interested in the set of all pairs (x, y) of elements of F such that

$$[x, y]=g, \tag{1}$$

where $[x, y]=xyx^{-1}y^{-1}$. If $g=1$, the problem is trivial. We assume henceforth that $g\neq 1$.

Wicks [4] gave a simple criterion for the existence of a solution of equation (1). Now, it is evident that $[x, y]$ is unchanged by either of the transformations

A: $(x, y)\mapsto(x, xy)$,

B: $(x, y)\mapsto(yx, y)$.

Thus, if (x, y) is obtained from a solution (x_0, y_0) by a succession of transformations $A^{\pm 1}, B^{\pm 1}$, then (x, y) will be another solution. Sharpening a result of Hmelevskii [2], Burns, Edmunds, and Farouqi [1] showed that all solutions fall into a finite number of (A, B)-families related in this way. They observed, moreover, that $[x, y]$ is in fact unchanged by transformations of the more general form

A^*: $(x, y)\mapsto(x, x_1y)$ *where* $[x_1, x]=1$,

B^*: $(x, y)\mapsto(y_1x, y)$ *where* $[y_1, y]=1$.

For example,

$$[x^2, y]=[x^2, xy], \tag{2}$$

where (x^2, y) and (x^2, xy) fall into the same (A^*, B^*)-family, but not (as we shall see) into the same (A, B)-family.

Burns, Edmunds, and Farouqi asked if, for every $g\neq 1$, all solutions of (1) lie in the same (A^*, B^*)-family. The primary purpose of this note is to give an example where this is not the case. (We give the simplest example we know, which is in some respects rather special; the general problem remains under investigation.)

Received by the editors June 6, 1979 and, in revised form, February 22, 1980.

2. Preliminaries and known results. After some preliminaries we give short proofs of the known results cited above, upon which our discussion depends.

The solutions of (1) for any conjugate of g correspond to the solutions for g in an obvious way. Thus nothing is lost if we take the convenient step of replacing equation (1) by the condition

(3) $[x, y]$ *is conjugate to* g *in* F.

Now, the conjugacy class of [x, y] is unchanged not only by the transformations A and B, but also by the transformations

C: $(x, y) \mapsto (\bar{y}, x)$,

D_w: $(x, y) \mapsto (x^w, y^w)$ *for* w *in* F,

where we have written $\bar{u} = u^{-1}$ and $u^v = \bar{v}uv$. The totality of transformations A, B, C, D_w generate a group G, acting on the set of all solutions of (3). We shall refer to the set of all solutions obtainable from a given solution by transformations in G as a *G-orbit.*

The case where F itself is generated by the solution (x, y) is illuminating. Since $[x, y] = g \neq 1$, the free group F is not abelian, whence F is free of rank 2, with basis (x, y). The transformations in G, acting on the basis (x, y), now induce automorphisms of F. A result of Nielsen [3] states that G is (isomorphic to) a subgroup of index 2 in the group Aut F of all automorphisms of F, which is in fact the preimage of $\mathrm{SL}(2, \mathbf{Z}_m)$ under the natural map of Aut F onto $\mathrm{GL}(2, \mathbf{Z})$. In the general case, if $U = \langle x, y\rangle$ is the subgroup of F generated by x and y, then G permutes the elements of the conjugacy class of U in F. If $\bar{U}$ is the image of U in the free abelian quotient group $\bar{F} = F/[F, F]$ of F, then evidently G leaves $\bar{U}$ fixed. In example (2) if $U_1 = \langle x^2, y\rangle$ and $U_2 = \langle x^2, xy\rangle$, then clearly $\bar{U}_1 \neq \bar{U}_2$, whence (x^2, y) and (x^2, xy) do not belong to the same G-orbit.

We define the BEF-*family* of a solution (x, y) of (3) to consist of all solutions obtainable from (x, y) by repeated applications of transformations from G, or of the form A^* or B^*. The previous example shows that, in general, the G-orbit of (x, y) is properly contained in the BEF-family. We introduce now a condition sufficient to ensure that the G-orbit and BEF-family coincide.

The transformation A^*: $(x, y) \mapsto (x, x_1 y)$ applies only if $[x_1, x] = 1$. This is equivalent to the condition that $x = z^n$ for some z in F and some integer n, and that x_1 is also a power of z. In the special case that $n = 1$, this application of A^* is simply a power of A. Similar remarks apply to B^* and B.

A subgroup U of F is called *root-closed in* F if and only if, for any w in F and any positive integer n, if $w^n \in U$ then $w \in U$.

Let (x, y) be a solution of (3) and suppose that $U = \langle x, y\rangle$ is root-closed in F. If (x', y') is in the G-orbit of (x, y), then (x', y') is a basis for U. Since U is root-closed in F, no element of a basis for U is a proper power. It follows that

https://doi.org/10.4153/CMB-1981-016-1 Published online by Cambridge University Press

any application of A^* or B^* to (x', y') is simply a power of A or B. We conclude the following:

(4) *If $U = \langle x, y\rangle$ is root-closed in F, then the BEF-family of the solution (x, y) reduces to a single G-orbit.*

We base proofs of the cited results of Wicks and of Hmelevskii and Burns–Edmunds–Farouqi on the following lemma.

LEMMA. *If $u_0, v_0 \in F$ and $[u_0, v_0] \neq 1$, then the G-orbit of (u_0, v_0) contains some (u, v) such that*

(i) *there is no cancellation in the product $v\bar{u}\bar{v}u$,*

(ii) *neither factor cancels entirely in the product uv.*

Proof. We may suppose (u, v) chosen such that the sum of the lengths, $|u|+|v|$, is a minimum for all (u, v) in the same G-orbit. It then follows that no factor cancels more than half in any of the products uv, $v\bar{u}$, $\bar{u}\bar{v}$, $\bar{v}u$, whence (ii) is satisfied.

If $[u, v]$ is cyclically reduced, in the sense that there is no cancellation in any of the products uv, $v\bar{u}$, $\bar{u}\bar{v}$, $\bar{v}u$, then (i) also holds and we are finished. If not, the transformation C may be used to effect a cyclic permutation of the factors u, v, $\bar{u}$, $\bar{v}$, thus allowing us to assume (after a possible change of notation) that uv is not reduced.

Suppose that $v\bar{u}$ is not reduced. If u ends with the letter $\bar{a}$, then v must have the (reduced) form $v = av_1\bar{a}$ for some v_1. Then conjugation D_a: $w \mapsto w^a$ replaces (u, v) by (u^a, v_1). Since $|u^a| \leq |u|$ while $|v_1| = |v| - 2$, this contradicts the assumption that $|u|+|v|$ is minimal. Therefore $v\bar{u}$ is reduced. A similar argument shows that $\bar{v}u$ is reduced.

Suppose finally that $\bar{u}\bar{v}$, as well as uv, is not reduced. Since at most half of each factor in these products can cancel, there are non-trivial words b and c such that u and v have reduced forms $u = bu_1\bar{c}$ and $v = cv_1\bar{b}$ for certain words u_1, v_1 with u_1v_1 and $\bar{u}_1\bar{v}_1$ both reduced. Further, $\bar{c}b$ is reduced, since $\bar{v}u$ is reduced. Now conjugation $D_b: w \mapsto w^b$ takes (u, v) to (u', v') where $u' = u_1 \cdot \bar{c} \cdot b$ and $v' = \bar{b}cv_1$, both reduced. Now $|u'|+|v'| = |u|+|v|$, minimal, and $u'v'$ is not reduced, whence, as before, $v'\bar{u}'$ and $\bar{v}'u'$ are reduced. Also, u_1 and v_1 are non-trivial, since neither factor can cancel more than half in the product $u'v'$. But now, from the fact that $\bar{u}_1\bar{v}_1$ is reduced, it follows that $\bar{u}'\bar{v}'$ is reduced, completing the proof of (i). $\square$

Next, let (u, v) be as in the lemma. Then, for certain words a, b, c in F, with $a \neq 1$, $b \neq 1$, we have reduced forms $u = a\bar{c}$, $v = cb$, and $uv = ab$. This gives $[u, v] = abc\bar{a}\bar{b}\bar{c}$, cyclically reduced. We depart from standard usage by writing $[a, b, c] = abc\bar{a}\bar{b}\bar{c}$. We note that, in the other direction, $[a, b, c] = [a\bar{c}, cb]$ identically. This establishes the following.

THEOREM (*Wicks*). *An element $g \neq 1$ in a free group F is a commutator if and only if, for certain elements a, b, c in F, the element g is conjugate to $abc\bar{a}\bar{b}\bar{c}$, where this product is cyclically reduced. Here c may be trivial, but a and b are non-trivial.*

Continuing with the same notation, we note that $|g| = 2(|a|+|b|+|c|)$ while, since $|a|$, $|b| \geq 1$, we have $|u| = |a\bar{c}| = |a|+|c| < |a|+|b|+|c|$ and $|v| = |cb| = |c|+|b| < |a|+|b|+|c|$. This yields a variant of the results of Hmelevskii and Burns-Edmunds-Farouqi.

THEOREM. *Every G-orbit of solutions of* (3) *contains a solution* (u, v) *such that* $|u|, |v| < \frac{1}{2}|g|$.

COROLLARY. *The totality of solutions of* (3) *consists of a finite number of G-orbits.*

3. An example. We seek two pairs (x_1, y_1) and (x_2, y_2) that are not in the same BEF-family, but are such that $[x_1, y_1] = [x_2, y_2]$. If we replace $[x_1, y_1]$ and $[x_2, y_2]$ by certain $[a_1, b_1, c_1]$ and $[a_2, b_2, c_2]$ as above, then $[a_1, b_1, c_1]$ and $[a_2, b_2, c_2]$ are both cyclically reduced and are conjugate, whence they are cyclic permutations of each other.

It turns out that we are able to obtain an example under the simplifying assumption that $c_1 = c_2 = 1$. For this example it is enough to find a_1, b_1, a_2, b_2 such that both products $[a_1, b_1]$ and $[a_2, b_2]$ are cyclically reduced and are cyclic permutations of each other, and that, at the same time, (a_1, b_1) and (a_2, b_2) are not in the same BEF-family.

[One is tempted to examine the even simpler situation where $[a_1, b_1] = [a_2, b_2]$, both cyclically reduced. But it can be shown that this implies that, for certain elements u and v of F and integers p_1, q_1, p_2, q_2, one has

$$a_1 = (uv)^{p_1}u, \qquad b_1 = v(uv)^{q_1}, \qquad a_2 = (uv)^{p_2}u, \qquad b_2 = v(uv)^{q_2}.$$

From this it can be shown that (a_1, b_1) and (a_2, b_2) belong to the same BEF-family.]

We narrow down the search by a further restrictive assumption. For any reduced word w, relative to a given basis X for F, let w^* be the word obtained by reversing the order of the letters in w. We call an element w of F *symmetric* if $w = w^*$. We now assume that a_1, b_1, a_2, and b_2 are symmetric.

Let $w \mapsto \tilde{w}$ be the automorphism of F carrying each element of the basis X to its inverse. Then the three functions $w \mapsto w^{-1}$, $w \mapsto w^*$, $w \mapsto \tilde{w}$ are the three non-trivial elements of a four-group. In particular, if w is symmetric, then $w^{-1} = \tilde{w}$.

We next assume that the two factorizations $[a_1, b_1]$ and $[a_2, b_2]$ of the cyclic word determined by g have factors that overlap in the simplest non-trivial manner. We assume that $g = g_1 \cdots g_8$, cyclically reduced, with all $g_i \neq 1$, and

https://doi.org/10.4153/CMB-1981-016-1 Published online by Cambridge University Press

that

$$(5)\qquad \begin{cases} a_1 = g_1g_2, & b_1 = g_3g_4, \quad \tilde{a}_1 = g_5g_6, \quad \tilde{b}_1 = g_7g_8, \\ a_2 = g_2g_3, & b_2 = g_4g_5, \quad \tilde{a}_2 = g_6g_7, \quad \tilde{b}_2 = g_8g_1. \end{cases}$$

These equations imply that for all i, taking subscripts modulo 8, one has $g_ig_{i+1} = (g_{i+4}g_{i+5})^{-1}$. Since g_ig_{i+1} is symmetric, this gives $g_ig_{i+1} = (g_{i+4}g_{i+5})^{\sim} = \tilde{g}_{i+4}\tilde{g}_{i+5}$. From the equations $|g_ig_{i+1}| = |g_{i+4}g_{i+5}|$ it follows that $|g_i| = |g_{i+4}|$ and hence that $g_{i+4} = \tilde{g}_i$ for all i.

The problem is now reduced, under these assumptions, to finding g_1, g_2, g_3, g_4, all non-trivial, such that

$$(6)\qquad g_1g_2,\ g_2g_3,\ g_3g_4,\ g_4\tilde{g}_1 \quad \textit{are all symmetric.}$$

After a cyclic permutation we may suppose that $|g_1| \le |g_2|, |g_3|, |g_4|$. We now single out the subcase that $|g_2|, |g_3| \le |g_4|$. It is routine to solve the system of conditions (6), under the given assumptions, in terms of certain parameters. Choosing these parameters in the simplest non-trivial way yields the following solution, in a free group F with basis (x, y).

$$(7)\qquad g_1 = x, \qquad g_2 = yxy\bar{x}yxyx, \qquad g_3 = yxyxy\bar{x}yxy, \qquad g_4 = \bar{x}yxyxy.$$

This gives

$$(8)\qquad \begin{aligned} a_1 &= (xyxy)\bar{x}(yxyx), & b_1 &= (yxyxy\bar{x}y)x(y\bar{x}yxyxy), \\ a_2 &= (yxy\bar{x}yxyx)y(xyxy\bar{x}yxy), & b_2 &= (\bar{x}yx)y(xy\bar{x}). \end{aligned}$$

It now follows that $[a_1, b_1]$ and $[a_2, b_2]$ are conjugate. It is easy to see by abelianizing that (a_1, b_1) and (a_2, b_2) are not in the same G-orbit, although we shall obtain this conclusion incidentally in the argument that follows. To show that (a_1, b_1) and (a_2, b_2) are not in the same BEF-family, it will suffice to show, in addition, that $U_1 = \langle a_1, b_1\rangle$ and $U_2 = \langle a_2, b_2\rangle$ are both root-closed.

Let $\Lambda_1 = \{a_1^{\pm 1}, b_1^{\pm 1}\}$. Inspection shows that if $L_1, L_2 \in \Lambda_1$ and $L_1L_2 \ne 1$, then there is no cancellation in the product L_1L_2. It follows that every element w of U_1 can be written uniquely as a product of factors L_i without cancellation. If U_1 and U_2 were conjugate, then b_2 would be conjugate to some word $w = L_1 \cdots L_m$ in U_1, where we may suppose that $L_mL_1 \ne 1$. But then w would be cyclically reduced as a word in the generators x, y of F, and, since w is conjugate to b_2, w would have the same length $|b_2| = 7$ as b_2, which is patently impossible. This shows that (a_1, b_1) and (a_2, b_2) are not in the same G-orbit.

To show that U_1 is root closed, let $w = L_1 \cdots L_m$, $m \ge 1$, without cancellation. We show that $w = z^n$ for some z in F and $n > 1$ implies that $z \in U_1$. We may suppose that w and z are cyclically reduced. Then $w = z_1 \cdots z_n$ without cancellation, a product of n blocks z_i, where each $z_i = z$. If the first block z_1 coincides with a part $L_1 \cdots L_k$ of w, then z is in U_1 as required.

Otherwise we have $z_1 = L_1 \cdots L_{k-1}P$ for some k, $1 \le k \le m$, where $L_k = PQ$

https://doi.org/10.4153/CMB-1981-016-1 Published online by Cambridge University Press

without cancellation and $P, Q \neq 1$. It follows that

$$w = L_1 \cdots L_m = QL_{k\ \ 1} \cdots L_m L_1 \cdots L_{k-1} P.$$

If $|L_1| < |QL_{k+1}|$, this implies that L_1 occurs as an interior segment of $L_k L_{k+1}$. If $|QL_{k+1}| < |L_1|$, this implies that L_{k+1} is a proper subword of L_1. Inspection of Λ_1 shows that neither alternative is possible.

We have shown that U_1 is root-closed in F, and an exactly parallel argument shows that U_2 is root closed. By (4), the BEF-families of (a_1, b_1) and (a_2, b_2) coincide with their G-orbits, and these have been shown to be distinct.

We restate the result in explicit terms. Let a_1, b_1, a_2, b_2 be as given in (8), and let $a_3 = xa_2\bar{x}$, $b_3 = xb_2\bar{x}$. Then $[a_1, b_1] = [a_3, b_3]$, while (a_1, b_1) and (a_3, b_3) are not related by any succession of transformations of the forms A^* and B^*.

*This work was begun while both authors attended the Symposium on Infinite Group Theory at the University of Warwick, April 1978, supported by the Science Research Council. The work of the first author was supported in part by the National Science Foundation.

References

1. Burns, R. G., Edmunds, C. C., Farouqi, I. H. *On commutator equalities and stabilizers in free groups.* Canadian Math. Bull. **19** (1976) 263–267.

2. Hmelevskii, Ju. I. *Systems of equations in a free group. I.* Izv. Akad. Nauk SSSR, Ser. Mat **35** (1971) 1237–1268. (Amer. Math. Soc. translation: Math. USSR Izvestija **5** (1971) 1245–1276.)

3. Nielsen, J. *Die Isomorphismen der Allgemeinen unendlichen Gruppe mit zwei Erzeugenden.* Math. Ann. **78** (1918) 385–397.

4. Wicks, M. J. *Commutators in free products.* J. London Math. Soc. **37** (1962) 433–444.

Reference added in proof:

5. McDonough, T. P., *Root-closure in free groups*, J. London Math. Soc., **2** (1970) 191–192.

University of Michigan
Ann Arbor, Michigan 48109
University of Singapore
Singapore 1025