PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 80, Number 1, September 1980

NORMAL CLOSURE OF ONE-VARIABLE EQUATIONS IN FREE GROUPS

C. SIBERTIN-BLANC[1]

ABSTRACT. Let $w(x)$ be a one-variable equation in a free group F of finite rank. Lyndon has proved that it is possible to associate effectively to $w(x)$ the set of its solutions, whereas Appel and Lorenc have provided a simpler representation of the set inferred. In this paper, we invert the problem and demonstrate that if the elements of any set $S \subset F$ are solutions of an equation $w(x)$, then $w(x)$ belongs to the normal closure of finitely many short equations associated to S. A few consequences are given.

Let F be a free group of finite rank. A one-variable equation on F is any element of the free group $F_*\langle x\rangle$; such an equation will be written as follows in its reduced form: $w(x) = c_1x^{\varepsilon_1}c_2x^{\varepsilon_2}\cdots c_tx^{\varepsilon_t}c_{t+1}$, with $c_i \in F$, $\varepsilon_i \in \{-1, 1\}$, $t \in \mathbf{N}$. The c_i are called the coefficients of $w(x)$, t is called the degree of $w(x)$ and M, twice the maximum of the lengths of the c_i, is called the size of $w(x)$. A solution of $w(x)$ is any element ω of F such that $w(\omega) = 1$.

In what follows, a parametric word[2] on F is an expression such as $U = dS^{\alpha}h$, in which α is a parameter, d, S and h belong to F and S is cyclically reduced and not a proper power (i.e. $S = g^n$ leads to $n = \pm 1$). A value of U is the element of F resulting from substituting integer value for α.

Appel [1] has shown the following result (we keep the preceding notations):

THEOREM A. *The set of solutions of any equation on a free group is the union of*:

(A) *A finite set of solutions whose lengths are* $\leqslant 4M$.

(B) *For a finite set of parametric words, the set of values of those parametric words such that* $|S^n| > (t + 6)$, M, $n > 0$.

In both cases, it is easy to find short equations accepting these solutions:

The shortest equation accepting $\omega \in F$ as a solution is ωx^{-1}.

The shortest equation accepting infinitely many values of the parametric word $U = dS^{\alpha}h$ as solutions is $u(x) = dSd^{-1}xh^{-1}S^{-1}hx^{-1}$.

The following proposition is obvious:

Received by the editors February 16, 1979 and, in revised form, July 26, 1979.

AMS (MOS) subject classifications (1970). Primary 20E05.

Key words and phrases. One-variable equation, set of solutions, free generator, parametric word, normal closure, primitive element, recursively enumerable.

[1]The author thanks Professor Roger C. Lyndon for providing a simplified proof of Theorem 2.

[2]The more general definition of parametric words is due to Lyndon [3].

0002-9939/80/0000-0405/$02.25

PROPOSITION 1. *Let $w(x)$ and $w'(x)$ be equations on F such that $w'(x)$ belongs to the normal closure of $w(x)$ (in the free group $F_*\langle x\rangle$). Then the solutions of $w(x)$ are solutions of $w'(x)$.*

The reverse of this proposition is not true (for instance consider $u(x)^2$ and $u(x)^3$). However it is correct if we keep to the two types of short equations mentioned previously, that is to say we have the two following theorems:

THEOREM 1. *Let $w(x)$ be an equation on a free group F and ω a solution of $w(x)$. Then $w(x)$ belongs to the normal closure of ωx^{-1}.*

PROOF. Let $a_1, \ldots, a_n$ be free generators of F, $\omega \in F$ and $x \notin F$. Since $a_1, \ldots, a_n, x$ are free generators of $F_*\langle x\rangle$, F admits the presentation $(a_1, \ldots, a_n, x;\ \omega x^{-1} = 1)$. Then, for any element $w(x)$ of $F_*\langle x\rangle$, we have $w(\omega) = 1$ iff $w(x)$ belongs to the normal closure of ωx^{-1}.

THEOREM 2. *Let $w(x)$ be an equation on a free group F. Let $U = dS^{\alpha}h$ be a parametric word on F whose infinitely many values are solutions of $w(x)$. Then $w(x)$ belongs to the normal closure of $u(x) = dSd^{-1}xh^{-1}S^{-1}hx^{-1}$.*

We call a nonempty subset S of F a solution set if there exists any equation $w(x)$ on F such that S is the set of solutions of $w(x)$. Let E_S be the normal subgroup of $F_*\langle x\rangle$ made up of equations whose set of solutions contains S. We do not know if there are other partial converses to Proposition 1 than Theorems 1 and 2: if E_S is generated–as a normal subgroup–by a single element, must S either have one single element or be the set of values of a parametric word? Is $F_*\langle x\rangle / E_S$ at least finitely presented?

The proof of Theorem 2 given below is due to the referee, Roger C. Lyndon. The proof of the author was more complicated: it studies, by a combinatorial way, the manner of doing cancellations which permit to come to 1 from the word $w(dS^nh)$, where n is "great"[3]. Both these proofs are constructive inasmuch as they give the possibility of writing $w(x)$ in a basis of the normal closure of $u(x)$.

We note $CN(g)$ the normal closure of any element g of a group G. Define $w_1(x) = w(dxh)$ and $u_1(x) = u(dxh) = dSxS^{-1}x^{-1}d^{-1}$. Then "infinitely many values of the parametric word $dS^{\alpha}h$ are solutions of $w(x)$" is equivalent to "$w_1(S^n) = 1$ for infinitely many n" and $w(x) \in CN(u(x))$ is equivalent to $w_1(x) \in CN(u(dxh)) = CN([S, x])$. Thus Theorem 2 is equivalent to

PROPOSITION 2. *Let $w(x)$ be an equation on a free group F and let $S \in F$ be cyclically reduced. If $w(S^n) = 1$ for infinitely many integers n, then $w(x) \in CN([S, x])$.*

The following results from a lemma of Appel [1].

---

[3]The ground lemma of this proof is the following ($\equiv$ denotes the equality between words): Let W be a word on the generators of a free group F such that $W = 1$. Then there exist two words W_1 and W_2 such that either (1) $W \equiv W_1W_2$ where $W_1 = W_2 = 1$ or (2) $W \equiv W_1W_2W_1^{-1}$ where W_2 is of the kind (1).

LEMMA 1. *Let $a, c \in F$, a cyclically reduced. Then there exists $N > 0$ such that, for all $n \geqslant N$:*

(1) *$a^{\pm n}c$ and $a^{\pm n}ca^{\pm n}$ begin with $a^{\pm 1}$;*

(2) *$ca^{\pm n}$ and $a^{\pm n}ca^{\pm n}$ end with $a^{\pm 1}$;*

(3) *if $[a, c] \neq 1$, then $a^{\pm n}ca^{\mp n}$ begins with $a^{\pm 1}$ and ends with $a^{\mp 1}$.*

COROLLARY 1. *Let $w(x) = c_1x^{\varepsilon_1}c_2x^{\varepsilon_2} \ldots x^{\varepsilon_t}c_{t+1}$, $t \geqslant 1$, $c_i \in F$, $\varepsilon_i = \pm 1$. Let $a \in F$ be cyclically reduced and, if $-\varepsilon_{i-1} = \varepsilon_i$, assume that $[a, c_i] \neq 1$. Then there exists $L \geqslant 0$ such that, for all $|n| \geqslant L$, $w(a^n) \neq 1$.*

PROOF. Let L be twice the upper bound of the N defined by the lemma. If $|n| \geqslant L$, any occurrences of a^n in $w(a^n)$ can cancel entirely. Thus $w(a_n) \neq 1$.

PROOF OF PROPOSITION 2. Let $w(x) = c_1x^{\varepsilon_1}c_2x^{\varepsilon_2} \ldots x^{\varepsilon_t}c_{t+1}$ such that $w(S^n) = 1$ for infinitely many n. We can not have $t \leqslant 1$ unless $w(x)$ is the empty word, and we will argue by induction on t if $t \geqslant 2$. By the corollary, some $\varepsilon_{i-1} = -\varepsilon_i$ and $[S, c_i] = 1$; thus there exists some integer p such that $c_i = S^p$, and we have $[S^{\varepsilon_i \cdot n}, c_i] = 1$. Define $w_1(x)$, $w_2(x)$ and $w'(x)$ such that $w(x) = w_1(x)x^{\varepsilon_{i-1}}c_ix^{\varepsilon_i}w_2(x)$ and $w'(x) = w_1(x)c_iw_2(x)$ of degree $t' \leqslant t - 2$. Since $S^{\varepsilon_{i-1} \cdot n}c_iS^{\varepsilon_i \cdot n} = c_i$, $w'(S^n) = w(S^n) = 1$ for infinitely many n and $w'(x) \in CN([S, x])$ by induction. Now $w(x) = w'(x)w_2^{-1}(x)[S^{-p}, x^{\varepsilon_{i-1}}]w_2(x)$ belongs to $CN([S, x])$.

Theorem 2 shows that if infinitely many values of a parametric word are solutions of an equation, then all its values are solutions. This leads to the following refinement of Appel's theorem referred to at the beginning of this paper, obtained by Lorenc [2]:

COROLLARY 2. *The set of solutions of any equation on a free group is the union of:*

(A) *A finite set of solutions whose lengths are $\leqslant 4M$;*

(B) *for a finite set of parametric words, the set of all the values of these parametric words.*

COROLLARY 3. *Let F be a free group and $S \subset F$. Then the subgroup E_S of $F_*\langle x\rangle$ of equations whose set of solutions contains S is recursively enumerable. (That is to say we are able to provide a list of the elements of E_S.)*

PROOF. $E_S \neq \{1\}$ iff there exist two finite sets $\{\omega_i;\ i = 1, \ldots, k, \omega_i \in F\}$ and $\{U_i = d_iS_i^{\alpha}h_i;\ i = k + 1, \ldots, l,$ and U_i parametric word on $F\}$ such that $S \subset \{\omega_i;\ i = 1, \ldots, k\} \cup \{d_iS_i^nh_i;\ i = k + 1, \ldots, l, n \in \mathbf{Z}\}$. We can suppose $\{\omega_i;\ i = 1, \ldots, k\} \subset S$ as well as $\{n:\ d_iS_i^nh_i \in S\}$ is infinite for every i, $i = k + 1, \ldots, l$. According to Theorems 1 and 2, E_S is the intersection of the normal closures of the equations $u_i(x) = \omega_ix^{-1}$, $i = 1, \ldots, k$, and $u_i(x) = d_iS_id_i^{-1}xh_i^{-1}S_i^{-1}h_ix^{-1}$, $i = k + 1, \ldots, l$. By listing the elements of F, we can number the elements of each of these normal closures and define recursive functions f_i, $i = 1, \ldots, l$, so that the number of any $w(x)$ of $CN(u_i(x))$ is majored by $f_i(|w(x)|)$. Then we are able to give a list of the intersection of these normal closures.

Now consider the set E_S^* of the equations whose set of solutions is strictly S. For providing a list of E_S^* we must take out of E_S the equations whose solutions are not all in S. If E_S^* is not empty, there exist as below two sets such that $S = \{\omega_i;\ i = 1, \ldots, k\} \cup \{d_i S_i^n h_i;\ i = k+1, \ldots, l, n \in \mathbf{Z}\}$. Let $w(x) \in F_*\langle x\rangle$ have size M and let $\Omega = \{\omega \in F;\ |\omega| \leqslant 4M\} \setminus \{\omega_i;\ i = 1, \ldots, k\}$ and

$$\mathfrak{U} = \{U = dS^\alpha h;\ U \text{ parametric word on } F,\ |dSh| \leqslant 5M\} \setminus \{U_i;\ i = k+1, \ldots, l\}.$$

According to Appel, any solution of $w(x)$ must either belong to Ω or be a value of a parametric word of $\mathfrak{U}$ or belong to S. Thus $w(x)$ lies in E_S^* iff $w(x) \in \bigcap_1^l CN(u_i(x))$ and $w(x) \notin \bigcup_\Omega CN(\omega^{-1}x) \cup \bigcup_{U\in\mathfrak{U}} CN(dSd^{-1}xh^{-1}S^{-1}hx^{-1})$. This second condition, as well as the first one, is decidable. This proves the following:

COROLLARY 4. *Let F be a free group and $S \subset F$. Then the subset of $F_*\langle x\rangle$ of equations whose set of solutions is strictly S is recursively enumerable.*

Here are two propositions related to elements which belong to a set of free generators of $F_*\langle x\rangle$, called primitive elements of $F_*\langle x\rangle$. For this, we will refer to the two following lemmas, due to Magnus and to Steinberg, and mentioned in [**4**, p. 107]. F' denotes the derived group of F.

LEMMA M. *If F is a free group and the normal closure in F of an element q contains some primitive element p, then q is conjugate to p or to p^{-1}.*

LEMMA S.[4] *Let p and q be primitive elements of a free group F. If the intersection of their normal closures is not contained in F', then q is conjugated to p or to p^{-1}.*

PROPOSITION 3. *A power of any primitive element of $F_*\langle x\rangle$ has one solution in F at most.*

PROOF. Let $w(x)$ be primitive and $\omega \in F$ such that $w(\omega) = 1$. According to Theorem 1, $w(x)$ belongs to the normal closure of ωx^{-1}. Since $w(x)$ is a primitive element, it is conjugated to $x^{-1}\omega$ or to $\omega^{-1}x$. Thus ω is the only solution of $w(x)$.

PROPOSITION 4. *Any equation on a free group F which has two solutions at least lies in $F_*\langle x\rangle'$.*

PROOF. By Theorem 1 and Lemma S.

We may notice that there are primitive elements without solution, as well as there exist equations in $F_*\langle x\rangle'$ which have one or zero solution; let F be the free group freely generated by a and b; then $axbx^{-1}$ is primitive without solution, $[a, x][a, b]$ has no solution and the empty word is the only solution of $[x, axbxb^{-1}]$.

---

[4] This lemma is badly enunciated in [**4**] where it is not stated that p and q both have to be primitive; but this lemma becomes false if q is not primitive: $q = p^2$ is conjugate neither to p nor to p^{-1}. See [**5**].

References

1. K. I. Appel, *One-variable equations in free groups*, Proc. Amer. Math. Soc. **19** (1968), 912–919.
2. A. A. Lorencs, *Representations of sets of solutions of systems of equations with one unknown in a free group*, Dokl. Akad. Nauk SSSR **178** (1968), 290–292.
3. R. C. Lyndon, *Equations in free groups*, Trans. Amer. Math. Soc. **96** (1960), 445–457.
4. R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Springer-Verlag, Berlin, 1977.
5. A. Steinberg, *On equations in free groups*, Michigan Math. J. **18** (1971), 87–95.

Current address: 17 Rue P. Couderc, 92330 Sceaux, France