COMPOSITIO MATHEMATICA

F. B. CANNONITO
R. W. GATTERDAM

The word problem in polycyclic groups is elementary

Compositio Mathematica, tome 27, nº 1 (1973), p. 39-45
<http://www.numdam.org/item?id=CM_1973__27_1_39_0>

COMPOSITIO MATHEMATICA, Vol. 27, Fasc. 1, 1973, pag. 39-45
Noordhoff International Publishing
Printed in the Netherlands

THE WORD PROBLEM IN POLYCYCLIC GROUPS IS ELEMENTARY

F. B. Cannonito and R. W. Gatterdam

1. Introduction

It is well known that the solution of the word problem for finitely presented (henceforth 'f.p.') groups can be arbitrarily difficult in the sense that it can have any preassigned recursively enumerable degree (see Boone [2], [3], and Clapham [7]). The study of the word problem with respect to the finer degrees of the relativized Grzegorczyk hierarchy was begun by Cannonito [4] and continued by Gatterdam [8]. A comprehensive background to this work can be found in the authors' paper [5], of which a knowledge on the part of the reader is assumed. The existence of f.p. groups with word problem stricly $\mathscr{E}^n(A)$ computale in the relativized Grzegorczyk hierarchy, for $n \geqq 4$ and A, a recursively enumerable subset of the natural numbers, was shown by Gatterdam [9]. It should be observed that the degree of solvability of the word problem for a finitely generated (henceforth 'f.g.') group is an invariant of the f.g. presentation. Groups with word problem $\mathscr{E}^n(A)$ computable are said to be '$\mathscr{E}^n(A)$ standard'.

The question being considered here is in the opposite direction and stems from current efforts to locate, if possible, with respect to the Grzegorczyk hierarchy, the level of computability of the word problem in f.p. residually finite groups (see [6] for some discussion). Thus, knowing how difficult the word problem can become for f.p. groups, we ask instead how 'easy' is it for classes of f.g. groups with known solvable word problem? In particular, some classes have word problem solvable by (Kalmár) elementary functions, $\mathscr{E}^3$ in the hierarchy. These classes include finite groups, free groups, automorphism groups of f.g. free groups, braid groups and f.g. abelian groups. More recently, the authors in [6] have shown why one relator groups may not have elementary word problem. The main result of this paper is to show the word problem for polycyclic groups and, hence, f.g. nilpotent groups is elementary. Now, Auslander has shown in [1] that any polycyclic group is embeddable in $Gl(n, \mathbb{Z})$ for suitable n, and since $Gl(n, \mathbb{Z})$ is isomorphic to the automorphism group of the free group of rank n, we have immediately from [5] Corollary 3.7 that the word problem in polycyclic groups is elementary. In this paper

we derive this result by analysing the construction of a polycyclic group given by (finitely many) cyclic extensions. In this manner, we also show the computability level for a wider class of groups is elementary and demonstrate a computability level preserving construction.

2. Group Extensions

In this section we develop some basic notions concerning the computability of group extensions. The background material on extensions can be found in MacLane [11], which we use without further reference.

Consider an extension, $0 \to K \xrightarrow{\kappa} G \xrightarrow{\sigma} Q \to 1$ with both K and Q f.g. and $\mathscr{E}^3$ standard. We write the group operation in K and Q additively even though they in general will not be abelian. A departure from the MacLane approach is that we will distinguish between K and $\kappa(K) < G$.

For every $q \in Q$ let $\lambda(q)$ be a lifting into G (in general not a homomorphism) so that $\sigma\lambda(q) = 1_Q$. Then conjugation of $\kappa(K)$ by $\lambda(q)$ in G yields a homomorphism $\psi : Q \to \text{Aut } K/\text{In } K$. For $q \in Q$ let $\phi(q) \in \psi(q)$ be a choice of automorphism of K in the class $\psi(q)$. Since K is f.g. and $\mathscr{E}^3$ standard, $\phi(q)$ is $\mathscr{E}^3$ computable for fixed q (see [5]; for $k_1, \cdots, k_n$ generators of K and $w(k_1, \cdots, k_n) \in K$, $\phi(q):w$, that is, the image of w under $\phi(q)$, can be obtained from $w(\phi(q):k_1, \cdots, \phi(q):k_n)$ by a bounded minimalization and $w(\phi(q):k_1, \cdots, \phi(q):k_n)$ can be obtained from $w(k_1, \cdots, k_n)$ by an $\mathscr{E}^3$ limited recursion).

The group G is determined (up to natural isomorphism) by the $\phi(q)$ and a function $f : Q \times Q \to K$ which expresses the deviation of λ from being a homomorphism $Q \to G$ by

$$\lambda(p)+\lambda(q) =_G \kappa f(p, q)+\lambda(p, q). \tag{1}$$

The associative law in G yields

$$\phi(p):f(q, r)+f(p, qr)=_K f(p, q)+f(pq, r). \tag{2}$$

Recalling $\phi(q):k =_G \lambda(q)+k-\lambda(q)$, conjugation by the left and right side of (1) in $\kappa(K) < G$ yields

$$\phi(p) \circ \phi(q):k =_K f(p, q)+\phi(pq):k-f(p, q). \tag{3}$$

By taking $\lambda(1) = 0$ we may as well have $\phi(1) = 1_K$ and $f(q, 1) =_K 0_K = f(1, q)$ for all $q \in Q$.

Now a simple computation ([11] lemma 8.1) shows $G = \{(k, q) | k \in K, q \in Q\}$ as a set with multiplication and inversion given by

$$(k, q)+(k', q') = (k+\phi(q):k'+f(q, q'), qq'), \tag{4}$$

$$-(k, q) = (-f(q^{-1}, q)-\phi(q^{-1}):k, q^{-1}). \tag{5}$$

LEMMA: *If under the above conditions* $f: Q \times Q \to K$ *is* $\mathscr{E}^3$ *computable with respect to standard indices on* Q *and* K *then* G *is* $\mathscr{E}^4$ *standard.*

PROOF: We need $\mathscr{E}^3$ pairing functions J, M_1, M_2 (see [5]; M_1 is K and M_2 is L of [5] § 2) and $\mathscr{E}^3$ standard indices (i_1, m_1, j_1) and (i_2, m_2, j_2) of K and Q respectively (again see [5]).

Then $G = \{(k, q) | k \in K, q \in Q\}$ as a set so we define $i(G)$ by $i(k, q) = J(i_1(k), i_2(q))$. Thus $x \in i(G) \leftrightarrow M_1(x) \in i_1(K) \wedge M_2(x) \in i_2(Q)$ so $i(G)$ is $\mathscr{E}^3$ decidable.

By (4) and (5) $m: i(G) \times i(G) \to i(G)$ and $j: i(G) \to i(G)$ can be defined in terms of f and ϕ suitably encoded. Thus let $\hat{f}: i_2(Q) \times i_2(Q) \to i_1(K)$ by $\hat{f}(i_2(p), i_2(q)) = i_1 f(p, q)$ and $\hat{\phi}: i_2(Q) \times i_1(K) \to i_1(K)$ by $\hat{\phi}(i_2(q), i_1(k)) = i_1(\phi(q):k)$. We have assumed $\hat{f}$ is $\mathscr{E}^3$ computable. Postponing the computability of $\hat{\phi}$, we can encode multiplication and inversion as follows:

$$m(x, y) = J(m_1(m_1(M_1(x), \hat{\phi}(M_2(x), M_1(y))), \hat{f}(M_2(x), M_2(y))), m_2(M_2(x), M_2(y))),$$

$$j(x) = J(m_1(j_1 \hat{f}(j_2 M_2(x), M_2(x)), j_1 \hat{\phi}(j_2 M_2(x), M_1(x))), j_2 M_2(x)).$$

Thus to show G is $\mathscr{E}^4$ we need to prove $\hat{\phi}$ is $\mathscr{E}^4$ computable. It suffices to show $\hat{\phi}(x, y)$ is $\mathscr{E}^4$ for $x \in i_2(Q)$ and $y = i_1$ (a generator of K) since then a standard $\mathscr{E}^3$ bounded recursion can be used to compute $\hat{\phi}(x, y)$ for arbitrary $y \in i_1(K)$ (see [5] proof of Theorem 3.2). Now, let $x = i_2(q_0 \cdots q_\beta)$ for $q_0 \cdots q_\beta$ a freely reduced word, each q_α being a generator or inverse of a generator of Q. Since K and Q are f.g. there are finitely many values $\hat{\phi}(x, y)$ for $x = i_2$ (generator of Q or the inverse of a generator of Q) and $y = i_1$(generator of K) so $\hat{\phi}(x, y)$ is $\mathscr{E}^4$ if $\beta = 0$. By means of a recursion on β, let $x' = i_2(q_1 \cdots q_\beta)$ and $x_0 = i_2(q_0)$. Then

$$\hat{\phi}(x, y) = m_1(j_1 \hat{f}(x_0, x'), m_1(\hat{\phi}(x_0, \hat{\phi}(x', y)), \hat{f}(x_0, x'))).$$

Since this recursion has no a priori $\mathscr{E}^3$ bound, the best that can be said in general is that $\hat{\phi}$ is $\mathscr{E}^4$ computable and, hence, G is an $\mathscr{E}^4$ computable group.

To show G is $\mathscr{E}^4$ standard let $a_1, \ldots, a_s$ generate K and $a_{s+1}, \ldots, a_{s+t}$ generate Q so G is generated by

$$\{(a_\alpha, 1) | \alpha = 1, \cdots, s\} \bigcup \{(0, a_\alpha) | \alpha = s+1, \cdots, s+t\}.$$

We must show the homomorphism $\tau: \langle a_1, \cdots, a_{s+t}; \rangle \to G$ by $a_\alpha \mapsto (a_\alpha, 0)$ if $1 \leqq \alpha \leqq s$, $a_\alpha \mapsto (1, a_\alpha)$ if $s+1 \leqq \alpha \leqq s+t$, is $\mathscr{E}^4$ computable, for then G is $\mathscr{E}^4$ standard by Theorem 3.4 of [5]. The idea is to write a freely reduced word in the free group as $b_0 \cdots b_\beta$ for each b symbol a generator a_α or an inverse a_α^{-1}. Then if $\tau(b_1 \cdots b_\beta) = (k', q')$ we have

$$\tau(b_0 \cdots b_\beta) = \begin{cases} (b_0 + k', q') & \alpha \leqq s, \\ (\phi(b_0){:}k' + f(b_0, q'), b_0 q') & \alpha > s. \end{cases}$$

Thus the encoding of τ can be given by a recursion involving $\mathscr{E}^3$ computable functions.

For the interested reader we record the details of the above. The notation is that of [5] (see also [10] p. 222 ff.) as is the assumed encoding of the free group. Define

$$\delta(x) = \begin{cases} \prod_{\gamma=0}^{lhx \dot{-} 1} p_\gamma \exp(x)_{\gamma \dot{-} 1}, \text{ if } M_2((x)_0) = 1 \vee M_2((x)_0) = 2, \\ 2 \exp J(M_1((x)_0), M_2((x)_0 \dot{-} 2)) \cdot \left(\prod_{\gamma=1}^{lhx} p_\gamma \exp(x)_\gamma\right), \text{ if } M_2((x)_0) > 2; \end{cases}$$

$$\rho(x) = \begin{cases} 2 \exp J(M_1((x)_0), 2), & \text{if } M_1((x)_0) \leqq s \wedge 2 | M_2((x)_0), \\ 2 \exp J(M_1((x)_0), 1), & \text{if } M_1((x)_0) \leqq s \wedge 2 \nmid M_2((x)_0), \\ 2 \exp J(M_1((x)_0) \dot{-} s), 2), & \text{if } M_1((x)_0) > s \wedge 2 | M_2((x)_0), \\ 2 \exp J(M_1((x)_0) \dot{-} s), 1), & \text{if } M_1((x)_0) > s \wedge 2 \nmid M_2((x)_0). \end{cases}$$

Then

$$\hat{\tau}(x) = \begin{cases} J(m_1(\rho(x), M_1 \hat{\tau}\delta(x)), M_2 \hat{\tau}\delta(x)), & \text{if } M_1((x)_0) \leqq s, \\ J(m_1(\hat{\phi}(\rho(x), M_1 \hat{\tau}\delta(x)), \hat{f}(\rho(x), M_2 \hat{\tau}\delta(x))), m_2(\rho(x), M_2 \hat{\tau}\delta(x))), & \\ & \text{if } M_1((x)_0) > s. \end{cases}$$

We note that if K and Q are f.g. $\mathscr{E}^n(A)$ standard for $n \geqq 3$ then G is f.g. $\mathscr{E}^{n+1}(A)$ standard by the same proof, replacing $\mathscr{E}^3$ by $\mathscr{E}^n(A)$ and $\mathscr{E}^4$ by $\mathscr{E}^{n+1}(A)$. Of more interest are situations when the recursion involved in the compitability of $\hat{\tau}$ can be bounded by an $\mathscr{E}^3$ function so that G is $\mathscr{E}^3$ standard.

COROLLARY: *If K is f.g., $\mathscr{E}^3$ standard and Q is a f.g. free group then G is $\mathscr{E}^3$ standard.*

PROOF: In this case the extension splits, i.e., the lifting λ can be taken to be a monomorphism. Then $f(p, q) = 0$ for all $p, q \in Q$ and $\phi : Q \to \text{Aut } k$ is a homomorphism.

The recursion defining $\hat{\tau}$ becomes

$$\hat{\tau}(x) = \begin{cases} J(m_1(\rho(x), M_1 \hat{\tau}\delta(x)), M_2 \hat{\tau}\delta(x)), & \text{if } M_1((x)_0) \leqq s, \\ J(\hat{\phi}(\rho(x), M_1 \hat{\tau}\delta(x)), m_2(\rho(x), M_2 \hat{\tau}\delta(x))), & \text{if } M_1((x)_0) > s. \end{cases}$$

To show G is $\mathscr{E}^3$ standard we must show $\hat{\tau}$ is $\mathscr{E}^3$ computable. It suffices to show $M_1 \hat{\tau}$ and $M_2 \hat{\tau}$ are $\mathscr{E}^3$ computable. Since $M_2 \hat{\tau}$ is the encoding of a homomorphism from a f.g. free group to the $\mathscr{E}^3$ standard group Q, it is $\mathscr{E}^3$ computable.

To see $M_1\hat{\tau}$ is $\mathscr{E}^3$ computable first observe that $\rho(x)$ encodes either a generator or inverse of a generator. Now for u the index of a generator or inverse thereof in Q, and $w \in i_1(K)$, $\hat{\phi}(u, w)$ is $\mathscr{E}^3$ computable since K is f.g. and $\mathscr{E}^3$ standard. We must show the recursion yielding $M_1\hat{\tau}$ is $\mathscr{E}^3$ limited. For $w \in i_1(K)$ let $\zeta(w)$ denote the length of the word (relative to the standard index presentation) w encodes. Similarly for x encoding a word in $F = \langle a_1, \cdots, a_{s+t}\rangle$; let $\beta(x)$ be the length of the word. It suffices to find an $\mathscr{E}^3$ bound on $\zeta M_1\hat{\tau}$ since $M_1\hat{\tau}(x) < \rho\zeta M_1\hat{\tau}(x)\ \exp(\zeta M_1\hat{\tau}(x) \cdot J(s, 2))$. For u encoding a generator or inverse thereof of Q and v encoding a generator of K set $z = \max \zeta\hat{\phi}(u, v)$. Then for $w \in i_1(K)$, $\zeta\hat{\phi}(u, w) \leqq z \cdot \zeta(w)$. Now in the recursion defining $M_1\hat{\tau}$ either m_1 or $\hat{\phi}$ is applied. In the first case $\zeta M_1\hat{\tau}$ is bounded by its previous value plus 1 and the latter by z times its previous value. Thus $\zeta M_1\hat{\tau}(x) \leqq z \exp \beta(x)$, an $\mathscr{E}^3$ function.

COROLLARY: *If K is f.g. $\mathscr{E}^3$ standard and Q is finite then G is $\mathscr{E}^3$ standard.*

PROOF: Q being finite it is $\mathscr{E}^3$ standard, $\hat{f}$ is $\mathscr{E}^3$ computable (there being only finitely many values for the argument), and $\hat{\phi}$ is $\mathscr{E}^3$ computable (K being f.g. and $\mathscr{E}^3$ standard). The problem, as above, is to $\mathscr{E}^3$ limit $\zeta M_1\hat{\tau}$. Here let $z = \max \zeta\hat{\phi}(u, v) + \max \hat{f}(u, w)$, the maximums taken over all u, $w \in i_2(Q)$ and v encoding a generator of K. Then $\zeta M_1\hat{\tau}(x) \leqq z \exp \beta(x)$.

Observe that in the corollaries if K is assumed f.g. and $\mathscr{E}^n(A)$ standard for $n \geqq 3$ the conclusion is that G is $\mathscr{E}^n(A)$ standard.

3. Main Results

We are now ready to prove the

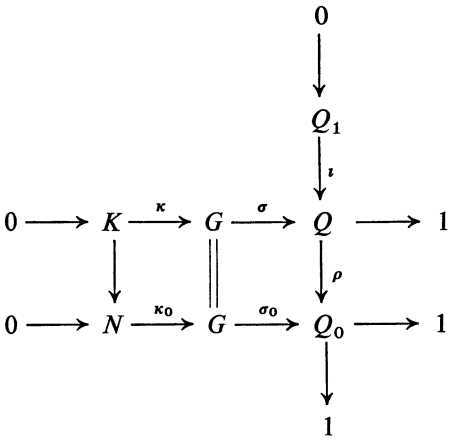
THEOREM: *Polycyclic groups have elementarily decidable word problem, i.e., are $\mathscr{E}^3$ standard.*

PROOF: If G is a polycyclic group it is necessarily f.g. and there exists a sequence $G_0, \cdots, G_n = G$ of groups such that G_0 is cyclic (hence $\mathscr{E}^3$ standard) and G_{m+1} is an extension of G_m by a cyclic group for $m < n$. Inductively assume G_m is $\mathscr{E}^3$ standard. Then it is extended either by an infinite cyclic group, i.e., a free group, or a finite cyclic group. By the corollaries of the preceding section G_{m+1} is $\mathscr{E}^3$ standard.

The theorem above can be generalized of course. Let $\mathscr{G}_0$ be the class of finite groups union that of f.g. free groups. Define $\mathscr{G}_{n+1}$ to be the class of extensions of a group in $\mathscr{G}_n$ by a group in $\mathscr{G}_0$ and $\mathscr{G} = \bigcup_{n=0}^{\infty} \mathscr{G}_n$. By the above argument the groups in $\mathscr{G}$ all are f.g. and $\mathscr{E}^3$ standard. We can say more.

THEOREM: *Let K be a f.g. $\mathscr{E}^n(A)$ standard group for $n \geqq 3$ and $Q \in \mathscr{G}$. Then any extension of K by Q is f.g. and $\mathscr{E}^n(A)$ standard.*

PROOF: K and Q are f.g. so an extension G of K by Q is f.g. Let $Q \in \mathscr{G}_m$. If $m = 0$, then G is $\mathscr{E}^3$ standard by the corollaries. Inductively if $m > 0$ then Q is an extension of $Q_1 \in \mathscr{G}_{m-1}$ by $Q_0 \in \mathscr{G}_0$. Consider



Here $\kappa_0 N = \ker \rho\sigma < G$ and G is an extension of N by $Q_0 \in \mathscr{G}_0$. We must show N is f.g. and $\mathscr{E}^n(A)$ standard. Consider the natural embedding $N/K \to G/K \cong Q$. Since $\sigma_0\kappa_0(N) = 0$, the image of N/K is in $\iota(Q_1)$. Thus we have an embedding $\zeta : N/K \to Q_1$. Now if $q \in Q_1$ there exists $g \in G$ such that $\sigma(g) = \iota(q)$. Then $\rho\sigma(g) = \rho\iota(q) = 0$ implies $g \in \kappa_0(N)$ so ζ is onto. Therefore $N/K \cong Q_1$ so N is an extension of the f.g. $\mathscr{E}^n(A)$ standard group K by $Q \in \mathscr{G}_{m-1}$ and by induction is f.g. and $\mathscr{E}^n(A)$ standard.

It should be noted that $\mathscr{G}$ contains f.g. abelian and polycyclic groups so in particular an extension of a f.g. $\mathscr{E}^n(A)$ standard group by a f.g. abelian or polycyclic group preserves the computability level.

REFERENCES

[1] L. AUSLANDER: On a problem of Phillip Hall. *Annals of Math.*, 86 (1967), 112–116.
[2] W. W. BOONE: Word problems and recursively enumerable degrees of unsolvability. *Annals of Math.*, 83 (1966), 520–591.
[3] W. W. BOONE: Word problems and recursively enumerable degrees of unsolvability. A sequel on finitely presented groups. *Annals of Math.*, 84 (1966), 49–84.
[4] F. B. CANNONITO: Hierarchies of computable groups and the word problem. *J. Symbolic Logic*, 31 (1966), 376–392.
[5] F. B. CANNONITO and R. W. GATTERDAM: The computability of group constructions, Part I. *Word Problems*, Boone, Cannonito, Lyndon eds., North-Holland Publishing Company, Amsterdam (1973).

[6] F. B. CANNONITO and R. W. GATTERDAM: *The word problem and power problem in 1-relator groups is primitive recursive* (submitted for publication).
[7] C. R. J. CLAPHAM: Finitely presented groups with word problem of arbitrary degree of insolubility. *Proc. London Math. Soc.*, 14 (1964), 633–676.
[8] R. W. GATTERDAM: *Embeddings of primitive recursive computable groups* (submitted for publication).
[9] R. W. GATTERDAM: The computability of group constructions, Part II *Bull. Australian Math. Soc.*, 8 (1973) 27–60.
[10] S. C. KLEENE: *Introduction to Metamathematics*. Van Nostrand, Princeton, New Jersey (1952).
[11] S. MACLANE: *Homology*. Springer-Verlag, Berlin (1963).

(Oblatum 7–VIII–1972)

Department of Mathematics
University of California – Irvine[1] USA
and
Department of Mathematics
University of Wisconsin – Parkside[1] USA

[1] Support for the first author by the Air Force Office of Scientific Research Grant AF-AFOSR 1321-67 and for the second author by the Wisconsin Alumni Research Fund Grant 130399 is gratefully acknowledged.