On complexity of multiplication in finite soluble groups

M.F. Newman [a], Alice C. Niemeyer [b],*

[a] Mathematical Sciences Institute, Australian National University, Canberra, ACT 0200, Australia
[b] Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics (M019), The University of Western Australia, 35 Stirling Highway, Crawley, WA 6009, Australia

A R T I C L E   I N F O

A B S T R A C T

We determine a reasonable upper bound for the complexity of collection from the left to multiply two elements of a finite soluble group by restricting attention to certain polycyclic presentations of the group. As a corollary we give an upper bound for the complexity of collection from the left in finite p-groups in terms of the group order.

© 2014 Elsevier Inc. All rights reserved.

Dedicated to the memory of Ákos Seress

1. Introduction

In studying groups using computers it is important to have practical programs for multiplication of elements. For finite soluble groups given by (finite) polycyclic presentations

* Corresponding author.
  E-mail addresses: newman@maths.anu.edu.au (M.F. Newman), Alice.Niemeyer@uwa.edu.au (A.C. Niemeyer).

this involves having practical programs for collection relative to a polycyclic presentation. See Section 2 for a description. Since the work of Vaughan-Lee [8] and that of Leedham-Green and Soicher [6] it has been known that collection from the left works well in practice. Collection from the left is the basis for multiplication in the computer algebra systems GAP [3] and MAGMA [1].

The cost of various collection strategies has been discussed in several papers, see for example [6], [4] and [5].

Leedham-Green and Soicher compared the performance of some collection strategies and did some complexity analysis on collection from the left for finite p-groups. We address a question they raised [6, p. 675] of finding for finite p-groups and, more generally finite soluble groups, polycyclic presentations which from a complexity point of view are favourable for collection from the left.

Gebhardt [4] extended the investigation of collection from the left to arbitrary polycyclic presentations. In particular, he substantially improved performance by modifying collection from the left to deal more effectively with large powers. His programs are the basis for the multiplication available in MAGMA.

Höfling [5] considered various favourable presentations.

In this paper we introduce a new kind of favourable presentation. Using these allows us to give an accessible complexity analysis for collection from the left. The theorem is stated in Section 2 and proved in Section 3. Our favourable presentations come from polycyclic series which refine series of normal subgroups with abelian sections such as the derived series. In practice, a better way of handling powers is by using repeated squaring as described by Gebhardt [4, Section 4].

Cannon et al. [2] consider other special presentations in relation to questions about finite soluble groups.

2. Preliminaries and favourable polycyclic presentations

We begin by recalling some terminology and notation.

A *finite polycyclic presentation* is a presentation $\{\mathcal{A} \mid \mathcal{R}\}$ where $\mathcal{A} = \{a_1, \ldots, a_m\}$ and $\mathcal{R}$ consists of relations in $\mathcal{A}$ of the form

$$a_i^{e_i} = v_{ii} \qquad \text{for } 1 \leq i \leq m$$
$$a_j a_i = a_i v_{ij} \quad \text{for } 1 \leq i < j \leq m,$$

where e_i is a positive integer for $1 \leq i \leq m$ and v_{ij} is a word in $\{a_{i+1}, \ldots, a_m\}$ for $1 \leq i \leq j \leq m$.

In this context it suffices to work only with non-negative words in $\mathcal{A}$, that is, words involving only letters from $\mathcal{A}$ but not their inverses. The order of the generators matters; we take $a_1 < \cdots < a_m$. As usual we use the abbreviation a^α for the concatenation of α copies of a. The words $a_1^{\alpha_1} \cdots a_m^{\alpha_m}$ for integers α_i with $0 \leq \alpha_i < e_i$ for $1 \leq i \leq m$ are the *normal* words in $\mathcal{A}$. We take the right-hand sides of the relations in $\mathcal{R}$ to be normal

words. The left-hand sides of the relations in $\mathcal{R}$ are precisely the *minimal non-normal words* in $\mathcal{A}$.

Every finite polycyclic presentation $\{\mathcal{A} \mid \mathcal{R}\}$ defines a finite soluble group with order dividing $e_1 \cdots e_m$. It is well-known that every finite soluble group has a finite polycyclic presentation. A polycyclic presentation for a finite soluble group G is *consistent* if $|G| = e_1 \cdots e_m$. In this case, every element of G can be written uniquely as a normal word.

Given a non-normal word w in $\mathcal{A}$ a *collection step* replaces a minimal non-normal subword of w with the right-hand side of the corresponding relation in $\mathcal{R}$. Collecting a word in $\mathcal{A}$ is the application of a sequence of collection steps starting at the word. Collecting a word in $\mathcal{A}$ *from the left* is the collection in which each step replaces the left-most minimal non-normal subword of the word being collected in that step. A more detailed discussion of collection and, more generally, rewriting can be found in Sims [7].

We measure complexity in a more conventional way than Leedham-Green and Soicher [6]. We estimate the number of collection steps required to collect the concatenation of two normal words to a normal word with respect to particular 'favourable' polycyclic presentations, and estimate the length of words which occur during such a collection.

A finite polycyclic presentation $\mathcal{F} = \{\mathcal{A} \mid \mathcal{R}\}$ will be called *favourable* if there is a positive integer d and a non-decreasing, surjective function $\delta : \mathcal{A} \to \{1, \ldots, d\}$ such that either v_{ii} is a_{i+1} or v_{ii} is a normal word in $\{a_k, \ldots, a_m\}$ with $\delta(a_k) > \delta(a_i)$ and for $j > i$ each v_{ij} is a normal word and equal either to v_{ij}^* or to $a_j v_{ij}^*$ where v_{ij}^* is a normal word in $\{a_k, \ldots, a_m\}$ with $\delta(a_k) > \delta(a_i)$. The integer d is the *soluble bound* of $\mathcal{F}$.

Lemma 1. *Every finite soluble group has a favourable polycyclic presentation.*

Proof. Let G be a finite soluble group. Let d be the derived length of G and let the derived series of G be $G = G^{(0)} > G^{(1)} > \cdots > G^{(d-1)} > G^{(d)} = \langle 1 \rangle$. For $1 \le \ell \le d$ choose a subset $\mathcal{A}_\ell$ in G so that $\mathcal{A}_\ell G^{(\ell)}$ is a minimal generating set for $G^{(\ell-1)}/G^{(\ell)}$ and put $\mathcal{A} = \mathcal{A}_1 \cup \cdots \cup \mathcal{A}_d$. A function δ is defined on $\mathcal{A}$ by $\delta(a) = \ell$ for $a \in \mathcal{A}_\ell$. The polycyclic presentation built on $\mathcal{A}$, in the usual way, is favourable. $\square$

Write $\mathcal{A} = \{a_1, \ldots, a_m\}$ and, for a_i in G^ℓ, write e_i for the order of a_i modulo $G^{\ell+1}$. A favourable presentation obtained from a group as in the proof is consistent and has all $e_i > 1$. We assume henceforth that the finite polycyclic presentations that occur have these properties. Note that a finite cyclic group has a favourable presentation on one generator and one relation. A finite metacyclic group may not have a favourable presentation on two generators but then it has a favourable presentation on three generators. The normal words have length at most $e_1 - 1 + \cdots + e_m - 1$ which we denote by N.

For a finite p-group we can take the e_i to be equal to p by replacing the minimality condition in the definition of $\mathcal{A}$ with choosing $\mathcal{A}$ via a polycyclic series which is a composition series refining the derived series.

Theorem. *Let $\mathcal{F} = \{\mathcal{A} \mid \mathcal{R}\}$ be a favourable polycyclic presentation with soluble bound d and maximum normal word length N. Every concatenation of two normal words in $\mathcal{A}$ can be collected from the left to a normal word in at most N^{3d-1} steps. All words occurring in the course of this collection have length at most $2N$ when $d = 1$ and at most $2(d-1)N^2$ otherwise.*

It remains an open question whether every finite soluble group has a finite polycyclic presentation and a collection using that presentation for which the number of collection steps is polynomial in the size of the input; which we are measuring by N.

3. Proof of the theorem

There is nothing to prove if either word is trivial. Let u and w be non-trivial normal words in $\mathcal{A}$. Let a_s be the first letter of w and write $w = a_s w_2$. Write $u = u_1 a_s^{\alpha_s} u_2$ where u_1 is a word in $\{a_1, \ldots, a_{s-1}\}$ and u_2 is a word in $\{a_{s+1}, \ldots, a_m\}$.

In collecting uw from the left the subword u_1 is never modified and the subword w_2 is not involved until collection of the subword $a_s^{\alpha_s} u_2 a_s$ to a normal word has been completed. As shown after the proof of Lemma 4, the theorem is a consequence of showing that the collection of the subword $a_s^{\alpha_s} u_2 a_s$ to a normal word takes at most N^{3d-2} steps and that, in context, the length of words occurring during the collection is at most $2N$ when $d = 1$ and at most $2(d-1)N^2$ otherwise.

For $d = 1$ collecting the subword $a_s^{\alpha_s} u_2 a_s$ to a normal word takes at most N steps and the length of words occurring during the collection is at most $2N$. Since the length of w is at most N, the number of steps in the collection of uw to a normal word is at most N^2. The length of words occurring during the collection remains at most $2N$.

For $d > 1$ we define the *derived* presentation $\mathcal{F}' = \{\mathcal{A}' \mid \mathcal{R}'\}$ of $\mathcal{F}$ as follows. Put $\mathcal{A}' = \{a \in \mathcal{A} \mid \delta(a) > 1\}$. Let $\mathcal{R}'$ denote the subset of all relations in $\mathcal{R}$ whose left-hand sides involve only generators in $\mathcal{A}'$. Define the function $\delta' : \mathcal{A}' \to \{1, \ldots, d-1\}$ by $\delta'(a) = \delta(a) - 1$. Clearly, δ' is non-decreasing and surjective. Then $\mathcal{F}'$ is a favourable presentation with soluble bound $d-1$. Let N' denote the maximum length of a normal word in $\mathcal{F}'$. By induction the least upper bound σ' on the number of steps required to collect the concatenation of two normal words in $\mathcal{A}'$ to a normal word is at most $N'^{(3d-4)}$ and the least upper bound λ' on the length of the words occurring during the collection is at most $2N'$ when $d = 2$ and at most $2(d-2)N'^2$ otherwise. Note $N' \leq N - 1$.

It will be convenient to write Π_1 for a normal word in $\mathcal{A}'$ and Π_r for the concatenation of r normal words in $\mathcal{A}'$; empty words are allowed. The following lemma is obvious.

Lemma 2. *For $r \geq 2$, collection from the left of Π_r to a normal word takes at most $(r-1)\sigma'$ steps and the length of words occurring is at most $\lambda' + (r-2)N'$.*

Lemma 3. *For $\delta(a) = 1$ collection from the left of $\Pi_1 a \Pi_1$ to a normal word takes at most $N' + N'\sigma'$ steps and the length of words occurring is at most $1 + \lambda' + (N' - 1)N'$.*

Proof. The collection begins with at most N' steps giving $a\Pi_{N'+1}$. All the words during these steps have length at most $1+(N'+1)N'$. Using Lemma 2 the collection is completed in at most $N'\sigma'$ further steps. The length of words during the collection is at most $1+\lambda'+(N'-1)N'$. $\quad\square$

Lemma 4. *Collection from the left of the subword $a_s^{\alpha_s}u_2a_s$ of $u_1a_s^{\alpha_s}u_2a_sw_2$ to a normal word takes at most N^{3d-2} steps and the length of words occurring is at most $2(d-1)N^2$.*

Proof. The result is obvious when $\delta(a_s)>1$. For $\delta(a_s)=1$ write $u_2=a_{t_1}\ldots a_{t_h}\Pi_1$ where $\delta(a_{t_1})=\cdots=\delta(a_{t_h})=1$; then $h\leq N-N'-1$. It takes at most $N-1$ steps to move a_s past u_2 giving

$$u_1a_s^{\alpha_s}a_sa_{t_1}\Pi_1\ldots a_{t_h}\Pi_1\Pi_{N'}w_2.$$

The length of this word is at most $2N+(N-1)N'$. When $\alpha_s<e_s-1$ the rest of the collection of $a_s^{\alpha_s}u_2a_s$ to a normal word consists of at most $N-N'-2$ stages using Lemma 3 followed by using Lemma 2 to collect $\Pi_{N'+1}$. The collection takes at most $N-1+(N-N'-2)(N'+N'\sigma')+N'\sigma'$ steps. This is at most N^{3d-2}. The length of the words occurring is at most $2N+(N-3)N'+1+\lambda'+(N'-1)N'$ when the lengths of u_1, w_2 are included; so is at most $\lambda'+2N^2$. When $\alpha_s=e_s-1$ the next step replaces $a_s^{\alpha_s}a_s$ by Π_1 or a_{s+1}. The length is at most $2N+NN'$. In the first case the rest of the collection might need $N-N'-1$ uses of Lemma 3 but still gives the stated result. In the second case it may be necessary to use up to h power relations collecting $a_t^{e_t}$ between uses of Lemma 3. Eventually one of these has the form $a_t^{e_t}=\Pi_1$. Then the rest of the collection using Lemma 3 enough times followed by using Lemma 2 gives the result. The length of the words occurring is at most $2N+(N-2)N'+1+\lambda'+(N'-1)N'$ when the lengths of u_1, w_2 are included; so is at most $\lambda'+2N^2$. $\quad\square$

Since the length of w is at most N, it follows from Lemma 4 that the number of steps in the collection of uw to a normal word is at most N^{3d-1} and the length of words occurring is at most $2N$ when $d=1$ and at most $2(d-1)N^2$ otherwise. $\quad\square$

Corollary 1. *A finite p-group G has a favourable presentation with respect to which every concatenation of two normal words can be collected from the left in at most $((p-1)\log_p|G|)^{3\log_2\log_p|G|+1}$ steps.*

Proof. Let the order of G be p^n. Let $\mathcal{F}=\{\mathcal{A}\mid\mathcal{R}\}$ be a favourable polycyclic presentation for G obtained by using a composition series refining the derived series. The maximum normal word length for $\mathcal{A}$ is at most $(p-1)n$. Moreover, the soluble bound d for $\mathcal{F}$ can be chosen to be the derived length of G. By a well-known result of P. Hall d is at most $1+\log_2(n-1)$ (e.g. [7, Corollary 9.1.11]). So by the theorem the number of steps in collection from the left is at most $((p-1)\log_p|G|)^{3\log_2\log_p|G|+1}$. $\quad\square$

Acknowledgments

References

[1] W. Bosma, J. Cannon, C. Playoust, The MAGMA algebra system. I. The user language, J. Symbolic Comput. 24 (3–4) (1997) 235–265.
[2] J.J. Cannon, B. Eick, C.R. Leedham-Green, Special polycyclic generating sequences for finite soluble groups, J. Symbolic Comput. 38 (5) (2004) 1445–1460, http://dx.doi.org/10.1016/j.jsc.2004.05.003.
[3] The GAP Group, GAP — Groups, Algorithms, and Programming, version 4.7.5, http://www.gap-system.org, 2014.
[4] V. Gebhardt, Efficient collection in infinite polycyclic groups, J. Symbolic Comput. 34 (3) (2002) 213–228.
[5] B. Höfling, Efficient multiplication algorithms for finite polycyclic groups, preprint, http://www.icm.tu-bs.de/~bhoeflin/preprints/collect.pdf, 2004, Braunschweig.
[6] C.R. Leedham-Green, L.H. Soicher, Collection from the left and other strategies, in: Computational Group Theory, Part 1, J. Symbolic Comput. 9 (5–6) (1990) 665–675.
[7] C.C. Sims, Computation with Finitely Presented Groups, Encyclopedia Math. Appl., Vol. 48, Cambridge University Press, Cambridge, 1994.
[8] M.R. Vaughan-Lee, Collection from the left, in: Computational Group Theory, Part 1, J. Symbolic Comput. 9 (5–6) (1990) 725–733.