Journal of Algebra 421 (2015) 425–430

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

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*

ARTICLE INFO

Article history:
Received 29 April 2014
Available online 8 September 2014
Communicated by William M. Kantor and Charles Leedham-Green

MSC:
primary 68Q25
secondary 20D10, 68W30

Keywords:
Collection from the left
Complexity
Finite soluble groups

ABSTRACT

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.

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).

http://dx.doi.org/10.1016/j.jalgebra.2014.08.036
0021-8693/© 2014 Elsevier Inc. All rights reserved.

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

$$\begin{aligned} a_i^{e_i} &= v_{ii} && \text{for } 1 \le i \le m \\ a_j a_i &= a_i v_{ij} && \text{for } 1 \le i < j \le m, \end{aligned}$$

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

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 $0 \le \alpha_i < e_i$ for $1 \le i \le m$ are the *normal* words in $\mathcal{A}$. We take the right-hand sides of the relations in $\mathcal{R}$ to be normal