ARTICLE IN PRESS
YJSCO:1665

Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Algorithms for polycyclic-by-finite groups ☆

S.K. Sinanan [b], D.F. Holt [a]

[a] Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom
[b] Department of Mathematics and Statistics, University of The West Indies, Saint Augustine, Trinidad and Tobago

ARTICLE INFO

Article history:
Received 27 April 2015
Accepted 8 February 2016
Available online xxxx

Keywords:
Polycyclic
Polycyclic-by-finite
Permutation
Finitely presented
Magma

ABSTRACT

A set of fundamental algorithms for computing with polycyclic-by-finite groups is presented.

Polycyclic-by-finite groups arise naturally in a number of contexts; for example, as automorphism groups of large finite soluble groups, as quotients of finitely presented groups, and as extensions of modules by groups. No existing mode of representation is suitable for these groups, since they will typically not have a convenient faithful permutation representation.

A mixed mode is used to represent elements of such a group, utilising either a power-conjugate presentation or a polycyclic presentation for the elements of the normal subgroup, and a permutation representation for the elements of the quotient.

1. Introduction

A group is *polycyclic-by-finite* if it has a normal polycyclic subgroup of finite index. That is, if it has a normal subgroup of finite index that admits a subnormal series with cyclic factors.

By a well-known theorem of P. Hall, every polycyclic-by-finite group is finitely presented — and in fact, polycyclic-by-finite groups form the largest known section-closed class of finitely presented groups. It is this fact that makes polycyclic-by-finite groups natural objects of study from the algorithmic standpoint.

☆ This research was supported by the University of Warwick Postgraduate Research Scholarship, and the Overseas Research Student Award Scheme (ORSAS). The latter is managed by Universities UK on behalf of the Department of Education and Skills of the United Kingdom.

E-mail addresses: Shavak.Sinanan@sta.uwi.edu (S.K. Sinanan), D.F.Holt@warwick.ac.uk (D.F. Holt).

URLs: https://sta.uwi.edu/fst/dms/Shavak_Sinanan.asp (S.K. Sinanan), http://homepages.warwick.ac.uk/~mareg/ (D.F. Holt).

http://dx.doi.org/10.1016/j.jsc.2016.02.008

The algorithmic decision theory of polycyclic-by-finite groups has been investigated in the theoretical context by Baumslag et al. (1991). However, from the computational standpoint, the algorithms presented by Baumslag et al. (1991) are not applicable, nor were they intended to be. In contrast, this paper explores the computational properties of polycyclic-by-finite groups from a practical perspective, detailing algorithms which lend themselves easily to computer implementation.

Specifically, the work presented in this paper aims to:

(a) Define a computationally effective representation for polycyclic-by-finite groups.
(b) Develop a set of implementable algorithms to perform fundamental computations such as element multiplication and subgroup construction, within the class of polycyclic-by-finite groups.
(c) Use the fundamental algorithms developed to design methods that perform more advanced computations such as the construction of centralisers and conjugacy testing, within the class of polycyclic-by-finite groups.

The algorithms presented here are targeted primarily at finite non-solvable groups with a large solvable (and hence, in this case, polycyclic) normal subgroup, as such groups often do not have a convenient permutation representation. Groups of this type arise naturally in many applications, such as automorphism groups of large finite solvable groups, as quotients of finitely presented groups, and as extensions of modules by groups.

The theory developed is by no means limited to the finite case. Apart from a few natural exceptions (such as computing Sylow subgroups), all of the algorithms apply equally to infinite polycyclic-by-finite groups.

Whilst there may be many different decompositions of a given polycyclic-by-finite group as an extension of a polycyclic group by a finite group, the algorithms presented in this paper are most useful for those decompositions in which the finite quotient admits a faithful permutation representation of manageable degree ($< 10^6$). Thus, it will hereinafter be assumed that the polycyclic-by-finite groups in question can be so decomposed.

Much of what is presented in the sequel requires familiarity with the already existing efficient algorithms for computing with finite permutation groups, and with polycyclic groups. The standard references for computation with permutation groups are Sims (1970, 1971), and Seress (2003). The notation used in this paper is consistent with the latter.

Polycyclic groups form a broad class of finitely presented groups in which extensive computation is possible. In the finite case, solvability is equivalent to polycyclicity, and the literature on algorithms for computing with finite solvable groups is extensive. See Laue et al. (1984), Mecky and Neubüser (1989), Glasby and Slattery (1990). Computing with infinite polycyclic groups is more cutting-edge; for excellent accounts, see Sims (1994, ch. 9), Eick (2001), and Holt et al. (2005, ch. 8). The notation used in this paper is consistent with the latter.

Let E be a polycyclic-by-finite group, and suppose that there is a black-box representation of E on the computer. Let $N \trianglelefteq E$ be polycyclic, and assume that $G = E/N$ admits a faithful permutation representation of manageable degree. Concretely, the central goal of the theory is to set up machinery so that elements of E can be manipulated by performing operations only within N and G, without appealing to the existing representation of E.

On the other hand, although the algorithms described here are designed for situations where one is unable to perform arithmetic in E, there may nevertheless be instances in which it would be efficient to be able to do this; and similar methods to those presented here may be applied to such groups. This happens, for example, in dealing with some types of large matrix groups over finite fields as described in Hulpke (2013).

2. Multiplication

This section contains a detailed description of a mode by which elements of a given polycyclic-by-finite group may be represented on the computer, and a strategy for multiplication of elements represented in this manner.

Please cite this article in press as: Sinanan, S.K., Holt, D.F. Algorithms for polycyclic-by-finite groups. J. Symb. Comput. (2016), http://dx.doi.org/10.1016/j.jsc.2016.02.008