Journal of Algebra 421 (2015) 234–259

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Algorithms for arithmetic groups with the congruence subgroup property

A.S. Detinko [a], D.L. Flannery [a,*], A. Hulpke [b]

[a] *School of Mathematics, Statistics and Applied Mathematics, National University of Ireland, Galway, Ireland, United Kingdom*
[b] *Department of Mathematics, Colorado State University, Fort Collins, CO 80523-1874, USA*

ARTICLE INFO

Article history:
Received 25 April 2014
Available online 18 September 2014
Communicated by William M. Kantor and Charles Leedham-Green

Keywords:
Algorithm
Arithmetic group
Congruence subgroup property
Orbit-stabilizer problem

ABSTRACT

We develop practical techniques to compute with arithmetic groups $H \leq \mathrm{SL}(n, \mathbb{Q})$ for $n > 2$. Our approach relies on constructing a principal congruence subgroup in H. Problems solved include testing membership in H, analyzing the subnormal structure of H, and the orbit-stabilizer problem for H. Effective computation with subgroups of $\mathrm{GL}(n, \mathbb{Z}_m)$ is vital to this work. All algorithms have been implemented in GAP.

Dedicated to the memory of Ákos Seress

In [8–10] we established methods for computing with finitely generated linear groups over an infinite field, based on the use of congruence homomorphisms. These have been applied to test virtual solvability and answer questions about solvable-by-finite (SF) linear groups.

Computing with finitely generated linear groups that are not SF is a largely unexplored topic. Significant challenges exist: these groups comprise a wide class in which

* Corresponding author.
E-mail addresses: alla.detinko@nuigalway.ie (A.S. Detinko), dane.flannery@nuigalway.ie (D.L. Flannery), hulpke@math.colostate.edu (A. Hulpke).

http://dx.doi.org/10.1016/j.jalgebra.2014.08.027
0021-8693/© 2014 Elsevier Inc. All rights reserved.

certain algorithmic problems are undecidable [6, Section 3]. We may be more confident of progress if we restrict ourselves to arithmetic subgroups of linear algebraic groups. Decision problems for such groups were investigated by Grunewald and Segal [14]; see also [7]. We note renewed activity focussed on deciding arithmeticity [28].

This paper is a starting point for computation with semisimple arithmetic groups that have the congruence subgroup property (CSP). A prominent example is $\varGamma_n = \mathrm{SL}(n, \mathbb{Z})$ for $n \geq 3$. Recall that $H \leq \mathrm{SL}(n, \mathbb{Q})$ is arithmetic if $\varGamma_n \cap H$ has finite index in both H and $\varGamma_n$ (in particular, finite index subgroups of $\varGamma_n$ are arithmetic). Each arithmetic group $H \leq \mathrm{SL}(n, \mathbb{Q})$ contains a principal congruence subgroup $\varGamma_{n,m}$ for some m, namely the kernel of the congruence homomorphism $\varGamma_n \to \mathrm{SL}(n, \mathbb{Z}_m)$ induced by natural surjection $\mathbb{Z} \to \mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ [3,23]. So if we know that $\varGamma_{n,m} \leq H$ then we can transfer much of the computing to $\mathrm{SL}(n, \mathbb{Z}_m)$, for which efficient machinery is available [17]. We give a method to construct $\varGamma_{n,m}$ in H. This implies decidability of membership testing and other fundamental problems.

We pay special attention to subnormality and the orbit-stabilizer problem. Aside from their computational importance, these were the earliest questions considered for arithmetic groups. The study of subnormal subgroups of $\varGamma_n$ originated in the late 19th century and led up to formulation of the Congruence Subgroup Problem. In turn, the solution of that problem used knowledge of $\varGamma_n$-orbits in $\mathbb{Q}^n$ [18, §17].

The paper is organized as follows. Section 1 provides background on arithmetic groups: basic facts; material about principal congruence subgroups (their generating sets, construction, and maximality); and subnormal structure. Section 2 details relevant theory of matrix groups over $\mathbb{Z}_m$ and computing in $\mathrm{GL}(n, \mathbb{Z}_m)$. Then in Section 3 we give a suite of algorithms for arithmetic groups in $\varGamma_n$. After verifying decidability, we describe computing a maximal principal congruence subgroup; membership testing; and aspects of subnormality, e.g., testing whether an arithmetic group $H \leq \varGamma_n$ is subnormal or normal, and constructing the normal closure of a subgroup of $\varGamma_n$. In Section 4 we solve the orbit-stabilizer problem for arithmetic groups in $\varGamma_n$ acting on $\mathbb{Q}^n$. Our solution draws on a comprehensive description of $\mathbb{Z}^n$-orbits and stabilizers for a principal congruence subgroup. Section 5 shows how to extend results from $\varGamma_n$ to $\mathrm{SL}(n, \mathbb{Q})$. Finally, we examine the performance of our GAP [13] implementation of the algorithms.

We remark that the scope of this paper may be widened to other groups with the CSP, such as $\mathrm{Sp}(2m, \mathcal{O}_{\mathbb{P}})$ or $\mathrm{SL}(n, \mathcal{O}_{\mathbb{P}})$ for $m \geq 2$ and $n > 2$, where $\mathcal{O}_{\mathbb{P}}$ is the ring of integers of a number field $\mathbb{P}$ that is not totally imaginary [3].

1. Arithmetic subgroups of SL$(n, \mathbb{Q})$: background

1.1. Preliminaries

Let R be a commutative ring with 1, and $I \subseteq R$ be an ideal. The natural surjection $R \to R/I$ induces a congruence homomorphism $\varphi_I : \mathrm{Mat}(n, R) \to \mathrm{Mat}(n, R/I)$. Let $G_n = \mathrm{GL}(n, R)$ and $\varGamma_n = \mathrm{SL}(n, R)$. The kernel of φ_I on $\varGamma_n$ or G_n is a *principal con-*