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/

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 $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$ for $n \geq 3$. Recall that $H \leq \mathrm{SL}(n, \mathbb{Q})$ is arithmetic if $\Gamma_n \cap H$ has finite index in both H and Γ_n (in particular, finite index subgroups of Γ_n are arithmetic). Each arithmetic group $H \leq \mathrm{SL}(n, \mathbb{Q})$ contains a principal congruence subgroup $\Gamma_{n,m}$ for some m, namely the kernel of the congruence homomorphism $\Gamma_n \to \mathrm{SL}(n, \mathbb{Z}_m)$ induced by natural surjection $\mathbb{Z} \to \mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ [3,23]. So if we know that $\Gamma_{n,m} \leq H$ 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 $\Gamma_{n,m}$ 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 Γ_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 Γ_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 Γ_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 $H \leq \Gamma_n$ is subnormal or normal, and constructing the normal closure of a subgroup of Γ_n. In Section 4 we solve the orbit-stabilizer problem for arithmetic groups in Γ_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 Γ_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 $\mathrm{SL}(n, \mathbb{Q})$: 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 $\Gamma_n = \mathrm{SL}(n, R)$. The kernel of φ_I on Γ_n or G_n is a *principal con-*

gruence subgroup (PCS) *of level I*. Such a subgroup of Γ_n will be denoted $\Gamma_{n,I}$. We set $\Gamma_{n,R} = \Gamma_n$. If $R = \mathbb{Z}$ then $R/I = \mathbb{Z}_m$ for some non-negative integer m, and the subscript 'I' is replaced by 'm'.

For computational purposes, Γ_n and G_n should be finitely generated, and proper quotients of R should be finite. The latter is true if $n > 2$ and $R = \mathcal{O}_{\mathbb{P}}$ or R is the univariate polynomial ring $\mathbb{F}_q[\mathrm{x}]$ over the finite field $\mathbb{F}_q$ of size q. These are two major types of ambient ring R encountered when computing with finitely generated linear groups.

Define $t_{ij}(a) = 1_n + e_{ij}(a)$, where $e_{ij}(a) \in \mathrm{Mat}(n, R)$ has a in position (i, j) and zeros everywhere else. The matrices $t_{ij}(a)$ for distinct i, j are *transvections*. The subgroup

$$E_{n,I} = \langle t_{ij}(a) : a \in I,\ 1 \le i, j \le n,\ i \ne j \rangle$$

of $\Gamma_{n,I}$ is the *elementary group of level I*. We write e_{ij}, t_{ij}, E_n for $e_{ij}(1)$, $t_{ij}(1)$, $E_{n,R}$ respectively.

Lemma 1.1.

(i) *For all $i \ne j$, $[t_{ij}(a), t_{ji}(b)] = 1_n + e_{ij}(a^2b) - e_{ji}(ab^2) + e_{ii}(ab + a^2b^2) - e_{jj}(ab)$.*
(ii) *If i, j, k are pairwise distinct then $[t_{ij}(a), t_{jk}(b)] = t_{ik}(ab)$ and $[t_{ij}(a), t_{ki}(b)] = t_{kj}(-ab)$.*
(iii) *If $i \ne l$ and $j \ne k$ then $t_{ij}(a)$ commutes with $t_{kl}(b)$.*

Proposition 1.2. *In each of the following situations, $\Gamma_n = E_n$:* (i) *$n \ge 2$ and R is Euclidean or semi-local;* (ii) *$n \ge 3$ and R is a Hasse domain of a global field.*

Proof. See [16, 4.3.9, pp. 172–173]. □

Remark 1.3. $\mathcal{O}_{\mathbb{P}}$ is a Hasse domain of a global field, $\mathbb{F}_q[\mathrm{x}]$ is Euclidean, and $\mathbb{Z}_m$ is semi-local.

Proposition 1.2 implies that φ_m maps $\mathrm{SL}(n, \mathbb{Z})$ onto $\mathrm{SL}(n, \mathbb{Z}_m)$. However, $\varphi_I : \mathrm{GL}(n, R) \to \mathrm{GL}(n, R/I)$ may not be surjective.

Proposition 1.4. *Let $R = \mathcal{O}_{\mathbb{P}}$ or $\mathbb{F}_q[\mathrm{x}]$. If $n > 2$ or $R = \mathcal{O}_{\mathbb{P}}$ then E_n, Γ_n, and G_n are finitely generated. None of the groups E_2, Γ_2, or G_2 is finitely generated when $R = \mathbb{F}_q[\mathrm{x}]$.*

Proof. If $n \ge 3$ then $\Gamma_n = E_n$ is finitely generated by [16, 4.3.11, p. 174]; hence so too is G_n, by [16, 1.2.17, p. 29] and Dirichlet's unit theorem. See [16, 4.3.16, p. 175] and subsequent comments for the remaining claims. □

The notation $A \le_f B$ means that A is of finite index in the group B. For $n \ge 3$, $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$ has the *congruence subgroup property*: $H \le_f \Gamma_n$ is equivalent to H containing some $\Gamma_{n,m}$ [3,23]. On the other hand, Γ_2 does not have the CSP [31, §1.1].

1.2. Generators of congruence subgroups

Let $R = \mathbb{Z}$. We first discuss generating sets for G_n and Γ_n, and thus for their homomorphic images $\overline{G}_n = \mathrm{GL}(n, \mathbb{Z}_m)$, $\overline{\Gamma}_n = \mathrm{SL}(n, \mathbb{Z}_m)$.

By Lemma 1.1 (ii), the transvections $t_{12}, \dots, t_{1n}, t_{21}, \dots, t_{n1}$ constitute a generating set for $\Gamma_n = E_n$. In fact Γ_n has a generating set of minimal size 2: t_{12} and

$$\begin{pmatrix} 0 & 1_{n-1} \\ (-1)^{n-1} & 0 \end{pmatrix};$$

see [27, p. 107]. Adding the diagonal matrix $\mathrm{diag}(-1, 1, \dots, 1)$ produces a generating set for G_n of size 3. Similarly, two generators of $\overline{\Gamma}_n$, together with all diagonal matrices $\mathrm{diag}(\alpha, 1, \dots, 1)$ as α runs over a generating set for the unit group $\mathbb{Z}_m^*$ of $\mathbb{Z}_m$, generate $\overline{G}_n$. If $m = 2$ or an odd prime power then $\overline{G}_n$ is 2-generated. For all $k \geq 3$, $\mathrm{GL}(n, \mathbb{Z}_{2^k})$ is 4-generated, and $\mathrm{GL}(n, \mathbb{Z}_4)$ is 3-generated.

The normal closure of A in B is denoted A^B. Let (k, l) be the permutation matrix obtained by swapping rows k and l of 1_n.

Lemma 1.5. *For any $i \neq j$, $E_{n,m}^{\Gamma_n} = \langle t_{ij}(m) \rangle^{\Gamma_n}$.*

Proof. Put $N = \langle t_{ij}(m) \rangle^{\Gamma_n}$. We prove that $t_{kl}(m) \in N$ for all $k \neq l$. By Lemma 1.1 (ii),

$$t_{kj}(m) = t_{ij}(m) t_{ij}(-m)^{t_{ki}}, \quad k \neq j, i;$$

so $t_{kj}(m) \in N$. Then $t_{kl}(m) = [t_{kj}(m), t_{jl}] \in N$ if $k, l \neq j$. Since $t_{kl}(m) = t_{lk}(-m)^{(k,l)d}$ where $d = \mathrm{diag}(1, \dots, 1, -1, 1, \dots, 1)$ with -1 in position k, this concludes the proof. □

Proposition 1.6. *If $n \geq 3$ and $i \neq j$ then $\Gamma_{n,m} = \langle t_{ij}(m) \rangle^{\Gamma_n} = E_{n,m}^{\Gamma_n}$ (hence $\Gamma_{n,m} = E_{n,m}^{G_n}$).*

Proof. See [3], [4], or [23]. □

Remark 1.7. For $n, m > 1$, $E_{n,m}$ is not normal in Γ_n.

Remark 1.8. $E_{n,m_1} \leq E_{n,m_2} \Leftrightarrow \Gamma_{n,m_1} \leq \Gamma_{n,m_2} \Leftrightarrow m_2 \mid m_1$.

A PCS in $\overline{\Gamma}_n$ for $n \geq 3$ is the image under φ_m of a PCS in Γ_n.

Corollary 1.9. *Let I be an ideal of $\mathbb{Z}_m$, so $\mathbb{Z}_m/I \cong \mathbb{Z}_a$ for some divisor a of m. If $n \geq 3$ then the kernel $\overline{\Gamma}_{n,a}$ of φ_I on $\overline{\Gamma}_n = \mathrm{SL}(n, \mathbb{Z}_m)$ is*

$$\{1_n + ax \in \overline{\Gamma}_n \mid x \in \mathrm{Mat}(n, \mathbb{Z}_m)\} = \varphi_m(\Gamma_{n,a}) = E_{n,a}^{\overline{\Gamma}_n}.$$

Furthermore, $\overline{\Gamma}_{n,a} = \langle t_{ij}(a) \rangle^{\overline{\Gamma}_n} = \langle t_{ij}(a) \rangle^{\overline{G}_n}$ for any i and $j \neq i$.

Proposition 1.10. *If $n \geq 3$ then $\Gamma_{n,m}$ has generating set*

$$\{t_{ij}(m)^g \mid 1 \leq i < j \leq n,\ g \in \Sigma\} \tag{1}$$

where

$$\Sigma = \{1_n, (k,l), 1_n - 2e_{kk} - 2e_{k+1,k+1} + e_{k+1,k} \mid 1 \leq k < l \leq n\}.$$

Proof. See [32]. □

We emphasize that the number of generators in (1) does not depend on m. The minimal size of a generating set for $\Gamma_{n,m}$ is unknown. However, by Lemma 2.10 below, this size can be no less than $n^2 - 1$. As Professor A. Lubotzky has pointed out to us, [29, Theorem 1] and Lemma 2.10 imply that $\Gamma_{n,m}$ has a generating set of size $n^2 + 2$. In [20] it is conjectured that $\Gamma_{n,m}$ for $n \geq 3$ contains a 2-generator subgroup of finite index (cf. [19, p. 412]). If the conjecture is true then $\Gamma_{n,m}$ is $(n^2 + 1)$-generated.

Let $\min(H)$ denote the size of a minimal generating set of H. Although $\min(H)$ can be arbitrarily large [32, pp. 355–356], we have

Lemma 1.11. *Suppose that $n \geq 3$ and $\Gamma_{n,m} \leq H \leq \Gamma_n$. Then $\min(H)$ is bounded above by a function of n, m only.*

Proof. This is clear from Proposition 1.10 and the fact that $|H : \Gamma_{n,m}| \leq |\mathrm{SL}(n, \mathbb{Z}_m)|$. □

1.3. Constructing a PCS in an arithmetic subgroup

Let $n \geq 3$. Our overall strategy rests on knowing some $\Gamma_{n,m}$ in the arithmetic group $H \leq \Gamma_n$. We show that such a PCS can always be constructed.

Proposition 1.12. *$\Gamma_{n,m^2} \leq E_{n,m}$; so $|\Gamma_n : E_{n,m}|$ is finite.*

Proof. Let $p_{ij} = t_{ij}(m)$ and $s_{ij} = t_{ij}(m^2)$. Then Γ_{n,m^2} is generated by the s_{ij} for $i < j$ and their conjugates as in Proposition 1.10. Our goal is to prove that these all lie in $E_{n,m}$, i.e., that they can be expressed as words in the p_{ij}. Since $s_{ij}^{(k,l)} = p_{i'j'}^m$ where $i' = i^{(k,l)}$ and $j' = j^{(k,l)}$, it suffices to consider conjugation by $c_l = 1_n - 2e_{ll} - 2e_{l+1,l+1} + e_{l+1,l}$ for $l < n$. Furthermore, if $l, l+1 \notin \{i,j\}$ then s_{ij} and c_l commute: thus it suffices to consider conjugation of s_{ij} by c_i, c_{i-1}, c_j, c_{j-1}.

First we suppose that the conjugating element has index i or $i-1$. For $j = i+1$ and $a \notin \{i, i+1\}$,

$$s_{ij}^{c_i} = p_{ai}^{-1} p_{aj} p_{ia}^{-1} p_{ja}^{-1} p_{aj}^{-1} p_{ai} p_{ja} p_{ia} = [p_{aj}^{-1} p_{ai}, p_{ja} p_{ia}]. \tag{2}$$

If $j \neq i+1$ we have

$$s_{ij}^{c_i} = \left(p_{i+1,j}^{-1}\right)^{m-1} p_{i,i+1} p_{i+1,j}^{-1} p_{i,i+1}^{-1}. \tag{3}$$

For $j \neq i-1$,

$$s_{ij}^{c_{i-1}} = p_{i,i-1} p_{i-1,j}^{-1} p_{i,i-1}^{-1} p_{i-1,j} = \left[p_{i,i-1}^{-1}, p_{i-1,j}\right], \tag{4}$$

while $s_{i,i-1}$ and c_{i-1} commute.

Now suppose that the index of the conjugating element is j or $j-1$. For $j \neq i+1$,

$$s_{ij}^{c_{j-1}} = p_{j-1,j} p_{i,j-1} p_{j-1,j}^{-1} p_{i,j-1}^{m-1}. \tag{5}$$

If $j = i+1$ then $c_{j-1} = c_i$ and (2) applies.

If $i \neq j+1$ then

$$s_{ij}^{c_j} = p_{j+1,j}^{-1} p_{i,j+1}^{-1} p_{j+1,j} p_{i,j+1} = [p_{j+1,j}, p_{i,j+1}], \tag{6}$$

and if $i = j+1$, again as noted above, $s_{ij} = s_{i,i-1}$ and $c_j = c_{i-1}$ commute. $\square$

The group Γ_n has a (finite) presentation $\langle t_{ij}, 1 \leq i, j \leq n, i \neq j \mid \mathcal{R}\rangle$ where $\mathcal{R}$ consists of all commutator relations $[t_{ij}, t_{km}] = 1$, $[t_{ij}, t_{jk}] = t_{ik}$ from Lemma 1.1 (ii) and (iii), with a single extra relation $(t_{12} t_{21}^{-1} t_{12})^4 = 1$ [25, Corollary 10.3].

Lemma 1.13. *Given $H \leq_f \Gamma_n$ we can find an elementary group in H.*

Proof. Express each generator of H as a product of transvections (for which see, e.g., [18, p. 99]). Then the Todd–Coxeter procedure with input Γ_n and H terminates, returning $m = |\Gamma_n : H|$. So for all i, j and known l we have $t_{ij}(l) = t_{ij}(1)^l \in H$ ($l = \mathrm{lcm}\{1, \ldots, m\}$ say). Hence $E_{n,l} \leq H$. $\square$

Using Proposition 1.12, we rescue one item (slightly generalized) from the proof of Lemma 1.13.

Lemma 1.14. *If $|\Gamma_n : H| \leq m$ then $\Gamma_{n,l^2} \leq H$ where $l = \mathrm{lcm}\{1, \ldots, m\}$.*

Proposition 1.12 and Lemma 1.13 yield the promised

Corollary 1.15. *Construction of a PCS in $H \leq_f \Gamma_n$ is decidable.*

1.4. Maximal congruence subgroups

In this subsection $n \geq 3$ and $G_n = \mathrm{GL}(n, \mathbb{Z})$.

Lemma 1.16. *Let m_1, m_2 be positive integers, $m = \gcd(m_1, m_2)$, and $l = \mathrm{lcm}(m_1, m_2)$. Then*

(i) $\Gamma_{n,m_1}\Gamma_{n,m_2} = \Gamma_{n,m}$.
(ii) $\Gamma_{n,m_1} \cap \Gamma_{n,m_2} = \Gamma_{n,l}$.

Proof. (i) For $x \in \Gamma_n$ and integers a, b such that $am_1 + bm_2 = m$,

$$t_{ij}(m)^x = \left(t_{ij}(m_1)^x\right)^a \cdot \left(t_{ij}(m_2)^x\right)^b \in \Gamma_{n,m_1}\Gamma_{n,m_2}.$$

Thus $\Gamma_{n,m} = \Gamma_{n,m_1}\Gamma_{n,m_2}$ by Proposition 1.6.

(ii) Certainly $\Gamma_{n,l} \leq \Gamma_{n,m_1} \cap \Gamma_{n,m_2}$. The reverse containment is just the Chinese Remainder Theorem. □

Corollary 1.17. *If $H \leq_f G_n$ then H contains a unique maximal PCS (of Γ_n): there is a positive integer m such that $\Gamma_{n,m} \leq H$, and $\Gamma_{n,k} \leq H \Rightarrow \Gamma_{n,k} \leq \Gamma_{n,m}$.*

Remark 1.18. If H has maximal PCS $\Gamma_{n,m}$ and $\gcd(k,m) = 1$ then $\varphi_k(H) = \mathrm{SL}(n, \mathbb{Z}_k)$. Hence we know ν such that $\varphi_p(H) = \mathrm{SL}(n, p)$ for all primes $p > \nu$; cf. the query raised at the foot of [21, p. 126].

Remark 1.19. Although H similarly contains a unique maximal elementary subgroup $E_{n,m}$, the Γ_n-normal closure of $E_{n,m}$ need not be the maximal PCS in H, nor even be in H.

Remark 1.20. Lemma 1.14 provides an upper bound on m such that $\Gamma_{n,m}$ is the maximal PCS of an arithmetic group in Γ_n; cf. [22, Proposition 6.1.1, p. 115].

Lemma 1.21. *Each subgroup of $\overline{G}_n = \mathrm{GL}(n, \mathbb{Z}_m)$ contains a (perhaps trivial) unique maximal PCS of $\overline{\Gamma}_n = \mathrm{SL}(n, \mathbb{Z}_m)$. In more detail, suppose that $\Gamma_{n,m} \leq H \leq \Gamma_n$ and $\Gamma_{n,r}$ is the maximal PCS in H; then $\overline{\Gamma}_{n,r} = \varphi_m(\Gamma_{n,r})$ is the maximal PCS in $\overline{H} = \varphi_m(H)$.*

Proof. Since $\Gamma_{n,m} \leq \Gamma_{n,r}$, we have that r divides m, and so $\overline{\Gamma}_{n,r}$ is a PCS in $\overline{H}$. Corollary 1.9 tells us that each PCS in $\overline{H}$ has the form $\overline{\Gamma}_{n,k} = \varphi_m(\Gamma_{n,k})$ for some $k \mid m$. Moreover $\Gamma_{n,k} \leq H$, because H contains $\ker \varphi_m$. Hence $\overline{\Gamma}_{n,r}$ is as claimed. □

1.5. Subnormal structure

Let $Z_{n,I}$ denote the full preimage of the center (scalar subgroup) of $\mathrm{GL}(n, R/I)$ in $G_n = \mathrm{GL}(n, R)$ under φ_I. As per [33, p. 166], the *level* $\ell(h)$ of $h = (h_{ij}) \in G_n$ is the ideal of R generated by

$$\{h_{ij} \mid i \neq j,\ 1 \leq i, j \leq n\} \cup \{h_{ii} - h_{jj} \mid 1 \leq i, j \leq n\}.$$

Then $\ell(A) := \sum_{a \in A} \ell(a)$ for $A \subseteq G_n$. So $\ell(A)$ is the smallest ideal I such that $A \subseteq Z_{n,I}$. When R is a principal ideal ring we write b in place of $I = bR$. For $R = \mathbb{Z}$ or $\mathbb{Z}_m$, $\ell(A)$

may be defined unambiguously as the non-negative integer or integer modulo m that generates $\ell(A)$; e.g., $\ell(Z_{n,k}) = \ell(\varGamma_{n,k}) = k$.

Lemma 1.22. *If $H = \langle S \rangle \leq G_n$ then $\ell(H) = \ell(S)$.*

Proof. It is evident from the definitions that $\ell(S) \subseteq \ell(H)$ and $\ell(ab) \subseteq \ell(a) + \ell(b)$ for $a, b \in G_n$. Since also $\ell(a) = \ell(a^{-1})$ by [33, Lemma 1], $\ell(H) \subseteq \ell(S)$ as required. $\square$

From now on in this subsection, $n \geq 3$ and $R = \mathbb{Z}$ or $\mathbb{Z}_m$. We write $H \operatorname{sn} G$ to denote that $H \leq G$ is subnormal. The *defect* of H is the least d such that there exists a series $H = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{d-1} \trianglelefteq H_d = G$.

Theorem 1.23. *$H \operatorname{sn} G_n$ if and only if*

$$\varGamma_{n,k^e} \leq H \leq Z_{n,k} \tag{7}$$

for some k, e. If (7) holds then $d \leq e+1$ where d is the defect of H, and the least possible e is bounded above by a function of n and d only.

Proof. See [33, Corollary 3]. $\square$

Although non-scalar subnormal subgroups of $\mathrm{GL}(n, \mathbb{Z})$ have finite index, this is not true for $n = 2$; the normal closure of $E_{2,m}$ in $\mathrm{SL}(2, \mathbb{Z})$ has infinite index [23, p. 31].

Theorem 1.24. *Let H be a subgroup of G_n of level $l \geq 1$, with maximal PCS $\varGamma_{n,r}$. Then $H \operatorname{sn} G_n$ if and only if $r \mid l^e$ for some e. In that event, the defect of H is bounded above by $e' + 1$ where e' is the least such e.*

Proof. If H is subnormal then $lR \subseteq kR$ and $\varGamma_{n,k^e} \leq \varGamma_{n,r}$ for k, e as in Theorem 1.23; so $k \mid l$ and $r \mid k^e$. Conversely, if $r \mid l^e$ then H satisfies (7) with $k = l$. $\square$

Lemma 1.25. *(See [33, p. 165].) $Z_{n,l}/\varGamma_{n,l^e}$ is nilpotent of class at most e.*

We now consider normality.

Lemma 1.26. *If $\varGamma_{n,l} \leq H \leq Z_{n,l}$ then $H \trianglelefteq G_n$ and $l = \ell(H) =$ the level of the maximal PCS in H.*

Proof. We first observe that $l = \ell(\varGamma_{n,l}) \geq \ell(H) \geq \ell(Z_{n,l}) = l$. Let $\varGamma_{n,r}$ be the maximal PCS in H. Then $r \mid l$; and $l \mid r$ because $\varGamma_{n,r} \leq Z_{n,l}$. $\square$

Lemma 1.27. *Suppose that $H \leq G_n$ has level l. Then*

(i) $\varGamma_{n,l} \leq H^{G_n} \leq Z_{n,l}$.
(ii) $H^{G_n} = \langle H, \varGamma_{n,l} \rangle$.

Proof. (i) The inclusion $H^{G_n} \leq Z_{n,l}$ is clear. If $h \in H$ has level a then $t_{12}(a) \in \langle h \rangle^{G_n}$ by Theorems 1 and 4 of [5]. As a consequence, $t_{12}(l) \in H^{G_n}$. Now this part is assured by Proposition 1.6 and Corollary 1.9.

(ii) Let $L = \langle H, \Gamma_{n,l} \rangle$. Since $L \trianglelefteq G_n$ (Lemma 1.26), $H^{G_n} \leq L$. Also $L \leq H^{G_n}$ by (i). □

Corollary 1.28. *$H \trianglelefteq G_n$ if and only if $\ell(H)$ is the level of the maximal PCS in H.*

Proposition 1.29. *Lemma 1.27 remains true with G_n replaced by $\Gamma_n = \mathrm{SL}(n, R)$. That is, $H^{\Gamma_n} = H^{G_n}$, and so $H \leq \Gamma_n$ is normal in Γ_n precisely when it is normal in G_n.*

2. Matrix groups over $\mathbb{Z}_m$

2.1. Relevant theoretical results

Let $m = p_1^{k_1} \cdots p_t^{k_t}$ where the p_i are distinct primes and $k_i \geq 1$. We define a ring isomorphism $\chi : \mathbb{Z}_m \to \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{k_t}}$ by $\chi(a) = (a_1, \ldots, a_t)$ where $0 \leq a \leq m-1$, $0 \leq a_i \leq p_i^{k_i} - 1$, and $a_i \equiv a \bmod p_i^{k_i}$.

Lemma 2.1.

(i) *The map χ extends to an isomorphism of $\mathrm{Mat}(n, \mathbb{Z}_m)$ onto $\bigoplus_{i=1}^t \mathrm{Mat}(n, \mathbb{Z}_{p_i^{k_i}})$, which restricts to isomorphisms $\mathrm{GL}(n, \mathbb{Z}_m) \to \bigtimes_{i=1}^t \mathrm{GL}(n, \mathbb{Z}_{p_i^{k_i}})$ and $\mathrm{SL}(n, \mathbb{Z}_m) \to \bigtimes_{i=1}^t \mathrm{SL}(n, \mathbb{Z}_{p_i^{k_i}})$.*

(ii) *Let $I = \langle a \rangle$ be an ideal of $\mathbb{Z}_m$, and let I_i be the ideal of $\mathbb{Z}_{p_i^{k_i}}$ generated by $a_i \equiv a \bmod p_i^{k_i}$. Denote by K_I, K_{I_i} the kernels of φ_I, φ_{I_i} on $\mathrm{GL}(n, \mathbb{Z}_m)$, $\mathrm{GL}(n, \mathbb{Z}_{p_i^{k_i}})$ respectively. Then*

$$\chi(K_I) = \bigtimes_{i=1}^{t} K_{I_i} \quad \textit{and} \quad \chi\big(K_I \cap \mathrm{SL}(n, \mathbb{Z}_m)\big) = \bigtimes_{i=1}^{t} \big(K_{I_i} \cap \mathrm{SL}(n, \mathbb{Z}_m)\big).$$

For $i \geq 1$,

$$M_{p,i} = \big\{h \in \mathrm{GL}(n, \mathbb{Z}_{p^k}) \mid h \equiv 1_n \bmod p^i\big\}, \qquad N_{p,i} = \mathrm{SL}(n, \mathbb{Z}_{p^k}) \cap M_{p,i}$$

are normal subgroups of $\mathrm{GL}(n, \mathbb{Z}_{p^k})$.

Lemma 2.2. *(Cf. Corollary 1.9.) If I is the ideal of $\mathbb{Z}_{p^k}$ generated by p^i, then $\varphi_I : \mathrm{GL}(n, \mathbb{Z}_{p^k}) \to \mathrm{GL}(n, \mathbb{Z}_{p^i})$ and $\varphi_I : \mathrm{SL}(n, \mathbb{Z}_{p^k}) \to \mathrm{SL}(n, \mathbb{Z}_{p^i})$ are surjective, with kernels $M_{p,i}$, $N_{p,i}$ respectively.*

The notation $M_{p,i}$, $N_{p,i}$ supersedes earlier notation for principal congruence subgroups in this special case. Let $d_j(a) = 1_n + ae_{jj} \in \mathrm{Mat}(n, \mathbb{Z}_m)$.

Lemma 2.3. *Suppose that $i < j \le 2i$ and $j \le k$. Then $M_{p,i}/M_{p,j} \cong C_{p^{j-i}}^{n^2}$, and $N_{p,i}/N_{p,j}$ has a subgroup isomorphic to $C_{p^{j-i}}^{n^2-1}$.*

Proof. Treating $\mathrm{Mat}(n, \mathbb{Z}_{p^{j-i}})$ as an additive group, we confirm that $\theta_j : M_{p,i} \to \mathrm{Mat}(n, \mathbb{Z}_{p^{j-i}})$ defined by $\theta_j(1_n + p^i x) = \varphi_{p^{j-i}}(x)$ is a homomorphism with kernel $M_{p,j}$. Now $t_{rs}(p^i) \in N_{p,i}$ and $d_r(p^i) \in M_{p,i}$, so θ_j is surjective. Since $N_{p,i}$ contains $1_n + p^i(e_{rr} - e_{r+1,r+1} + e_{r,r+1} - e_{r+1,r})$, the second assertion follows too. □

Lemma 2.4. $[M_{p,i}, M_{p,j}] = [N_{p,i}, N_{p,j}] = N_{p,i+j}$.

Proof. (Cf. Lemma 1.25.) Let $a = 1_n + p^i x \in M_{p,i}$ and $b = 1_n + p^j y \in M_{p,j}$. For some z, and $\bar{x}$, $\bar{y}$ such that $a^{-1} = 1_n + p^i \bar{x}$ and $b^{-1} = 1_n + p^j \bar{y}$, we have

$$\begin{aligned}
[a, b] &= \left(1_n + p^i \bar{x} + p^j \bar{y} + p^{i+j} \bar{x}\bar{y}\right)\left(1_n + p^i x + p^j y + p^{i+j} xy\right) \\
&= 1_n + p^i(x + \bar{x}) + p^{2i} \bar{x} x + p^j(y + \bar{y}) + p^{2j} \bar{y} y + p^{i+j} z \\
&= 1_n + p^{i+j} z.
\end{aligned}$$

Therefore $[M_{p,i}, M_{p,j}] \le M_{p,i+j} \cap \mathrm{SL}(n, \mathbb{Z}_{p^k}) = N_{p,i+j}$. Also $t_{21}(p^{i+j}) = [t_{23}(p^i), t_{31}(p^j)] \in [N_{p,i}, N_{p,j}] \trianglelefteq \mathrm{SL}(n, \mathbb{Z}_{p^k})$; thus $N_{p,i+j} \le [N_{p,i}, N_{p,j}]$ by Corollary 1.9. □

Lemma 2.5.

(i) $|M_{p,i}| = p^{n^2(k-i)}$.
(ii) $|\mathrm{GL}(n, \mathbb{Z}_{p^k})| = |\mathrm{GL}(n, p)| \cdot p^{n^2(k-1)}$.

Proof. Lemma 2.3 takes care of (i). By Lemma 2.2, we then get (ii). □

Corollary 2.6. *If $2i > k$ then $M_{p,i}$ is abelian of exponent p^{k-i}.*

The next two corollaries use Lemma 2.1. Let $a = p_1^{j_1} \cdots p_t^{j_t}$ where $0 \le j_i \le k_i$. Note that $a_i \equiv a \bmod p_i^{k_i}$ generates the ideal $\langle p_i^{j_i} \rangle$ of $\mathbb{Z}_{p_i^{k_i}}$. Set $M_{p_i,0} = \mathrm{GL}(n, \mathbb{Z}_{p_i^{k_i}})$ and $N_{p_i,0} = \mathrm{SL}(n, \mathbb{Z}_{p_i^{k_i}})$.

Corollary 2.7.

(i) $|\mathrm{GL}(n, \mathbb{Z}_m)| = \prod_{i=1}^t (|\mathrm{GL}(n, p_i)| \cdot p_i^{n^2(k_i-1)})$.
(ii) *The PCS of $\mathrm{GL}(n, \mathbb{Z}_m)$ of level a has order $\prod_{i=1}^t |M_{p_i,j_i}|$.*

Lemma 2.8.

(i) $|\mathrm{SL}(n, \mathbb{Z}_{p^k})| = |\mathrm{SL}(n, p)| \cdot p^{(n^2-1)(k-1)}$.
(ii) *For $i \ge 1$, $N_{p,i}/N_{p,i+1} \cong C_p^{n^2-1}$ and $|N_{p,i}| = p^{(n^2-1)(k-i)}$.*

Proof. The unit group of $\mathbb{Z}_{p^k}$ has order $(p-1)p^{k-1}$, so (i) follows from Lemma 2.5 (ii). Lemma 2.3 implies that $|N_{p,i}/N_{p,i+1}| \geq p^{n^2-1}$. Thus, if $|N_{p,j}/N_{p,j+1}| \neq p^{n^2-1}$ for some j then $|N_{p,1}| > p^{(n^2-1)(k-1)}$, which contradicts (i) by Lemma 2.2. $\square$

Corollary 2.9.

(i) $|\mathrm{SL}(n,\mathbb{Z}_m)| = \prod_{i=1}^{t}(|\mathrm{SL}(n,p_i)| \cdot p_i^{(n^2-1)(k_i-1)})$.
(ii) *The PCS of* $\mathrm{SL}(n,\mathbb{Z}_m)$ *of level* a *has order* $\prod_{i=1}^{t}|N_{p_i,j_i}|$.

Define subsets

$$S_c = \{t_{rs}(c),\ 1_n + c(e_{uu} + e_{u,u+1} - e_{u+1,u} - e_{u+1,u+1}) \mid r \neq s,\ 1 \leq r,s \leq n,\ 1 \leq u \leq n-1\}$$

of $\mathrm{SL}(n,\mathbb{Z}_m)$ and

$$T_c = \{t_{rs}(c), d_1(c), \ldots, d_n(c) \mid r \neq s,\ 1 \leq r,s \leq n\}$$

of $\mathrm{Mat}(n,\mathbb{Z}_m)$. We see that $T_c \leq \mathrm{GL}(n,\mathbb{Z}_m)$ if and only if $1+c$ is a unit of $\mathbb{Z}_m$.

Lemma 2.10. *Suppose that* $1 \leq i < k$.

(i) $N_{p,i}$ *has minimal generating set* S_{p^i}, *so* $\min(N_{p,i}) = n^2 - 1$.
(ii) *Unless* $p = 2$, $k \geq 3$, *and* $i = 1$, $\min(M_{p,i}) = n^2$ *and* $M_{p,i}$ *has minimal generating set* T_{p^i}.
(iii) $M_{2,1}$ *for* $k \geq 3$ *has minimal generating set* $T_2 \cup \{\mathrm{diag}(-1,1,\ldots,1)\}$ *of size* n^2+1.

Proof. In the proof of Lemma 2.3 we saw that $N_{p,i} = \langle S_{p^i}, N_{p,2i}\rangle$. Since $N_{p,i}$ is nilpotent with derived group $N_{p,2i}$ by Lemma 2.4, we have $N_{p,i} = \langle S_{p^i}\rangle$. So $\min(N_{p,i}) = \min(N_{p,i}/N_{p,i+1}) = n^2 - 1$ by Lemma 2.8 (ii).

The rest of the proof is along similar lines. Note that $M_{p,i} = \langle T_{p^i}, M_{p,2i}\rangle$, and $M_{p,2i}/N_{p,2i}$ is trivial when $2i \geq k$, or cyclic of order p^{k-2i} generated by the coset of $d_1(p^{2i})$ otherwise. Also $1 + p^{2i} \in \langle 1 + p^i\rangle \leq \mathbb{Z}_{p^k}^*$ unless $p = 2$, $k \geq 3$, and $i = 1$; whereas $5 \in \langle -1, 3\rangle = \mathbb{Z}_{2^k}^*$ for $k \geq 3$. Therefore $M_{p,i} = \langle T_{p^i}, N_{p,2i}\rangle = \langle T_{p^i}\rangle$ in (ii). Since $|T_{p^i}| = n^2$ and $M_{p,i}/M_{p,i+1}$ has rank n^2, this proves (ii). The verification of (iii) is left as an exercise. $\square$

Proposition 2.11. *Let* H, K *be non-trivial principal congruence subgroups of level* $a = p_1^{j_1} \cdots p_t^{j_t}$ *in* $\mathrm{GL}(n,\mathbb{Z}_m)$, $\mathrm{SL}(n,\mathbb{Z}_m)$ *respectively. Suppose further that* $1 \leq j_i < k_i$ *for some* i. *Then*

(i) $\min(H) = n^2$ *unless* $k_2 \geq 3$ *and the Sylow* 2*-subgroup of* $\chi(H)$ *is* $M_{2,1}$*; in the latter case* $\min(H) = n^2 + 1$.
(ii) $\min(K) = n^2 - 1$.

Proof. If X, Y are groups of coprime order with minimal generating sets $\{x_1, \dots, x_{r_1}\} \subseteq X$ and $\{y_1, \dots, y_{r_2}\} \subseteq Y$, where $r_1 \leq r_2$, then $\min(X \times Y) = r_2$. Indeed

$$X \times Y = \langle (x_i, y_i), (1, y_j) : 1 \leq i \leq r_1;\ r_1 + 1 \leq j \leq r_2 \rangle.$$

Therefore $\min(H) \geq n^2$ or $n^2 + 1$ and $\min(K) \geq n^2 - 1$ by Lemmas 2.1 (ii) and 2.10. For those indices i such that $1 \leq j_i < k_i$ does not hold, the Sylow p_i-subgroups of $\chi(H)$ and $\chi(K)$ are either trivial or $\mathrm{GL}(n, \mathbb{Z}_{p_i^{k_i}})$, $\mathrm{SL}(n, \mathbb{Z}_{p_i^{k_i}})$ respectively. As $\mathrm{GL}(n, \mathbb{Z}_b)$ is 4-generated and $\mathrm{SL}(n, \mathbb{Z}_b)$ is 2-generated, we are done. □

Remark 2.12. The proof of Proposition 2.11 shows how to construct minimal generating sets for H and K with the aid of Lemma 2.10. Note that we get a generating set for a PCS in $\mathrm{SL}(n, \mathbb{Z}_m)$ by reducing (1) in Proposition 1.10 modulo p.

2.2. *Computing in* $\mathrm{GL}(n, \mathbb{Z}_m)$

As above, suppose that $m \geq 2$ has prime factorization $\prod_{i=1}^t p_i^{k_i}$. Let χ be the isomorphism introduced just before Lemma 2.1. We identify $H \leq \mathrm{GL}(n, \mathbb{Z}_m)$ with $\chi(H)$.

To compute with H, we use composition tree methods and the data structure from [17]. The latter consists of an effective homomorphism into $\times_{i=1}^t \mathrm{GL}(n, p_i)$ whose kernel K is the solvable radical of H, and a polycyclic generating sequence (PCGS) for K. Data structures for the images of the projections of H modulo $p_i^{k_i}$ can be combined into a data structure for H. We therefore assume that $m = p^k$.

Clearly H/K is isomorphic to a quotient of $\varphi_p(H) \leq \mathrm{GL}(n, p)$, and a PCGS for the radical of $\varphi_p(H)$ gives the initial terms of a PCGS for K; the rest are found by reductions modulo p^e (cf. Subsection 2.1). As we have seen, if M is the kernel of reduction modulo p^e and N the kernel of reduction modulo p^{e+1}, then M/N is described by matrices $1_n + p^e x$ for $x \in \mathrm{Mat}(n, p)$, which multiply by addition of their x-parts. A PCGS for the elementary abelian group M/N can be determined easily by linear algebra.

2.3. *Subnormal structure*

Let $n \geq 3$. We adhere to previous notation and conventions.

Let `Level` be a function that returns $\ell(H)$ for a subgroup $H = \langle S \rangle$ of $G_n = \mathrm{GL}(n, \mathbb{Z}_m)$; see Lemma 1.22.

`MaxPCS`(H)

Input: $H \leq G_n$.
Output: a generating set for a maximal PCS of $\Gamma_n = \mathrm{SL}(n, \mathbb{Z}_m)$ in H.

(1) $l :=$ `Level`(H).

(2) If $l = 0$ then return 1_n,

else return a generating set L for the PCS of level a in Γ_n as given by Proposition 2.11, where a is minimal subject to a dividing m, l dividing a, and $L \subseteq H$.

Step (2) requires membership testing. As an application of `MaxPCS`, we have

`IsSL`(H)

Input: $H \le \Gamma_n$.
Output: `true` if $H = \Gamma_n$; `false` otherwise.

If `Level`(`MaxPCS`(H)) $= 1$ then return `true`

else return `false`.

The following reiterates Theorem 1.24.

`IsSubnormal`(H)

Input: $H \le G_n$.
Output: `true` and an upper bound d on the defect of H if $H \operatorname{sn} G_n$; `false` otherwise.

(1) $l_1 :=$ `Level`(H), $l_2 :=$ `Level`(`MaxPCS`(H)).
(2) If $\nexists e$ such that $l_2 \mid l_1^e$ then return `false`,

else return `true` and $d := e' + 1$ where $e' :=$ the least e such that $l_2 \mid l_1^e$.

Remark 2.13. Let $H \le \Gamma_n$. Obviously $H \operatorname{sn} \Gamma_n$ if and only if $H \operatorname{sn} G_n$. The defect of H as a subnormal subgroup of Γ_n is either equal to or one less than its defect as a subgroup of G_n.

`NormalClosure`(H) returns the normal closure of H in G_n according to Lemma 1.27. `IsNormal` tests whether $H \trianglelefteq G_n$, returning `true` if and only if $l_2 = l_1$ (Corollary 1.28).

By Proposition 1.29, `NormalClosure` also returns the normal closure in Γ_n of $H \le \Gamma_n$, and `IsNormal` tests whether $H \trianglelefteq \Gamma_n$.

We can list the subnormal subgroups of G_n in H.

`NormalSubgroups`(H, l)

Input: $H \le G_n$ and a positive integer l.
Output: all normal subgroups of G_n in H of level l.

(1) $r :=$ `Level`(`MaxPCS`(H)).
(2) If r does not divide l then return $\emptyset$.
(3) $\mathcal{L} :=$ a list of all subgroups of $\varphi_l(H) \cap \varphi_l(Z_{n,l})$.
(4) Return the full preimage of $\mathcal{L}$ in H under φ_l.

We next sketch a more general method. Let $\mathcal{L}_{a,b}$ be the list of all K such that $\Gamma_{n,b} \leq K \leq H \cap Z_{n,a}$. Define $\mathcal{L} = \bigcup_k \mathcal{L}_{k,k^t}$ where k ranges over the multiples of $\ell(H)$ dividing m, and $t = t(k)$ is maximal subject to $r \mid k^t$. Then $\mathcal{L}$ is a complete list of the subnormal subgroups of G_n in H. By Lemma 1.25, $\mathcal{L}_{k,k^t}$ consists of preimages of subgroups of the nilpotent group $\varphi_{k^t}(Z_{n,k})$. Redundancies in $\mathcal{L}$ are removed using $\mathcal{L}_{k_1,k_1^{t_1}} \cap \mathcal{L}_{k_2,k_2^{t_2}} = \mathcal{L}_{\mathrm{lcm}(k_1,k_2),\gcd(k_1,k_2)^t}$ where $t = \min(t_1, t_2)$, by Lemma 1.16.

3. Computing with arithmetic groups in $\mathrm{SL}(n, \mathbb{Z})$

3.1. Decision problems

An arithmetic subgroup H of an algebraic $\mathbb{Q}$-group $G \leq \mathrm{GL}(n, \mathbb{C})$ is 'explicitly given' if (i) an upper bound on $|G_{\mathbb{Z}} : H|$ is known, and (ii) membership testing in H is possible; i.e., for any $g \in G_{\mathbb{Z}}$ it can be decided whether $g \in H$ [14, pp. 531–532]. Conditions (i) and (ii) were assumed in [14] to prove decidability of algorithmic problems for H. As the next lemma shows, for $G = \mathrm{GL}(n, \mathbb{C})$ and $n > 2$, these conditions are equivalent to knowing a PCS in H. Such a PCS can always be found: see Corollary 1.15.

Lemma 3.1. *Let $H \leq_f \Gamma_n$. The following are equivalent.*

(i) *A positive integer m such that $\Gamma_{n,m} \leq H$ is known.*
(ii) *An upper bound on $|\Gamma_n : H|$ is known, and testing membership of $x \in \Gamma_n$ in H is decidable.*

Proof. (i) ⇒ (ii). $|\Gamma_n : H| \leq |\mathrm{SL}(n, \mathbb{Z}_m)|$, and $x \in H$ if and only if $\varphi_m(x) \in \varphi_m(H)$.

(ii) ⇒ (i). Suppose that $|\Gamma_n : H| \leq r$. For $g \in \Sigma$ as in Proposition 1.10 and each pair i, j, after no more than r rounds we are guaranteed to find positive integers $r_{g,i,j} \leq r$ such that $t_{ij}(r_{g,i,j})^g = (t_{ij}^g)^{r_{g,i,j}} \in H$. Thus, if m is any common multiple of the $r_{g,i,j}$ then $\Gamma_{n,m} \leq H$. □

Proposition 3.2. *If H is a finite index subgroup of Γ_n specified by a finite generating set then testing membership of any $g \in \Gamma_n$ in H is decidable.*

Proof. This follows from Corollary 1.15 and Lemma 3.1. □

A key problem that arose naturally in our research is

> (AT) *Arithmeticity testing*: if H is a finitely generated subgroup of Γ_n,
>
> determine whether $|\Gamma_n : H|$ is finite.

We are unaware of any proof that (AT) is decidable—although it seems not to be [24]. Nonetheless, (AT) is decidable when G is solvable [7]. See also [28] for an indication of the significance of (AT).

3.2. Algorithms for arithmetic groups

Now we design algorithms for arithmetic groups $H \leq \Gamma_n = \mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$, given by a finite generating set.

By Corollary 1.15 (and the proof of Lemma 1.13), we obtain a procedure $\texttt{LevelPCS}(H)$ that returns the level of a PCS in H. It depends on representing elements of Γ_n as products of transvections. Say $\texttt{LevelPCS}(H) = m$; then $\texttt{GeneratorsPCS}(m)$ returns a generating set for $\Gamma_{n,m}$ as in Proposition 1.10.

Let $\overline{H} = \varphi_m(H) \leq \overline{\Gamma}_n = \mathrm{SL}(n, \mathbb{Z}_m)$. Lemma 1.21 underpins the following, which finds the maximal PCS $\Gamma_{n,r}$ in H. (To improve efficiency we could substitute r for m in algorithms of this section.)

$\texttt{MaxPCS}(H, m)$

Input: $H \leq \Gamma_n$ such that $\Gamma_{n,m} \leq H$.
Output: a generating set for the maximal PCS in H.

(1) $r := \texttt{Level}(\texttt{MaxPCS}(\overline{H}))$.
(2) Return $\texttt{GeneratorsPCS}(r)$.

Remember that the level of a finitely generated subgroup of Γ_n is calculated straightforwardly by Lemma 1.22. $\texttt{IsSL}(H, m)$ returns $\texttt{true}$ if $\texttt{MaxPCS}(H, m)$ has level 1 and $\texttt{false}$ otherwise.

We mention a few more sample procedures.

$\texttt{Index}(H, \Gamma, m)$ returns $|\Gamma_n : H| = |\overline{\Gamma}_n : \overline{H}|$.

$\texttt{IsSubgroup}(H, L, m)$ tests whether a finitely generated subgroup L of Γ_n is contained in H, returning $\texttt{true}$ if and only if $\overline{L} \leq \overline{H}$.

$\texttt{Intersect}(H_1, H_2, m)$. Suppose that $\Gamma_{m_i} \leq H_i \leq \Gamma_n$, $i = 1, 2$. Let $l = \mathrm{lcm}(m_1, m_2)$. This procedure returns $H_1 \cap H_2$, which by Lemma 1.16 (ii) is the full preimage in Γ_n under φ_l of $\varphi_l(H_1) \cap \varphi_l(H_2)$.

$\texttt{IsSubnormal}(H, m)$ returns $\texttt{true}$ and a bound on the defect of H if $H \,\mathrm{sn}\, \Gamma_n$; otherwise it returns $\texttt{false}$. The steps mimic those of $\texttt{IsSubnormal}(H)$ from Subsection 2.3, but are now carried out over $\mathbb{Z}$. The same comment applies to normality testing of H.

$\texttt{NormalClosure}(H)$: as before, immediate from Lemma 1.27. We do not need to know a PCS in H.

$\texttt{Normalizer}(H, m)$ returns $N_{\Gamma_n}(H)$, the full preimage in Γ_n of $N_{\overline{\Gamma}_n}(\overline{H})$. Note that $C_{\Gamma_n}(H)$ is either trivial if n is odd or $\langle -1_n \rangle$ if n is even, because H is absolutely irreducible over $\mathbb{Q}$.

$\texttt{NormalSubgroups}(H, m)$ returns all normal subgroups of Γ_n in H containing $\Gamma_{n,m}$: this is the full preimage of the list $\bigcup_l \texttt{NormalSubgroups}(\overline{H}, l)$ as l ranges over the divisors

of m. All subnormal subgroups of Γ_n in H containing $\Gamma_{n,m}$ are extracted similarly from the corresponding list in $\overline{\Gamma}_n$.

4. The orbit-stabilizer problem

Let R be a commutative ring with 1, and let $H = \langle S \rangle \leq \mathrm{GL}(n, R)$. This section addresses the *orbit-stabilizer problem*: for arbitrary u, $v \in R^n$,

(I) decide whether there is $g \in H$ such that $gu = v$, and find a g if it exists;
(II) determine $\mathrm{Stab}_H(u) = \{g \in H \mid gu = u\}$.

The element g and a generating set for $\mathrm{Stab}_H(u)$ should be written as words over $S \cup S^{-1}$. We solve (I) and (II) for $R = \mathbb{Q}$ and $H \leq_f \Gamma_n = \mathrm{SL}(n, \mathbb{Z})$. Along the way, partial results for subgroups of $\overline{\Gamma}_n = \mathrm{SL}(n, \mathbb{Z}_m)$ are proved as well.

4.1. Preliminaries

Suppose that $\Gamma_{n,m} \leq H \leq \Gamma_n$. Denote images under φ_m by overlining.

Lemma 4.1. *Let $u, v \in \mathbb{Z}^n$, and let K be the full preimage of $\mathrm{Stab}_{\overline{H}}(\bar{u})$ in H. Then*

(i) *$v \in Hu$ if and only if $\bar{v} \in \overline{H}\bar{u}$ and $hv \in Ku$ for any $h \in H$ such that $\bar{h}\bar{v} = \bar{u}$.*
(ii) *$\mathrm{Stab}_H(u) = \mathrm{Stab}_K(u)$.*

Proposition 4.2. *If we can solve the orbit-stabilizer problem for $\Gamma_{n,m}$ (acting on $\mathbb{Z}^n$), then we can solve it for H.*

Proof. (Cf. [11, p. 255] and [12, Lemma 3.1].) First, note that K permutes the $\Gamma_{n,m}$-orbits in $\mathbb{Z}^n$. Let $\{y_1, \ldots, y_k\}$ be a set of representatives for the K-orbit of $\Gamma_{n,m}u$. In the notation of Lemma 4.1,

$$v \in Hu \iff hv \in Ku \iff hv, y_i u \text{ are in the same } \Gamma_{n,m}\text{-orbit for some } i.$$

Secondly, we can find (Schreier) generators $h_1, \ldots, h_s$ of $\mathrm{Stab}_K(\Gamma_{n,m}u)$; and also find $g_i \in \Gamma_{n,m}$ such that $g_i u = h_i u$, $1 \leq i \leq s$. Then

$$\mathrm{Stab}_H(u) = \mathrm{Stab}_K(u) = \langle g_1^{-1}h_1, \ldots, g_s^{-1}h_s, \mathrm{Stab}_{\Gamma_{n,m}}(u) \rangle. \qquad \square$$

As suggested by Proposition 4.2, we aim initially to solve the orbit-stabilizer problem for a PCS in Γ_n.

Let $u = (u_1, \dots, u_n)^\top \in R^n$, and let $\langle u \rangle$ denote the ideal of R generated by the u_i.

Lemma 4.3. *$\langle xu \rangle = \langle u \rangle$ for any $x \in \mathrm{GL}(n, R)$; thus, $\langle u \rangle = \langle v \rangle$ if u and v are in the same $\mathrm{GL}(n, R)$-orbit.*

A vector $u \in R^n$ such that $\langle u \rangle = R$ is said to be *unimodular*. By Lemma 4.3, $\mathrm{GL}(n, R)$ permutes the unimodular vectors among themselves.

4.2. $\overline{\Gamma}_n$-orbits in $\mathbb{Z}_m^n$

Suppose that m has prime factorization $p_1^{e_1} \cdots p_s^{e_s}$, and write $a \in \mathbb{Z}_m$ as $(a_1, \dots, a_s)$, $a_i \in \mathbb{Z}_{p_i^{e_i}}$.

Lemma 4.4. *If $(u_1, \dots, u_n)^\top \in \mathbb{Z}_m^n$ is unimodular then $u_1 + \sum_{i=2}^n b_i u_i$ is a unit of $\mathbb{Z}_m$ for some $b_2, \dots, b_n \in \mathbb{Z}_m$.*

Lemma 4.4 is proved in [18, p. 104]. We summarize the proof as follows.

`Auxiliary1`(u)

Input: unimodular $u = (u_1, \dots, u_n)^\top \in \mathbb{Z}_m^n$.
Output: $b_2, \dots, b_n$ as in Lemma 4.4.

(1) For $j = 1, \dots, s$ do
  let k be the least index such that $p_j^{e_j - 1} u_{kj} \not\equiv 0 \bmod p_j^{e_j}$;
  $b_{kj} := 1$ and $b_{ij} := 0$ for $i \neq k$.

(2) Return $b_2 := (b_{21}, b_{22}, \dots, b_{2s}), \dots, b_n := (b_{n1}, b_{n2}, \dots, b_{ns})$.

Lemma 4.5. *If $u \in \mathbb{Z}_m^n$ is unimodular then $gu = (1, 0, \dots, 0)^\top$ for some $g \in \overline{\Gamma}_n$.*

Proof. By Lemma 4.4,

$$t_{12}(b_2) \cdots t_{1n}(b_n) u = (v_1, u_2, \dots, u_n)^\top$$

where $v_1 = u_1 + \sum_{i=2}^n b_i u_i$ is a unit of $\mathbb{Z}_m$. Further,

$$t_{n1}\left(-v_1^{-1} u_n\right) \cdots t_{21}\left(-v_1^{-1} u_2\right)(v_1, u_2, \dots, u_n)^\top = (v_1, 0, \dots, 0)^\top.$$

Finally,

$$t_{21}(-1) t_{12}(1 - v_1) t_{21}\left(v_1^{-1}\right)(v_1, 0, \dots, 0)^\top = (1, 0, \dots, 0)^\top. \qquad \square$$

Corollary 4.6. *The set of all unimodular vectors is a $\overline{\Gamma}_n$-orbit in $\mathbb{Z}_m^n$.*

Proposition 4.7. *Non-zero vectors $u, v \in \mathbb{Z}_m^n$ are in the same $\overline{\Gamma}_n$-orbit if and only if $\langle u \rangle = \langle v \rangle$.*

Proof. Suppose that $\langle u \rangle = \langle v \rangle$; so $u = a\tilde{u}$ and $v = a\tilde{v}$ for some a dividing m, $1 \le a < m$, and unimodular $\tilde{u}$, $\tilde{v}$. Now the result is apparent by Lemma 4.3 and Corollary 4.6. □

Corollary 4.8. *The map defined by $\overline{\Gamma}_n u \mapsto \langle u \rangle$ is a bijection between the set of $\overline{\Gamma}_n$-orbits in $\mathbb{Z}_m^n$ and the set of ideals of $\mathbb{Z}_m$.*

4.3. Orbits in $\mathbb{Z}^n$

4.3.1. Γ_n-orbits

Lemma 4.9. *Let $u = (u_1, \dots, u_n)^\top \in \mathbb{Z}^n \setminus \{0\}$ and let d be the gcd of the non-zero entries of u. Then $tu = (d, 0, \dots, 0)^\top$ for some $t \in \Gamma_n$.*

Proof. (Cf. [30, Lemma 3, pp. 72–73].) Say the non-zero entries of u are $u_{j_1}, \dots, u_{j_l}$ where $j_1 < \cdots < j_l$. If $u_i = 0$ then

$$t_{j_i i}(-1)t_{i j_i}(1)u = (u_1, \dots, u_{i-1}, u_{j_i}, u_{i+1}, \dots, u_{j_i-1}, 0, u_{j_i+1}, \dots, u_n)^\top.$$

So the lemma holds for $l = 1$, and we may assume that $j_i = i$ and $l \ge 2$.

Formally, the proof is by induction on l. We manufacture t by applying the Euclidean algorithm repeatedly to pairs of adjacent nonzero entries of u. To begin, put $r_0 = u_{l-1}$, $r_1 = u_l$; then for $i \ge 0$ and while $r_{i+1} \ne 0$, let q_{i+1}, r_{i+2} be the integers such that $r_i = r_{i+1}q_{i+1} + r_{i+2}$ and $0 \le r_{i+2} < |r_{i+1}|$. If r_k is the last non-zero remainder then

$$t^* u = (u_1, \dots, u_{l-2}, r_k, 0, 0, \dots, 0)^\top$$

where

$$t^* = \begin{cases} t_{l,l-1}(-1)t_{l-1,l}(1)t_{l-1,l}(-q_k)\cdots t_{l,l-1}(-q_2)t_{l-1,l}(-q_1) & k \text{ odd}, \\ t_{l,l-1}(-q_k)\cdots t_{l,l-1}(-q_2)t_{l-1,l}(-q_1) & k \text{ even}. \end{cases}$$

At the next stage we put $r_0 = u_{l-2}$, $r_1 = r_k$, and repeat the above. Continuing in this fashion ultimately gives t as desired. □

Proposition 4.10. *(Cf. [30, Corollary 1, p. 73].) Vectors u, $v \in \mathbb{Z}^n$ belong to the same Γ_n-orbit if and only if $\langle u \rangle = \langle v \rangle$.*

Proof. In the notation of Lemma 4.9, $\langle u \rangle = d\mathbb{Z}$. □

Corollary 4.11. *There is a one-to-one correspondence between the set of Γ_n-orbits in $\mathbb{Z}^n$ and the set of ideals of $\mathbb{Z}$.*

`Orbit1Gamma` accepts $u \in \mathbb{Z}^n \setminus \{0\}$ and (as per the proof of Lemma 4.9) returns a pair (d, t) where $t \in \Gamma_n$, d is the gcd of all non-zero entries of u, and $tu = (d, 0, \dots, 0)^\top$.

By Proposition 4.10, the next procedure solves the orbit problem for Γ_n acting on $\mathbb{Z}^n$.

`OrbitGamma`(u, v)

Input: $u, v \in \mathbb{Z}^n \setminus \{0\}$.
Output: $g \in \Gamma_n$ such that $gu = v$, or `false` if u, v are not in the same Γ_n-orbit.

(1) $(d_1, t_1) :=$ `Orbit1Gamma`(u),
 $(d_2, t_2) :=$ `Orbit1Gamma`(v).
(2) If $d_1 \neq d_2$ then return `false`,
 else return $t_2^{-1} t_1$.

4.3.2. $\Gamma_{n,m}$-orbits

Lemma 4.12. *(See [18, Lemma 2, p. 105].) Let $u, v \in \mathbb{Z}^n$. Suppose that there is a non-empty subset $I \subseteq \{1, \dots, n\}$ such that $u_i = v_i$ for $i \in I$ and $u_i \equiv v_i \bmod mm'$ for $i \notin I$, where $m'\mathbb{Z} = \langle u_j : j \in I \rangle$. Then u, v are in the same $\Gamma_{n,m}$-orbit.*

We outline the proof of Lemma 4.12 in the form of an algorithm.

`Auxiliary2`(u, v, I)

Input: $u, v \in \mathbb{Z}^n$, I as in Lemma 4.12.
Output: $g \in \Gamma_{n,m}$ such that $gu = v$.

(1) For $i \in I$ and $j \in \{1, \dots, n\} \setminus I$, find $c_{ji} \in \mathbb{Z}$ such that $v_j = u_j + m \sum_{i \in I} c_{ji} u_i$.
(2) Return $g := \prod_{i \in I, j \notin I} t_{ji}(mc_{ji})$.

Theorem 4.13. *Let $u, v \in \mathbb{Z}^n \setminus \{0\}$ where $\langle u \rangle = a\mathbb{Z}$. Then u and v are in the same $\Gamma_{n,m}$-orbit if and only if $\langle u \rangle = \langle v \rangle$ and $u_i \equiv v_i \bmod am$, $1 \le i \le n$.*

Proof. See the theorem on p. 101 of [18] for $n > 2$. Suppose that $n = 2$, $\langle u \rangle = \langle v \rangle$, and $u_i \equiv v_i \bmod am$. Then $tv = (a, 0)^\top$ and $tu = a(1 + mr, ms)^\top$ for some $t \in \Gamma_2$ and $r, s \in \mathbb{Z}$ such that $\langle 1 + mr, ms \rangle = \mathbb{Z}$, say $x(1 + mr) + yms = 1$. Consequently $h^t u = v$ where

$$h = \begin{pmatrix} 1 - mrx & -mry \\ -ms & 1 + mr \end{pmatrix}. \qquad \square$$

The procedure below incorporates the method for $n > 2$ in [18, pp. 105–106]. Lines beginning '#' contain explanatory comments.

`OrbitGamma_m`(u, v)

Input: $u, v \in \mathbb{Z}^n$, $n \geq 2$.
Output: $g \in \Gamma_{n,m}$ such that $gu = v$, or `false` if u, v are not in the same $\Gamma_{n,m}$-orbit.

(1) If `OrbitGamma`$(u, v) =$ `false` then return `false`.

(2) If $u_i \not\equiv v_i \bmod am$ for some i, where $(a, t) :=$ `Orbit1Gamma`(v), then return `false`,

else $u := \frac{1}{a}tu$.

\# u is now unimodular, $u_1 \equiv 1 \bmod m$, and $u_i \equiv 0 \bmod m$ for $i > 1$.

(3) Apply `Auxiliary1` to find $b_3, \ldots, b_n \in \mathbb{Z}$ such that $c := u_2 + r\sum_{i=3}^n b_i u_i$ is coprime to u_1, where $u_1 = 1 - r$, $r \in m\mathbb{Z}$.

\# u unimodular $\Longrightarrow (u_2, ru_3, \ldots, ru_n)^\top$ unimodular mod u_1.

(4) If $n \geq 3$ then

$s_1 :=$ `Auxiliary2`$(u, (u_1, c, u_3, \ldots, u_n)^\top, \{3, \ldots, n\})$,

\# u, $(u_1, c, u_3, \ldots, u_n)^\top$, and $I = \{3, \ldots, n\}$ satisfy the hypotheses of Lemma 4.12.

$s_2 :=$ `Auxiliary2`$((u_1, c, u_3, u_4, \ldots, u_n)^\top, (u_1, c, r, 0, \ldots, 0)^\top, \{1, 2\})$.

\# Lemma 4.12 again, with $m' = \gcd(u_1, c) = 1$.

(5) If $n = 2$ then $s := h$ as in the proof of Theorem 4.13,

else $s := s_3 s_2 s_1$ where $s_3 := t_{13}(-1)t_{31}(-r)t_{21}(-c)t_{13}(1)$.

\# $s_3 \in \Gamma_{n,m}$ because $\Gamma_{n,m} \trianglelefteq \Gamma_n$.

(6) Return $g := s^t$.

\# $s^t \in \Gamma_{n,m}$ and $s\frac{1}{a}tu = (1, 0, \ldots, 0)^\top = t\frac{1}{a}v$ for the original input u, v.

4.4. Stabilizers in Γ_n and $\Gamma_{n,m}$

Suppose that $\Gamma_{n,m} \leq H \leq \Gamma_n$ and $u \in \mathbb{Z}^n \setminus \{0\}$. As an arithmetic subgroup of an algebraic group, $\mathrm{Stab}_H(u)$ is finitely generated [15, p. 744]. Indeed, $\mathrm{Stab}_{\Gamma_n}(u) = \Lambda_n^t$ where `Orbit1Gamma`$(u) = (d, t)$ and Λ_n is the affine group

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & & & \\ \vdots & & \Gamma_{n-1} & \\ 0 & & & \end{pmatrix}.$$

Hence $\mathrm{Stab}_{\Gamma_n}(u)$ is generated by $t_{12}(1)^t, \ldots, t_{1n}(1)^t$, $\mathrm{diag}(1, x)^t$, and $\mathrm{diag}(1, y)^t$, where x, y are the generators of Γ_{n-1} given in Subsection 1.2. Next,

$$\mathrm{Stab}_{\Gamma_{n,m}}(u) = \mathrm{Stab}_{\Gamma_n}(u) \cap \Gamma_{n,m} = (\Lambda_n \cap \Gamma_{n,m})^t.$$

Plainly $\Lambda_n \cap \Gamma_{n,m}$ is generated by $\mathrm{diag}(1, x)$ as x ranges over a generating set of $\Gamma_{n-1,m}$ (see Proposition 1.10), together with $t_{12}(m), \ldots, t_{1n}(m)$. We denote by `StabGamma_m` the procedure that returns the set of t-conjugates of these matrices for input u.

4.5. Solution of the orbit-stabilizer problem for arithmetic groups

Recalling Proposition 4.2 and its proof, we now describe the main algorithms.

As $\Gamma_{n,m} \lhd H$, the orbits of $\Gamma_{n,m}$ form a block system for H. All vectors in a block have the same reduction modulo m (but vectors with equal reduction may not be in the same block). We first check for equivalence of vectors under the action by $\overline{H} = \varphi_m(H)$, and compute generators for stabilizers in $\overline{H}$. Then we represent each $\Gamma_{n,m}$-orbit by a vector in $\mathbb{Z}^n$ and use `OrbitGamma_m` to test orbit equality. We shall write $\underline{u}$ for $\Gamma_{n,m}u$; that is, $\underline{u} = \underline{v}$ if and only if `OrbitGamma_m`(u, v) is not `false`.

To determine stabilizers (and thereby eliminate surplus generators) in H we calculate the induced action of $\overline{H}$ and then take preimages.

If $h \in H$ stabilizes $\underline{u}$ then we put $g_h =$ `OrbitGamma_m`(u, hu). Hence $\mathrm{Stab}_H(u)$ is generated by `StabGamma_m`(u) together with the corrected elements $g_h^{-1}h$.

We state the algorithms below.

`Orbit`(u, v, S)

Input: $u, v \in \mathbb{Z}^n \setminus \{0\}$ and $S \subseteq \Gamma_n$ such that $\Gamma_{n,m} \leq H = \langle S \rangle$.
Output: $h \in H$ such that $hu = v$, if $v \in Hu$; `false` otherwise.

(1) Determine $\mathrm{Stab}_{\overline{H}}(\bar{u})$ and $\overline{H}\bar{u}$.
 If $\bar{v} \notin \overline{H}\bar{u}$ then return `false`,
  else select $\overline{h_1} \in \overline{H}$ such that $\overline{h_1 v} = \bar{u}$ and replace v by $h_1 v$.
(2) Determine the K-orbit of $\underline{u}$, where K is the full preimage of $\mathrm{Stab}_{\overline{H}}(\bar{u})$ in H.
 If $\underline{v} \notin K\underline{u}$ then return `false`,
  else select $h_2 \in K$ such that $\underline{h_2 v} = \underline{u}$ and replace v by $h_2 v$.
(3) $g :=$ `OrbitGamma_m`(u, v).
(4) Return $h_1^{-1}h_2^{-1}g$.

`Stabilizer`(u, S)

Input: $u \in \mathbb{Z}^n \setminus \{0\}$ and $S \subseteq \Gamma_n$ such that $\Gamma_{n,m} \leq H = \langle S \rangle$.
Output: a generating set for $\mathrm{Stab}_H(u)$.

(1) $K :=$ the full preimage of $\mathrm{Stab}_{\overline{H}}(\bar{u})$ in H.
(2) $L := \mathrm{Stab}_K(\underline{u})$.
(3) $g_h :=$ `OrbitGamma_m`(u, hu) for each generator h of L,
 $A := \{g_h^{-1}h \mid h \text{ a generator of } L\}$.
(4) Return $A \cup$ `StabGamma_m`(u).

4.6. Remarks on and refinements of the algorithms

The stabilizer calculations for $\bar{u}$ and $\underline{u}$ are done in $\overline{H}$ via the data structure of Subsection 2.2. We use the solvable radical of $\overline{H}$ to deal with orbits, as in [17]. Typically the main obstacle is that $\overline{H}\bar{u}$ can be very long. To ameliorate this we take orbits of $\varphi_r(u)$ for an increasing sequence of divisors r of m.

A further refinement (as with any linear action) is given by the imprimitivity system arising from the relation of vectors being unit multiples of each other. Here $\overline{H}$ acts on blocks projectively; i.e., as $\overline{H}Z/Z$ where $Z = Z(\mathrm{SL}(n, \mathbb{Z}_r)) = \{a1_n \mid a \in \mathbb{Z}_r^*\}$. We implement this action by representing each block by a normalized vector. For prime r, this means scaling the vector so that its first nonzero entry is 1. If the original entry has a common divisor with r greater than 1, then a minimal associate will be different from 1 and will usually have a nontrivial stabilizer. This stabilizer is then used to minimize entries in subsequent positions.

4.7. Preimages under φ_m

A basic operation when utilizing congruence homomorphisms is to find preimages: for $b \in \overline{\Gamma}_n$ find $c \in \Gamma_n$ such that $\varphi_m(c) = b$ (any preimage will do because $\Gamma_{n,m} \leq H$). We cannot simply treat b as an integer matrix; it need not have determinant 1 over $\mathbb{Z}$.

Matrix group recognition [1] maintains a history of how each element of $\overline{H}$ was obtained as a word in congruence images of generators of H. Long product expressions tend to build up when constructing a composition tree for $\overline{H}$ using pseudo-random products. Evaluating these expressions back in characteristic 0 leads to large matrix entries.

We could write b as a product of transvections in $\overline{\Gamma}_n$ and then form the same product over $\mathbb{Z}$. Similarly, suppose that c has Smith Normal Form $c_L c_D c_R$ where c_L, $c_R \in \Gamma_n$ and $\overline{c_D} = 1_n$. Thus $\overline{c_L c_R} = \bar{c} = b$ and $c_L c_R$ is a suitable preimage. Still, these approaches sometimes produced larger matrix entries than in the following heuristic.

Let x be the transposed adjugate $\det(c)(c^{-1})^\top$. Adding 1 to c_{ij} for $i \neq j$ adds x_{ij} to $\det(c)$. If $\det(c) \neq 1$ and $\det(c) + amx_{ij}$ is positive of smaller absolute value, then add am to c_{ij}. Repeat with updated x. If no such x_{ij} exists (all entries of x are larger in absolute value than $\det(c)$), then we can try to use instead the gcd of two entries of x in the same row or column. Eventually $\det(c) = 1$, or we have to defer to the other methods.

5. Generalizing to any arithmetic group in $\mathrm{SL}(n, \mathbb{Q})$

Let $H \leq \mathrm{SL}(n, \mathbb{Q})$ be arithmetic. We explain how to compute $g \in \mathrm{GL}(n, \mathbb{Q})$ such that $H^g \leq \Gamma_n$. Our algorithms may therefore be modified to accept any arithmetic group in $\mathrm{SL}(n, \mathbb{Q})$; i.e., not necessarily given by a generating set of integer matrices.

Lemma 5.1. *The following are equivalent, for a finitely generated subgroup H of* $\mathrm{GL}(n, \mathbb{Q})$.

- *$H_{\mathbb{Z}} := H \cap \Gamma_n$ has finite index in H.*
- *H is $\mathrm{GL}(n,\mathbb{Q})$-conjugate to a subgroup of $\mathrm{GL}(n,\mathbb{Z})$.*
- *There exists a positive integer d such that $dH \subseteq \mathrm{Mat}(n,\mathbb{Z})$.*
- *$\mathrm{tr}(H) = \{\mathrm{tr}(h) \mid h \in H\} \subseteq \mathbb{Z}$.*

Proof. See [7, Section 3] and [2, Theorem 2.4]. □

An integer $d = d(H)$ as in Lemma 5.1 is a *common denominator* for H. Suppose that $H = \langle S \rangle \leq \mathrm{SL}(n,\mathbb{Q})$ is arithmetic. Hence d exists. Let $\mathcal{A} = \{a_1, \ldots, a_{n^2}\} \subseteq H$ be a basis of the enveloping algebra $\langle H \rangle_{\mathbb{Q}}$, and let c be a common multiple of the denominators of all entries in the a_i. By the proof of [2, Theorem 2.4] we can take $d = c \det([\mathrm{tr}(a_i a_j)]_{ij})$. A basis $\mathcal{A}$ can be found by, e.g., a standard 'spinning-up' process. However, when we know m such that $\Gamma_{n,m}$ is in the finite index subgroup $H_{\mathbb{Z}}$ of Γ_n, we can write down $\mathcal{A}$ directly. Let $b_k(m)$ be the block diagonal matrix with

$$\begin{pmatrix} 1+m & m \\ -m & 1-m \end{pmatrix}$$

in rows/columns k, $k+1$, and 1s elsewhere on the main diagonal. Then

$$\bigl\{1_n,\ t_{ij}(m),\ b_k(m) \mid 1 \leq i,j \leq n,\ i \neq j,\ 1 \leq k \leq n-1\bigr\}$$

is a basis $\mathcal{A} \subseteq H$ with $c = 1$.

With a common denominator $d = d(H)$ in hand, we invoke `BasisLattice` from [7, Section 3] with input S, d. If g is any matrix whose columns are the elements of $\texttt{BasisLattice}(S,d)$ then $g \in \mathrm{GL}(n,\mathbb{Q})$ and $H^g \leq \Gamma_n$.

6. Implementation

Our algorithms have been implemented in GAP [13]. For matrix group recognition, we rely on the `recog` package [26] developed by Max Neunhöffer and Ákos Seress.

To demonstrate practicality, and the effect that parameters of the input (degree n, number of generators, size of matrix entries, index in Γ_n) have on performance, we ran experiments on a range of arithmetic groups. Except for the elementary groups (see Proposition 1.12), we chose a value of m that exposed a nontrivial quotient but which we cannot yet prove to be maximal; that is, the groups all contain $\Gamma_{n,m}$.

In Table 1, '# gens' is the number of generators outside $\Gamma_{n,m}$, and l is the decadic logarithm of the largest generator entry. Times (in seconds on a 3.7 GHz Quad-Core late 2013 Mac Pro with 32 GB memory) are for computing the index in Γ_n.

The RAN_i are generated by $\Gamma_{n,m}$ and products of transvections of level dividing m, but seem to be different from any elementary group. Explicit matrices are given at http://www.math.colostate.edu/~hulpke/examples/arithmetic.html.

Table 1
Runtimes for setting up the initial data structure.

Group	# gens	n	m	l	Index in Γ_n	Time
$E_{4,12}$	12	4	$2^4 3^2$	1	$2^{35} 3^{11} 5^2 7 \cdot 13$	0.8
$E_{4,53}$	12	4	53^2	2	$2^9 3^6 5 \cdot 7 \cdot 13^3 53^9 281 \cdot 409$	0.1
$E_{4,3267}$	12	4	$3^6 11^4$	4	$2^{16} 3^{47} 5^4 7 \cdot 11^{27} 13 \cdot 19 \cdot 61$	2
$E_{8,7}$	56	8	7^2	1	$2^{22} 3^9 5^4 7^{35} 19^2 29 \cdot 43 \cdot 1201 \cdot 2801 \cdot 4733$	13
RAN_1	5	4	$2^5 3^2$	21	$2^{50} 3^{18} 5^2 7 \cdot 13$	1
RAN_2	3	4	$2^8 3^4$	21	$2^{74} 3^{30} 5^2 7 \cdot 13$	6
RAN_3	2	4	$2^5 5^2 11^2$	4	$2^{45} 3^4 5^{12} 7^2 11^7 13 \cdot 19 \cdot 31$	9
RAN_4	10	6	$2^2 5^2$	4	$2^{54} 3^8 5^{41} 7^3 11 \cdot 13 \cdot 31^3 71$	0.5
β_{-2}	3	3	2^6	1	$2^{19} 7$	0.6
β_{-1}	3	3	11	1	$7 \cdot 19$	1.2
β_1	3	3	5	1	31	0.4
β_2	3	3	2^5	1	$2^{17} 7$	0.3
β_3	3	3	$3^3 73$	2	$2^3 3^{11} 13 \cdot 1801$	2
β_4	3	3	$2^7 23$	2	$2^{31} 7^2 79$	2
β_5	3	3	$5^3 367$	3	$2^4 3^2 5^{10} 13 \cdot 31 \cdot 3463$	14
β_6	3	3	$2^8 3^3 5$	3	$2^{29} 3^{10} 7 \cdot 13 \cdot 31$	3
β_7	3	3	$7^3 1021$	3	$2^5 3^4 5 \cdot 7^{10} 19 \cdot 347821$	40
ρ_0	3	3	11	1	$7 \cdot 19$	1
ρ_1	3	3	3^4	1	$2^2 3^{15} 13$	0.2
ρ_2	3	3	$5 \cdot 7$	1	$2^4 3^2 5 \cdot 7^2 19 \cdot 31$	1
ρ_3	3	3	13	1	$2^2 3 \cdot 13^2 61$	1
ρ_4	3	3	$3^3 7$	1	$2^4 3^{11} 7^2 13 \cdot 19$	2
ρ_5	3	3	$19 \cdot 31$	2	$2^2 3^3 5 \cdot 31^2 127 \cdot 331$	3

Table 2
Runtimes for stabilizer computations.

Group	m	u	l_1	l_2	Time
$E_{4,12}$	$2^4 3^2$	$(1, 0, 0, 0)$	$2^6 3^3$	1	1
$E_{4,12}$	$2^4 3^2$	$(3, 3, 9, 9)$	2^8	3^4	1.6
$E_{4,12}$	$2^4 3^2$	$(6, 6, 6, 6)$	2^4	$2^4 3^4$	158
RAN_1	$2^5 3^2$	$(0, 0, 0, 1)$	$2^{10} 3^3$	1	1
RAN_1	$2^5 3^2$	$(0, 0, 0, 6)$	2^6	$2^4 3^3$	31
RAN_1	$2^5 3^2$	$(0, 0, 0, 12)$	2^3	$2^7 3^3$	2346
RAN_2	$2^8 3^4$	$(0, 0, 0, 1)$	$2^{22} 3^{10}$	1	6.5
RAN_2	$2^8 3^4$	$(0, 0, 0, 2)$	$2^{18} 3^{10}$	2^4	7.5
RAN_2	$2^8 3^4$	$(0, 0, 0, 3)$	$2^{22} 3^6$	3^4	315
RAN_2	$2^8 3^4$	$(0, 0, 0, 6)$	$2^{18} 3^6$	$2 \cdot 2^3 3^4$	–
β_{-2}	2^6	$(1, 0, 0)$	$2^{13} 3$	1	0.6
β_{-2}	2^6	$(4, 0, 0)$	$2^7 3$	2^6	1.1
β_{-2}	2^6	$(8, 0, 0)$	$2^4 3$	2^9	32
β_3	$3^3 73$	$(1, 0, 0)$	$2^5 3^6 37 \cdot 73$	1	2
β_3	$3^3 73$	$(9, 9, 9)$	$2^6 3^2 37 \cdot 73$	3^6	86
β_5	$5^3 367$	$(1, 0, 0)$	$2^6 3^2 5^3 23 \cdot 61 \cdot 367$	1	16
β_5	$5^3 367$	$(0, 0, 5)$	$2^6 3^2 5 \cdot 23 \cdot 61 \cdot 367$	5^2	17
ρ_1	3^4	$(1, 0, 0)$	3^{11}	1	0.3
ρ_1	3^4	$(3, 0, 0)$	3^8	3^3	0.35
ρ_1	3^4	$(9, 0, 0)$	3^5	3^6	61
ρ_1	3^4	$(9, 9, 9)$	3^5	3^6	72

The β_T and ρ_k are $\Gamma_{3,m}$-closures of their namesakes from [19, p. 414]. Apart from ρ_1, these are known to be arithmetic [19, Theorems 3.1 and 4.1], although a PCS is not known. We discovered that β_7 has larger index than the lower bound in [19].

For a second family of examples we tested our orbit-stabilizer algorithms. Because of their similarity, in Table 2 we only give timings for $\mathtt{Stabilizer}(u, S)$.

The groups $H = \langle S \rangle$ are as in Table 1. Times include the setup for $\overline{H}$. Here l_1 is the length of $\overline{H}\bar{u}$, and l_2 is the length of the orbit of $\underline{u} = \Gamma_{n,m}u$ under the preimage of $\mathrm{Stab}_{\overline{H}}(\bar{u})$. While the u look rather specific, random choices of u do not alter runtimes appreciably. The magnitude of m also has minor impact; if m is composite then the calculation of $\overline{H}\bar{u}$ can be separated into orbits modulo divisors of m.

What does have an impact is divisibility of entries in u by divisors of m, which yields longer orbits of $\underline{u}$. The reason that this affects runtime appears to be twofold. First, we need to compare representatives for $\underline{u}$ using `OrbitGamma_m`. The number of comparisons is quadratic in orbit length. Moreover, integer entries grow quickly even for modest examples (it can happen that stabilizer elements have entries with 10–20 digits). As the auxiliary operations entail iterated gcd calculations and integer factorization, each equivalence test becomes relatively expensive.

We do not report on other procedures from Subsection 3.2 that are essentially computations in $\mathrm{GL}(n, \mathbb{Z}_m)$. Timing these would not give further information about the practicality of computing with arithmetic groups.

Acknowledgments

The authors received support from Science Foundation Ireland grant 11/RFP.1/MTH3212 (Detinko and Flannery) and Simons Foundation Collaboration Grant 244502 (Hulpke). We thank Professors A. Lubotzky, C.F. Miller III, and T.N. Venkataramana for helpful advice.

References

[1] H. Bäärnhielm, D.F. Holt, C.R. Leedham-Green, E.A. O'Brien, A practical model for computation with matrix groups, J. Symbolic Comput. (2014), http://dx.doi.org/10.1016/j.jsc.2014.08.006, in press.

[2] L. Babai, R. Beals, D.N. Rockmore, Deciding finiteness of matrix groups in deterministic polynomial time, in: Proc. of International Symposium on Symbolic and Algebraic Computation, ISSAC '93, ACM Press, 1993, pp. 117–126.

[3] H. Bass, M. Lazard, J.-P. Serre, Sous-groupes d'indice fini dans $\mathrm{SL}(n, \mathbf{Z})$, Bull. Amer. Math. Soc. 70 (1964) 385–392.

[4] H. Bass, J. Milnor, J.-P. Serre, Solution of the congruence subgroup problem for $\mathrm{SL}_n (n \geq 3)$ and $\mathrm{Sp}_{2n} (n \geq 2)$, Inst. Hautes Études Sci. Publ. Math. (33) (1967) 59–137.

[5] J. Brenner, The linear homogeneous group, III, Ann. of Math. (2) 71 (1960) 210–223.

[6] A.S. Detinko, B. Eick, D.L. Flannery, Computing with matrix groups over infinite fields, London Math. Soc. Lecture Note Ser. 387 (2011) 256–270.

[7] A.S. Detinko, D.L. Flannery, W. de Graaf, Integrality and arithmeticity of solvable linear groups, J. Symbolic Comput. (2014), http://dx.doi.org/10.1016/j.jsc.2014.08.011, in press.

[8] A.S. Detinko, D.L. Flannery, E.A. O'Brien, Algorithms for the Tits alternative and related problems, J. Algebra 344 (2011) 397–406.

[9] A.S. Detinko, D.L. Flannery, E.A. O'Brien, Recognizing finite matrix groups over infinite fields, J. Symbolic Comput. 50 (2013) 100–109.

[10] A.S. Detinko, D.L. Flannery, E.A. O'Brien, Algorithms for linear groups of finite rank, J. Algebra 393 (2013) 187–196.

[11] J.D. Dixon, The orbit-stabilizer problem for linear groups, Canad. J. Math. 37 (2) (1985) 238–259.
[12] B. Eick, G. Ostheimer, On the orbit-stabilizer problem for integral matrix actions of polycyclic groups, Math. Comp. 72 (243) (2003) 1511–1529.
[13] The GAP Group, GAP – Groups, Algorithms, and Programming, http://www.gap-system.org.
[14] F. Grunewald, D. Segal, Some general algorithms. I. Arithmetic groups, Ann. of Math. (2) 112 (3) (1980) 531–583.
[15] F. Grunewald, D. Segal, Decision problems concerning S-arithmetic groups, J. Symbolic Logic 50 (3) (1985) 743–772.
[16] A.J. Hahn, O.T. O'Meara, The Classical Groups and K-Theory, Grundlehren Math. Wiss., vol. 291, Springer-Verlag, Berlin, 1989.
[17] A. Hulpke, Computing conjugacy classes of elements in matrix groups, J. Algebra 387 (2013) 268–286.
[18] J. Humphreys, Arithmetic Groups, Lecture Notes in Math., vol. 789, Springer, Berlin, 1980.
[19] D.D. Long, A.W. Reid, Small subgroups of $\mathrm{SL}(3, \mathbb{Z})$, Experiment. Math. 20 (4) (2011) 412–425.
[20] A. Lubotzky, Dimension function for discrete groups, London Math. Soc. Lecture Note Ser. 121 (1986) 254–262.
[21] A. Lubotzky, One for almost all: generation of $\mathrm{SL}(n, p)$ by subsets of $\mathrm{SL}(n, \mathbb{Z})$, Contemp. Math. 243 (1999) 125–128.
[22] A. Lubotzky, D. Segal, Subgroup Growth, Birkhäuser, Basel, 2003.
[23] J.L. Mennicke, Finite factor groups of the unimodular group, Ann. of Math. (2) 81 (1965) 31–37.
[24] C.F. Miller III, personal communication.
[25] J. Milnor, Introduction to Algebraic K-Theory, Ann. of Math. Stud., vol. 72, Princeton Univ. Press, Princeton, NJ, 1971.
[26] M. Neunhöffer, Á. Seress, A data structure for a uniform approach to computations with finite groups, in: ISSAC 2006, ACM, New York, 2006, pp. 254–261.
[27] M. Newman, Integral Matrices, Pure Appl. Math., vol. 45, Academic Press, New York, 1972.
[28] P. Sarnak, Notes on thin matrix groups, in: Thin Groups and Superstrong Approximation, in: Math. Sci. Res. Inst. Publ., vol. 61, 2014, pp. 343–362.
[29] R. Sharma, T.N. Venkataramana, Generations for arithmetic groups, Geom. Dedicata 114 (2005) 103–146.
[30] D.A. Suprunenko, Matrix Groups, Transl. Math. Monogr., vol. 45, American Mathematical Society, Providence, RI, 1976.
[31] B. Sury, The congruence subgroup problem, J. Indian Inst. Sci. (4) 87 (2007) 457–465.
[32] B. Sury, T.N. Venkataramana, Generators for all principal congruence subgroups of $\mathrm{SL}(n, Z)$ with $n \geq 3$, Proc. Amer. Math. Soc. 122 (2) (1994) 355–358.
[33] J.S. Wilson, The normal and subnormal structure of general linear groups, Proc. Cambridge Philos. Soc. 71 (1972) 163–177.