LINEAR GROUPS AND COMPUTATION

A. S. DETINKO AND D. L. FLANNERY

ABSTRACT. We present an exposition of our ongoing project in a new area of applicable mathematics: practical computation with finitely generated linear groups over infinite fields. Methodology and algorithms available for this class of groups are surveyed. We illustrate the solution of hard problems by computer experimentation. Possible avenues for further progress are discussed.

1. INTRODUCTION

A *linear group* (interchangeably, *matrix group*) of degree n over a field $\mathbb{F}$ is a subgroup of the group $\mathrm{GL}(n, \mathbb{F})$ of all $n \times n$ invertible matrices with entries in $\mathbb{F}$. Linear groups have impact throughout mathematics, in diverse branches such as topology, geometry, number theory, and analysis. They are amenable to calculation and modeling transformations, so provide a bridge between algebra and the physical sciences. For example, applications arise in crystallography [29], theoretical physics [21], error-correcting codes [50], cryptography [80], even quantum computing [30].

The study of matrix groups goes back to the origin of group theory. Klein and Lie discovered their role in geometry and differential equations, but the foundations were really laid down by Jordan [63]. Pioneering contributions were also made by Schur, Burnside, Frobenius, and Blichfeldt.

Linear group theory supplements representation theory. It has played a large part in the classification of finite simple groups (see [2], [52, pp. 76–78]) and the theory of infinite solvable groups [66, Chapter 3]. Important classes of groups exhibit linearity: e.g., each polycyclic-by-finite or countable free group has a faithful representation over the integers $\mathbb{Z}$.

Detailed accounts of our subject may be found in the books [47, 102, 105] and surveys [108, 109, 110].

1.1. CGT and matrix groups.

Computational group theory (CGT) is a modern discipline interfacing algebra and computer science. It deals with the design, implementation, and analysis of algorithms for groups and related objects. Progress in CGT is tied to the evolution of computer algebra systems such as GAP [54],

2010 *Mathematics Subject Classification.* Primary 20-02; secondary 20G15, 20H20.

Key words and phrases. Matrix group, algorithm, computation, decidable.

To appear in Expositiones Mathematicae.

MAGMA [17], and SageMath [95]. Other systems (e.g., Maple [74] and Mathematica [75]) allow some group-theoretical computation. We refer to [58, 59, 97, 99] for coverage of aspects of CGT.

Typically a group is input to the computer as permutations, or as a presentation (generating elements and relations between them), or as matrices acting on a vector space. Matrix representations have the advantage of compactness; a huge (even infinite) group can be represented by input of small size. For example, the smallest permutation representation of the Monster simple group has degree about 10^{20}, whereas R. A. Wilson found a linear representation of the Monster in dimension 196882 over the 2-element field. (An early triumph of CGT was its deployment in proofs of existence of sporadic simple groups [58, p. 4].) At the other end of the historical spectrum, Jordan's description of solvable matrix groups over a finite field can be viewed as a prototype CGT algorithm, constructing groups inductively from ones in smaller degrees.

Matrix groups have become a primary focus of CGT. Currently the emphasis is on practical algorithms that permit fruitful computer experimentation. Tremendous effort has been expended on groups over finite fields, coalescing around the 'Matrix Group Recognition Project' [10, 85]. This is now at an advanced stage, thanks to many authors. It comprises a substantial part of the armory of CGT. Given a matrix group G over a finite field, preliminary objectives are to compute the composition series of G and recognize series factors. Thereafter one determines a presentation of G, and proceeds to tasks such as exploring subgroup structure.

1.2. **Computing with linear groups over infinite domains.** Matrix groups over infinite fields have received comparatively scant attention in CGT. Since these groups are potentially infinite, methods for groups over finite fields or for permutation groups are not immediately applicable. Note that infinite linear groups need not be finitely presentable. Even if we have a presentation, we may still be unable to use it or other helpful knowledge about the group efficiently. Complexity issues (such as growth of matrix entries during computation) cause bottlenecks. More seriously, certain algorithmic problems for infinite groups are undecidable: an algorithm to solve the problem for all input does not exist (see [79, Section 5]).

Despite the pitfalls noted above, there is reason to be optimistic. In [9, 14, 15], Babai and his collaborators initiated the development of algorithms for linear groups over infinite fields (mainly the rationals $\mathbb{Q}$). They rely on algorithms for matrix algebras; cf. [94]. These papers establish existence of low complexity (e.g., polynomial-time) solutions of the algorithmic problems considered. Several years later, people became interested in computing with linear groups of special kinds. Representations over $\mathbb{Z}$ figure prominently in the theory of polycyclic groups ([12], [66, Section 9.2]). This is a gateway to algorithms for polycyclic groups where the input is a finite set of generating matrices over $\mathbb{Z}$ or $\mathbb{Q}$. Inspired by Dixon [48], work in this area was undertaken by Lo and Ostheimer [67, 86], then Assmann and

Eick [5, 6]. The latter was incorporated into [4], one of the first software packages dedicated to computing with infinite linear groups.

On a separate front, algorithms for linear algebraic groups have been developed by Cohen et al. beginning in the late 1990s [22, 26]. Here the input groups are not finitely generated, so are given by a finite set of polynomials, or Lie algebras, rather than a finite set of matrices. See [24, 25, 27] for pertinent material here.

A massive amount of classification data for linear groups over infinite fields has accumulated over the years. While much of this is yet to be implemented, some notable classifications are available in GAP and MAGMA. One of these is the library of almost crystallographic groups in [29]. Another is the MAGMA database of irreducible maximal finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$ for $n \leq 23$ derived from work by Plesken et al. on integral representation of finite groups (see also [81]).

Several cognate topics lie outside the scope of this article. Perhaps the most relevant is computational representation theory, which has been active from the 1960s up to now.

1.3. **Algorithms for finitely generated linear groups.** To compute with linear groups over infinite fields, we must first decide how the groups will be designated in a computer. Of course, input will be a finite set. A convenient format is a finite set of generating matrices. Although not every matrix group can be so designated, those that are constitute a major class, and occur frequently in applications.

This article is an exposition of our ongoing project to compute with groups given by a finite set of generating matrices over an (arbitrary) infinite field. We

(i) formulate general methodology;
(ii) apply (i) to design effective algorithms;
(iii) implement the algorithms and demonstrate their practicality.

As (ii) and (iii) indicate, an overarching goal is to obtain algorithms that complete in reasonable time for a wide range of inputs. Ideally, the software would replace traditional mathematics by machine computation, simplifying the solution of problems, and leading to the solution of formerly intractable problems.

Our methodology draws on (classical) theory of linear groups, as in [47, 105]. This equips us with well-tried tools, such as the 'method of finite approximation'. Apart from underpinning the success of our approach, linear group theory and its central concerns guide our choice of problems to give priority. One of these is realizing the Tits alternative computationally. That is, we devise and implement a practical algorithm to test whether a finitely generated linear group is solvable-by-finite (recall that G is X-*by-finite*, or *virtually* X, if there exists a finite index normal subgroup of G that has property X). Then we dispose of further questions for solvable-by-finite linear groups: recognition problems such as testing whether a group is finite, solvable, or nilpotent. Later parts of the article are occupied with the second class of the Tits alternative, specifically arithmetic and Zariski dense

subgroups of semisimple algebraic groups. We conclude by discussing avenues for future research.

The aims of this project were achieved with our colleagues Willem de Graaf, Bettina Eick, Alexander Hulpke, and Eamonn O'Brien, to whom we are deeply grateful.

2. Computing with finitely generated linear groups

This section introduces some of the basic ideas in computing with linear groups by means of congruence homomorphisms.

2.1. **How to input groups.** The computer algebra system in which we implement our algorithms must support computation over the defining field or ring of the input. A field that one often meets in practice is $\mathbb{R}$. Floating point representation of real numbers is popular in applied mathematics, but it is unsuitable for computing with linear groups defined over an arbitrary field $\mathbb{F}$: CGT entails inherently symbolic computation; output should be exact.

Let $G = \langle S \rangle$ where $S = \{g_1, \ldots, g_r\} \subseteq \mathrm{GL}(n, \mathbb{F})$. Suppose for simplicity that $g^{-1} \in S$ if $g \in S$. The group G is defined over the subfield of $\mathbb{F}$ generated by all entries of the g_i. So we assume that $\mathbb{F}$ is a finitely generated extension of its prime subfield $\mathbb{F}_0$.

Lemma 2.1. *There exist algebraically independent* $\mathrm{x}_1, \ldots, \mathrm{x}_m \in \mathbb{F}$, $m \geq 0$, *such that* $\mathbb{F}$ *is a finite extension of the function field* $\mathbb{F}_0(\mathrm{x}_1, \ldots, \mathrm{x}_m)$.

Remark 2.2. For an algorithm to compute the x_i as in Lemma 2.1, see [101].

By Lemma 2.1, 'arbitrary field' for us is one of

(I) $\mathbb{Q}$;
(II) a number field $\mathbb{P}$ (finite degree extension of $\mathbb{Q}$);
(III) a function field $\mathbb{E}(\mathrm{x}_1, \ldots, \mathrm{x}_m)$, $m \geq 1$, where $\mathbb{E} = \mathbb{Q}$, $\mathbb{P}$, or a finite field $\mathbb{F}_q$ of size q;
(IV) a finite degree extension of $\mathbb{E}(\mathrm{x}_1, \ldots, \mathrm{x}_m)$.

Happily, Magma supports computation in these fields. Of course, (I) and (III) are specializations of (II) and (IV), respectively; but we choose to distinguish between the four types. When computing over number fields $\mathbb{P}$, we do not inflate matrix dimension by the degree $|\mathbb{P} : \mathbb{Q}|$ according to the action of $\mathbb{P}$ on a $\mathbb{Q}$-basis of $\mathbb{P}$, to get matrices with entries in $\mathbb{Q}$. This is a standard trick, but risks increasing the dimension beyond the boundaries of practicality.

2.2. **Finite approximation.** Let R be the subring of $\mathbb{F}$ generated by the entries of all elements of S. Hence R is a finitely generated integral domain and $G \leq \mathrm{GL}(n, R)$.

Lemma 2.3 ([105, p. 50])**.** *The ring* R *is approximated by finite fields; i.e.,*

(i) *if ϱ is a maximal ideal of R then R/ϱ is a finite field,*
(ii) *if $a \in R \setminus \{0\}$ then R has a maximal ideal not containing a.*

Lemma 2.3 underlies the following, due to Mal'cev (see [108, (2.1), p. 74]).

Theorem 2.4. *Each finitely generated subgroup of $\mathrm{GL}(n, \mathbb{F})$ is approximated by matrix groups of degree n over finite fields.*

Theorem 2.4 is at the heart of our computational strategy. The word 'approximated' expresses the residual finiteness of G: if $g \in G \setminus \{1\}$ then there exists a homomorphism f from G onto a subgroup of $\mathrm{GL}(n, q)$ for some prime power q, such that $f(g) \neq 1$. In the proof of Theorem 2.4 in [105, Theorem 4.2, p. 51], f is a *congruence homomorphism*. We now begin to set up the formalism that we adopt to compute with these homomorphisms.

Let ϱ be a (proper) ideal of an associative unital ring Δ. Natural surjection $\Delta \to \Delta/\varrho$ induces an algebra homomorphism $\mathrm{Mat}(n, \Delta) \to \mathrm{Mat}(n, \Delta/\varrho)$, which then restricts to a group homomorphism $\mathrm{GL}(n, \Delta) \to \mathrm{GL}(n, \Delta/\varrho)$. We denote all these homomorphisms by φ_ϱ. The *principal congruence subgroup (PCS)* $\Gamma_{n,\varrho}$ *of level* ϱ is the kernel of φ_ϱ in $\mathrm{GL}(n, \Delta)$. Theorem 2.4 tells us that for each $g \neq 1$ in G there exists a maximal ideal ϱ of R such that $\varphi_\varrho(g)$ is a non-identity element of the general linear group $\mathrm{GL}(n, R/\varrho)$ over the finite field R/ϱ. The accuracy of information about G provided by its congruence images $\varphi_\varrho(G)$, and how we compute with matrix groups over finite rings, govern the effectiveness of this overall approach to computing with finitely generated subgroups of $\mathrm{GL}(n, \mathbb{F})$.

2.3. **Constructing congruence homomorphisms.** We explain how to construct congruence homomorphisms for the main field types (I)–(IV), in line with Theorem 2.4.

2.3.1. If $\mathbb{F} = \mathbb{Q}$ then $R = \frac{1}{\mu}\mathbb{Z} = \mathbb{Z}[\frac{1}{\mu}]$, the ring of rationals whose denominators are powers of a fixed integer μ. We can take μ to be the least common multiple of the denominators of the entries of the g_i. For any positive $b \in \mathbb{Z}$ not dividing μ, entrywise reduction of the g_i modulo b defines a congruence homomorphism φ_ϱ where $\varrho = bR$. We write 'b' in place of 'ϱ' as a subscript in the notation. If $b = p$ is prime then ϱ is a maximal ideal of R and $R/\varrho = \mathbb{F}_p$. Set $\varphi_{1,p} := \varphi_p$.

2.3.2. Let $\mathbb{F}$ be a number field $\mathbb{P}$ of degree k over $\mathbb{Q}$. There is an algebraic integer α with minimal polynomial $f(t) = a_0 + a_1 t + \cdots + a_{k-1}t^{k-1} + t^k \in \mathbb{Z}[t]$ such that $\mathbb{P} = \mathbb{Q}(\alpha)$. We have $R \subseteq \frac{1}{\mu}\mathbb{Z}[\alpha]$ for some $\mu \in \mathbb{Z}$. Let $p \in \mathbb{Z}$ be a prime not dividing μ, and set $\bar{b}_i = \varphi_p(b_i)$, $\bar{a}_i = \varphi_p(a_i)$. For any root $\bar{\alpha}$ of $\bar{f}(t) = \sum_{i=0}^{k-1} \bar{a}_i t^i$, define the homomorphism $\varphi_{2,p}$ of R onto the finite field $\mathbb{F}_p(\bar{\alpha})$ by

$$\textstyle\sum_{i=0}^{k-1} b_i \alpha^i \mapsto \sum_{i=0}^{k-1} \bar{b}_i \bar{\alpha}^i.$$

Let $\bar{f}_j(t)$ be an irreducible factor of $\bar{f}(t)$. If $f_j(t)$ is a preimage of $\bar{f}_j(t)$ in $\mathbb{Z}[t]$ then the ideal of R generated by p and $f_j(\alpha)$ is maximal, and $\varphi_{2,p} = \varphi_\varrho$.

2.3.3. Let $\mathbb{F} = \mathbb{E}(\mathrm{x}_1, \ldots, \mathrm{x}_m)$. Then $R \subseteq \frac{1}{\mu}\mathbb{E}[\mathrm{x}_1, \ldots, \mathrm{x}_m]$ for some polynomial $\mu = \mu(\mathrm{x}_1, \ldots, \mathrm{x}_m) \in \mathbb{E}[\mathrm{x}_1, \ldots, \mathrm{x}_m]$. Let $\alpha = (\alpha_1, \ldots, \alpha_m)$ be a non-root of μ, where each α_i is in the algebraic closure $\overline{\mathbb{E}}$ of $\mathbb{E}$. The α_i can be chosen in $\mathbb{E}$ if $\operatorname{char}\mathbb{E} = 0$ and in a finite extension $\mathbb{F}_{q^c}$ if $\mathbb{E} = \mathbb{F}_q$. Define $\varphi_{3,\alpha}$ on R to be the homomorphism that substitutes α_i for x_i, $1 \leq i \leq m$. Then $\varphi_{3,\alpha,p} := \varphi_{i,p} \circ \varphi_{3,\alpha}$ where $i = 1$ if $\mathbb{E} = \mathbb{Q}$ and $i = 2$ if $\mathbb{E} \neq \mathbb{Q}$ is a number field.

2.3.4. Suppose that $\mathbb{F}$ is an extension of $\mathbb{L} = \mathbb{E}(\mathrm{x}_1, \ldots, \mathrm{x}_m)$ of degree e: say $\mathbb{F} = \mathbb{L}(\beta)$. Such β exist if $\operatorname{char}\mathbb{F} = 0$ or $\mathbb{F}$ is perfect in positive characteristic. Let $f(t) = t^e + a_{e-1}t^{e-1} + \cdots + a_1 t + a_0$ be the minimal polynomial of β. Then $R \subseteq \frac{1}{\mu}\mathbb{L}_0[\beta]$ where $\mu \in \mathbb{L}_0 = \mathbb{E}[\mathrm{x}_1, \ldots, \mathrm{x}_m]$. We may assume that $f(t) \in \mathbb{L}_0[t]$.

Define $\varphi_{4,\alpha}$ on $\mathrm{GL}(n, R)$ as follows. Take a non-root $\alpha = (\alpha_1, \ldots, \alpha_m) \in \overline{\mathbb{E}}^m$ of μ. (Remember that we can find $\alpha_i \in \mathbb{E}$ if $\operatorname{char}\mathbb{E} = 0$ and $\alpha_i \in \mathbb{F}_{q^c}$ if $\mathbb{E} = \mathbb{F}_q$.) Further, let $\tilde{\beta}$ be a root of $\tilde{f}(t) = \sum_{i=0}^{e-1} \tilde{a}_i t^i + t^e$, where $\tilde{a}_i = \varphi_{3,\alpha}(a_i)$. Each element of $\frac{1}{\mu}\mathbb{L}_0[\beta]$ has a unique expression as $\sum_{i=0}^{e-1} c_i\beta^i$ for $c_i \in \frac{1}{\mu}\mathbb{L}_0$. Then

$$\varphi_{4,\alpha} : \textstyle\sum_{i=0}^{e-1} c_i\beta^i \mapsto \sum_{i=0}^{e-1} \tilde{c}_i\tilde{\beta}^i$$

where $\tilde{c}_i = \varphi_{3,\alpha}(c_i)$. In zero characteristic, $\varphi_{4,\alpha,p} := \varphi_{i,p} \circ \varphi_{4,\alpha}$ with $i = 1$ when $\mathbb{E} = \mathbb{Q}$ and $\tilde{\beta} \in \mathbb{Q}$, and $i = 2$ when $\mathbb{E} = \mathbb{P}$.

As 2.3.1–2.3.4 show, constructing congruence homomorphisms is straightforward. The main operations are reduction modulo primes $p \in \mathbb{Z}$ and substitution of indeterminates. These define an appropriate maximal ideal ϱ and hence image field. The sort of ideal ϱ chosen will depend on the problem at hand.

2.4. **Computational finite approximation.** We continue with the notation above: $R \subseteq \mathbb{F}$ is determined by a generating set for $G \leq \mathrm{GL}(n, \mathbb{F})$, ϱ is a maximal ideal of R, and φ_ϱ is the corresponding homomorphism $\mathrm{GL}(n, R) \to \mathrm{GL}(n, R/\varrho)$, with R/ϱ a finite field. Denote the kernel of φ_ϱ on G by G_ϱ, i.e., $G_\varrho = G \cap \Gamma_{n,\varrho}$ where $\Gamma_{n,\varrho}$ is $\ker\varphi_\varrho$ on $\mathrm{GL}(n, R)$.

There are two parts of our method, one for $\varphi_\varrho(G)$ and one for $G_\varrho \trianglelefteq G$. Since G_ϱ has finite index in a finitely generated group, it is finitely generated too. None of our algorithms call for a full generating set of G_ϱ (which may be hard or even impossible to acquire), but rather a *normal generating set*: a finite subset N of G_ϱ such that G_ϱ is the normal closure $\langle N\rangle^G$ of $\langle N\rangle$ in G. There is a standard CGT procedure to obtain N; see [58, pp. 299–300]. For this we need a presentation of $\varphi_\varrho(G)$ in the form $\langle \varphi_\varrho(g_1), \ldots, \varphi_\varrho(g_r) \,|\, w_1, \ldots, w_l\rangle$ where $\{g_1, \ldots, g_r\}$ is the input generating set S of G and the w_j are words in the $\varphi_\varrho(g_i)$. Efficient algorithms to compute such a presentation are available [7]. Replacing $\varphi_\varrho(g_i)$ by g_i in each w_j, we get words $\tilde{w}_j$ over S. Then $N = \{\tilde{w}_1, \ldots, \tilde{w}_l\}$. Label this process $\texttt{NormalGenerators}(S, \varphi_\varrho)$.

We summarize our computational version of finite approximation.

(1) Select a maximal ideal ϱ of R.

(2) Construct the congruence image $\varphi_\varrho(G)$ over the finite field R/ϱ.
(3) Find a presentation of $\varphi_\varrho(G)$.
(4) Compute a normal generating set of G_ϱ.

The bulk of the computation is in step 3; but it is done over a finite rather than infinite domain. This eases complexity issues such as matrix entry growth. We also gain access to the powerful algorithms for matrix groups over finite fields.

The clarity of our method flows from deep results such as Theorem 2.4, which ensure that the method may be converted into an efficient algorithm. The solution of the orbit-stabilizer problem for nilpotent-by-finite groups over $\mathbb{Q}$ presented in [48] is a model for this kind of computing with infinite linear groups. As noted previously, Dixon's paper was an impetus for subsequent work by Assmann, Eick, and Ostheimer on computing with polycyclic groups over $\mathbb{Q}$. Other algorithms for infinite matrix groups that use congruence homomorphisms appear in [14, 15, 93]. Those algorithms feature randomization, which we have so far eschewed.

3. Deciding finiteness

An obvious launching point for the investigation of a potentially infinite group is to decide whether or not it is finite. Algorithms to test finiteness of finitely generated matrix groups over $\mathbb{Q}$ were developed in [8, 9]. These mix deterministic and randomized techniques, and have integrality testing as a subprocedure. Finiteness testing of groups over fields other than $\mathbb{Q}$ is considered in [31, 62, 93]; none of the algorithms from those papers were implemented. Ideas from [9] are utilized in the GAP package GRIM [13]. Both GAP and MAGMA use [9] for their default procedures to test finiteness over $\mathbb{Q}$. In this section we present an algorithm to test finiteness over any field.

3.1. **Selberg–Wehrfritz theorems.** By a result of Schur's [102, p. 181], if the finitely generated subgroup G of $\mathrm{GL}(n,\mathbb{F})$ is periodic (all elements are torsion, i.e., have finite order) then G is finite. Usually we expect the torsion part of G to be 'small', which in characteristic zero means that G is virtually torsion-free.

We define more terminology. An element g of $\mathrm{GL}(n,\mathbb{F})$ is *unipotent* if it is conjugate to a unitriangular matrix in $\mathrm{GL}(n,\mathbb{F})$; equivalently, g has characteristic polynomial $(\mathrm{x}-1_n)^n$. If $\mathrm{char}\,\mathbb{F}=p>0$ then the unipotent elements of $\mathrm{GL}(n,\mathbb{F})$ are precisely its p-elements. A subgroup H of $\mathrm{GL}(n,\mathbb{F})$ is called unipotent if every element of H is unipotent; equivalently, H may be conjugated into the group $\mathrm{UT}(n,\mathbb{F})$ of all $n\times n$ upper unitriangular matrices over $\mathbb{F}$. In positive characteristic p, the unipotent subgroups of $\mathrm{GL}(n,\mathbb{F})$ are the p-subgroups. Unipotent groups are nilpotent.

We now state a well-known key result for finitely generated linear groups (see [105, Corollary 4.8, p. 56]).

Theorem 3.1. *G has a normal subgroup H of finite index whose torsion elements are unipotent. In particular, if $\mathrm{char}\,\mathbb{F}=0$ then H is torsion-free.*

Selberg proved Theorem 3.1 for zero characteristic; Wehrfritz extended it to all characteristics. The proof in [105, p. 56] does not give H as a congruence subgroup; unlike the following (which implies Theorem 3.1).

Proposition 3.2 ([45, Proposition 2.1])**.** *Let Δ be a Noetherian integral domain, and ρ be a maximal ideal of Δ. If $g \in \Gamma_{n,\rho}$ has finite order then $|g|$ is a power of* $\mathrm{char}(\Delta/\rho)$.

Finitely generated integral domains are Noetherian. Proposition 3.2 specifies ideals ϱ such that $G_\varrho = H$ as per Theorem 3.1. For such ϱ we call φ_ϱ an *SW-homomorphism*. If $\mathrm{char}\,\mathbb{F} > 0$ and ϱ is any maximal ideal of R then φ_ϱ is an SW-homomorphism.

Proposition 3.2 is still not enough for our purposes. We also need

Proposition 3.3 ([102, Theorem 4, p. 70])**.** *Suppose that Δ is a Dedekind domain of characteristic zero, and ρ is a maximal ideal of Δ such that* $\mathrm{char}(\Delta/\varrho)$ *is an odd prime p. If $p \notin \varrho^2$ then $\Gamma_{n,\rho}$ is torsion-free.*

If $\Delta = \mathbb{Z}$ then Proposition 3.3 is a result of Minkowski: $\Gamma_{n,p}$ is torsion-free for odd primes p (indeed $\Gamma_{n,m}$ is torsion-free for any odd integer m [83, Theorem IX.8]).

3.2. **Constructing SW-homomorphisms.** We adhere to the notation and conventions of Subsection 2.3.

3.2.1. If $R = \frac{1}{\mu}\mathbb{Z}$ then $\varphi_{1,p}$ is an SW-homomorphism for any odd prime p not dividing μ.

3.2.2. Let $\mathbb{F} = \mathbb{P} = \mathbb{Q}(\alpha)$ for an algebraic number α with minimal polynomial $f(t)$ of degree k; then $R \subseteq \frac{1}{\mu}\mathbb{Z}[\alpha]$. Let p be a prime not dividing μ, such that either $p > nk + 1$ (so that $\mathrm{GL}(n, \mathbb{F})$ does not contain non-trivial p-subgroups) or p does not divide the discriminant of $f(t)$. It follows from Propositions 3.2 and 3.3 that $\varphi_{2,p}$ is an SW-homomorphism (see [45, p. 103]).

3.2.3. Let $\mathbb{F} = \mathbb{E}(\mathrm{x}_1, \ldots, \mathrm{x}_m)$ where $\mathbb{E}$ is $\mathbb{Q}$, $\mathbb{P}$, or $\mathbb{F}_q$. By Proposition 3.2, $\varphi_{3,\alpha}$ and $\varphi_{3,\alpha,p}$ are SW-homomorphisms.

3.2.4. Let $\mathbb{F} = \mathbb{L}(\beta)$ where $\mathbb{L} = \mathbb{E}(\mathrm{x}_1, \ldots, \mathrm{x}_m)$ and $|\mathbb{F} : \mathbb{L}| = e$, so $R \subseteq \frac{1}{\mu}\mathbb{L}_0[\beta]$. If $\mathrm{char}\,\mathbb{F} = 0$ then $\varphi_{4,\alpha}$ has torsion-free kernel by Proposition 3.2; hence the composition $\varphi_{4,\alpha,p}$ of $\varphi_{4,\alpha}$ with φ_p as in 3.2.1 or 3.2.2 is an SW-homomorphism. If $\mathbb{E} = \mathbb{F}_q$ then $\varphi_{4,\alpha}$ is already an SW-homomorphism.

Thus, SW-homomorphisms always exist, and there are infinitely many ϱ such that φ_ϱ is an SW-homomorphism. Moreover, if $\mathbb{F}$ is $\mathbb{Q}$ or $\mathbb{P}$ then φ_ϱ is an SW-homomorphism for all but a finite number of ϱ (cf. [45, Section 3.5]).

3.3. **The algorithm.** The next lemma recaps the definition of SW-homomorphism.

Lemma 3.4. *Let φ_ϱ be an SW-homomorphism on $G \leq \mathrm{GL}(n, R)$.*

(i) *Suppose that* $\mathrm{char}\, R = 0$*. Then G is finite if and only if $G_\varrho = 1$.*
(ii) *Suppose that* $\mathrm{char}\, R = p > 0$*. Then G is finite if and only if G_ϱ is a finite p-group (i.e., is unipotent).*

Lemma 3.4 guarantees correctness of the following.

`IsFinite`(S)

Input: a finite subset S of $\mathrm{GL}(n, R)$, $\mathrm{char}\, R = p \geq 0$.
Output: `true` if $G = \langle S \rangle$ is finite; `false` otherwise.

(1) Select an ideal ϱ of R such that φ_ϱ is an SW-homomorphism, and construct $\varphi_\varrho(G) \leq \mathrm{GL}(n, q)$ where $|R/\varrho| = q$.
(2) $N :=$ `NormalGenerators`(S, φ_ϱ).
(3) If $p = 0$ and $N = 1$, or $p > 0$ and $\langle N \rangle^G$ is unipotent, then return `true`; else return `false`.

If $\mathrm{char}\, R = 0$ then to confirm finiteness of G it is enough to verify that N (i.e., G_ϱ) is trivial. If $p > 0$ then we use the procedure `IsUnipotentClosure`(T, G) from [43, Section 5.2] in Step 3. For a finite set $T \subseteq \mathrm{GL}(n, \mathbb{F})$, this tests whether $\langle T \rangle^G$ is unipotent. The computation is done in the enveloping algebra of $\langle T \rangle^G$ (smallest subalgebra of $\mathrm{Mat}(n, \mathbb{F})$ containing $\langle T \rangle^G$). Testing unipotency of finitely generated subgroups of $\mathrm{GL}(n, \mathbb{F})$ is easier; see, e.g., [33, p. 108].

As an auxiliary step, we might check whether randomly chosen elements (words over S) have finite order: by Schur's result, infinite G contains elements of infinite order. This has turned out to be a reliable way of certifying infiniteness quickly.

For certain input `IsFinite` may be further modified. If $\mathbb{F}$ is a function field then we only need the substitution homomorphism $\varphi_{3,\alpha}$ and computation with enveloping algebras, in place of `NormalGenerators`. This may be helpful insofar as the words that arise are shorter than the words over S that can arise in a run of `NormalGenerators`. See [35, 42].

Apart from being a practical algorithm valid over an arbitrary infinite field, `IsFinite` justifies decidability of the finiteness problem in the class of finitely generated linear groups.

3.4. **Recognition of finite matrix groups.** Let $G \leq \mathrm{GL}(n, \mathbb{F})$ be finite. If $\mathrm{char}\, \mathbb{F} = 0$ then an SW-homomorphism φ_ϱ maps G isomorphically onto $\varphi_\varrho(G)$, a matrix group over some finite field $\mathbb{F}_q$. If $\mathrm{char}\, \mathbb{F} = p > 0$ then G_ϱ could be a non-trivial finite p-group. However, an SW-isomorphism in this case may be obtained from an ad hoc recursion, as in [45, Section 4.3].

Once we have an isomorphic copy $\varphi_\varrho(G) \leq \mathrm{GL}(n, q)$ of G in some $\mathrm{GL}(n, q)$, we 'recognize' G by subjecting $\varphi_\varrho(G)$ to the gamut of algorithms for matrix groups

over finite fields [7, 10, 82]. Amongst other things, we can: compute $|G|$; test whether G is solvable or nilpotent; compute a composition series of G; find a presentation of G; test membership of $g \in \mathrm{GL}(n, \mathbb{F})$ in G.

4. Computing with virtually solvable linear groups

We move on to the next phase of investigating a finitely generated linear group.

4.1. **The Tits alternative.** Tits proved the following milestone result [104].

Theorem 4.1 (The Tits alternative)**.** *A finitely generated subgroup of* $\mathrm{GL}(n, \mathbb{F})$ *either is solvable-by-finite, or contains a non-abelian free subgroup.*

If $\mathrm{char}\, \mathbb{F} = 0$ then the conclusion of Theorem 4.1 holds for all $G \leq \mathrm{GL}(n, \mathbb{F})$. Results analogous to the Tits alternative for other kinds of groups are given in [19], [46, Section 2], [65], and [98, Section 4.5, pp. 154–162].

The Tits alternative divides all finitely generated linear groups into two disparate classes, and it is vital that we are able to determine the class to which a given group belongs. An algorithm for doing this is given later in the section.

Proposition 4.2 ([105, Corollary 10.18, p. 146])**.** *Linear groups satisfying the maximal condition on subgroups are polycyclic-by-finite, and vice versa.*

Proposition 4.2 points to the computational tractability of polycyclic-by-finite groups. It implies termination of a procedure to compute the normal closure $\langle N \rangle^G$ of a finite subset N in a polycyclic-by-finite (linear) group G.

We note another condition for virtual solvability.

Theorem 4.3 ([105, Theorem 10.9, p. 141])**.** *Suppose that each finitely generated subgroup of the linear group G can be generated by d elements, for some fixed positive integer d. Then G is solvable-by-finite.*

Existing proofs of Theorem 4.1 (as in, e.g., [46, 104]) do not translate into a practical algorithm to test virtual solvability (over any field $\mathbb{F}$). We proceed instead by way of computational finite approximation.

4.2. **Solvable-by-finite linear groups and congruence homomorphisms.** A *block (upper) triangular group* in $\mathrm{GL}(n, \mathbb{F})$ is a subgroup of the form

$$H = \begin{pmatrix} H_1 & * & \cdots & * \\ 0 & H_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & H_k \end{pmatrix}$$

with zeros beneath the 'diagonal part' $\mathrm{diag}(H_1, \ldots, H_k)$, where $H_i \leq \mathrm{GL}(n_i, \mathbb{F})$. If all $H_i = 1$ then $H \leq \mathrm{UT}(n, \mathbb{F})$; and if all $n_i = 1$ then $H \leq \mathrm{T}(n, \mathbb{F})$, the group of upper triangular matrices. Any subgroup of $\mathrm{GL}(n, \mathbb{F})$ is conjugate to one of the form $(\dagger)$ where each H_i is irreducible as a subgroup of $\mathrm{GL}(n_i, \mathbb{F})$. If H

is unipotent-by-abelian then it is conjugate in $\mathrm{GL}(n, \overline{\mathbb{F}})$ to a subgroup of $\mathrm{T}(n, \overline{\mathbb{F}})$. The set of all upper unitriangular matrices in H is a unipotent normal subgroup $U(H)$; this is the kernel of the projection of H onto its 'completely reducible part' $\mathrm{diag}(H_1, \ldots, H_k)$.

Theorem 4.4 (Lie–Kolchin–Mal'cev)**.** *Each solvable-by-finite linear group contains a unipotent-by-abelian subgroup of finite index.*

There are algebraic and topological proofs of Theorem 4.4 (see [102, Theorem 7, p. 135] and [105, Theorem 5.8, p. 77]). The theorem implies that a solvable-by-finite linear group can be conjugated to the form $(\dagger)$ with (irreducible) abelian-by-finite blocks H_i.

The next result enables us to compute with a finite index unipotent-by-abelian subgroup of a given solvable-by-finite linear group.

Theorem 4.5 (Wehrfritz [106])**.** *Let $G \leq \mathrm{GL}(n, R)$ be solvable-by-finite, and let ϱ be an ideal of R. Then G_ϱ is unipotent-by-abelian if*

(i) *R/ϱ has prime characteristic greater than n; or*
(ii) *R is a Dedekind domain of characteristic zero, ϱ is a maximal ideal of R, R/ϱ has odd characteristic p, and $p \notin \varrho^{p-1}$.*

Remark 4.6. G_ϱ in Theorem 4.5 (ii) is Zariski-connected (see Subsection 5.2).

Theorem 4.5 is proved in [48, Lemma 9] for $\mathbb{F} = \mathbb{Q}$. This was background for the algorithm in [5] to test virtual solvability over $\mathbb{Q}$. The Monte Carlo algorithm of [14] to decide the Tits alternative over $\mathbb{Q}$ relies on solvability testing of matrix groups over finite fields [73].

4.3. **A computational version of the Tits alternative.** Call φ_ϱ for an ideal $\varrho \subseteq R$ as in Theorem 4.5 a *W-homomorphism*.

4.3.1. $\varphi_{1,p}$ for an odd prime $p \in \mathbb{Z}$ as in 3.2.1 is a W-homomorphism.

4.3.2. $\varphi_{2,p}$ as in 3.2.2 is a W-homomorphism if either $p > n$, or p is coprime to the discriminant of the minimal polynomial $f(t)$ of α.

4.3.3. If $\mathrm{char}\,\mathbb{F} = 0$ then $\varphi_{3,\alpha,p}$ is a W-homomorphism; if $\mathrm{char}\,\mathbb{F} = p > n$ then the substitution map $\varphi_{3,\alpha}$ on its own is a W-homomorphism (see 3.2.3).

4.3.4. If $\mathrm{char}\,\mathbb{F} = 0$ then $\varphi_{4,\alpha,p}$ is a W-homomorphism; if $\mathbb{E} = \mathbb{F}_q$ then $\varphi_{4,\alpha}$ is a W-homomorphism (see 3.2.4).

Our computational realization of the Tits alternative follows.

`IsSolvableByFinite`(S)

Input: $S = \{g_1, \ldots, g_r\} \subseteq \mathrm{GL}(n, R)$.
Output: `true` if $G = \langle S \rangle$ is solvable-by-finite; `false` otherwise.

(1) Select $\varrho \subseteq R$ such that φ_ϱ is a W-homomorphism, and construct $\varphi_\varrho(G)$.
(2) $N := \texttt{NormalGenerators}(S, \varphi_\varrho)$.
(3) Return `true` if $\langle N \rangle^G$ is unipotent-by-abelian; else return `false`.

Step 3 is a matrix algebra computation. (The normal closure cannot be computed directly by a standard recursion, as this may not terminate if G is not polycyclic-by-finite; cf. Proposition 4.2.) To find a basis of the enveloping algebra $\langle G_\varrho \rangle_{\mathbb{F}}$, or to test whether $\langle N \rangle^G$ is unipotent-by-abelian, only a normal generating set for G_ϱ is required. We already have this from Step 2. Even if we can find a full generating set of G_ϱ, the enveloping algebra method may still be preferable to a direct normal closure computation (see the penultimate paragraph of Subsection 3.3).

4.4. **Other group-theoretic properties.** We now test narrower attributes of the input solvable-by-finite linear group G: whether it is nilpotent-by-finite, abelian-by-finite, central-by-finite, solvable, nilpotent. Maintaining a common theme, we give practical algorithms that justify decidability.

A class ostensibly not too far removed from finitely generated solvable-by-finite groups is polycyclic-by-finite groups. However, there is in fact a large distance between the classes: a polycyclic-by-finite group is finitely presentable, has every subgroup finitely generated, and satisfies the maximal condition on subgroups; whereas none of this is true in general for solvable-by-finite groups. So algorithmic methods for polycyclic-by-finite groups may not work at all for solvable-by-finite groups (cf. the comments after Proposition 4.2).

To test solvability of G we add checking solvability of $\varphi_\varrho(G)$ to `IsSolvableByFinite`. This single extra step is readily accomplished; see [5, 7, 73].

For nilpotent-by-finite groups, we combine some theory of nilpotent linear groups with the next result.

Proposition 4.7 ([43, Corollary 5.2])**.** *Suppose that R is a Dedekind domain of characteristic zero, and ϱ is a maximal ideal of R such that $\mathrm{char}(R/\varrho) = p > 2$, where $p \notin \varrho^{p-1}$. Then $G \leq \mathrm{GL}(n, R)$ is nilpotent-by-finite (respectively, abelian-by-finite) if and only if G_ϱ is nilpotent (respectively, abelian).*

Proposition 4.7 follows from Theorem 4.5 (ii). Since it is connected, G_ϱ is nilpotent (respectively, abelian) if it is nilpotent-by-finite (respectively, abelian-by-finite).

Denote by g_d, $g_u \in \mathrm{GL}(n, \mathbb{F})$ the diagonalizable and unipotent parts of $g \in \mathrm{GL}(n, \mathbb{F})$. So g_d is conjugate to a diagonal matrix over $\overline{\mathbb{F}}$, g_u is unipotent, and $g = g_d g_u = g_u g_d$. This is the Jordan decomposition of g; see [105, Theorem 7.2, p. 91]. For $X \subseteq \mathrm{GL}(n, \mathbb{F})$ set $X_d = \{h_d \mid h \in G\}$, $X_u = \{h_u \mid h \in G\}$.

Lemma 4.8. *Let $G = \langle S \rangle \leq \mathrm{GL}(n, \mathbb{F})$.*

(i) *G is nilpotent if and only if $\langle S_d \rangle$, $\langle S_u \rangle$ are nilpotent and centralize each other.*

(ii) *If G is nilpotent then $G \leq \langle S_d \rangle \times \langle S_u \rangle$.*

Proofs of Lemma 4.8 are in [34] and [102].
Now we can state an algorithm to test virtual nilpotency, based on the above.

`IsNilpotentByFinite`(S)

Input: a finite subset S of $\mathrm{GL}(n, R)$, R a Dedekind domain of characteristic 0.
Output: `true` if $G = \langle S \rangle$ is nilpotent-by-finite; otherwise `false`.

(1) Select ϱ such that φ_ϱ is a W-homomorphism.
(2) $N :=$ `NormalGenerators`(S, φ_ϱ).
(3) If $\langle x^g : x \in N_d,\ g \in G \rangle$ is abelian, $\langle y^g : y \in N_u,\ g \in G \rangle$is unipotent, and these two groups commute elementwise, then return `true`; else return `false`.

Step 3 uses `IsAbelianClosure` and `IsUnipotentClosure` from [43, p. 404]. Once more these involve computation in related enveloping algebras.

The procedure `IsAbelianByFinite`(S) tests whether $G = \langle S \rangle \leq \mathrm{GL}(n, R)$ is abelian-by-finite, where R is a Dedekind domain of characteristic zero. All steps are the same as in `IsNilpotentByFinite` except for Step 3, which now simply returns `IsAbelianClosure`(N, S).

Next we show how to decide whether G is central-by-finite.

Lemma 4.9 ([43, Corollary 5.8])**.** *Let $G \leq \mathrm{GL}(n, R)$ where $\mathrm{char}\, R = 0$, and let φ_ϱ be an SW-homomorphism on $\mathrm{GL}(n, R)$. Then G is central-by-finite if and only if G_ϱ is central in G.*

If G is central-by-finite then the commutator subgroup $[G, G]$ generated by all $[x, y] = x^{-1}y^{-1}xy$ is finite. The non-trivial direction of Lemma 4.9 follows from this and G_ϱ being a torsion-free normal subgroup of G. Thus `IsCentralByFinite` returns `true` if the input S centralizes `NormalGenerators`(S, φ_ϱ) and `false` otherwise.

We round out the section with nilpotency testing (in characteristic zero). This will not be a simple modification of `IsNilpotentByFinite`, as an extension of one nilpotent group by another need not be nilpotent (cf. testing solvability via `IsSolvableByFinite`).

Lemma 4.10 ([34, Lemma 4.9])**.** *Let $G \leq \mathrm{GL}(n, R)$ be nilpotent, $\mathrm{char}\, R = 0$, and suppose that $G = G_d$. If φ_ϱ is an SW-homomorphism then $G_\varrho \leq Z(G)$.*

Lemmas 4.8 and 4.10 lead to the following.

`IsNilpotent`(S)

Input: a finite subset S of $\mathrm{GL}(n, \mathbb{F})$, $\mathrm{char}\, \mathbb{F} = 0$.

Output: `true` if $G = \langle S \rangle$ is nilpotent; otherwise `false`.

(1) $H := \langle S_d \rangle$, $K := \langle S_u \rangle$.
(2) If K is not unipotent, or $[H, K] \neq 1$, then return `false`.
(3) Select ϱ such that φ_ϱ is an SW-homomorphism on $\mathrm{GL}(n, R)$. If $\varphi_\varrho(G)$ is not nilpotent then return `false`.
(4) If $H_\varrho \not\leq Z(H)$ then return `false`; else return `true`.

For nilpotency testing over finite fields (Step 3), see [33]. The papers [33, 34] contain many more algorithms for nilpotent linear groups.

4.5. **Structure of solvable-by-finite linear groups.** Further study of a solvable-by-finite subgroup $G = \langle S \rangle$ of $\mathrm{GL}(n, \mathbb{F})$ begins by computing its main structural components. This leads inevitably to a consideration of ranks.

We may assume that G is block triangular with completely reducible abelian-by-finite diagonal part (cf. Subsection 4.2). Let π be the projection of G onto its diagonal part. Then $\ker \pi = U(G)$, the unipotent radical of G. Certainly $\pi(G)$ is finitely generated, whereas $U(G)$ is finitely generated if and only if G is polycyclic-by-finite.

We note two related procedures: `IsCR` and `CRPart`. `IsCR` tests whether G is completely reducible; equivalently, whether $U(G) = 1$. `CRPart` returns a generating set of $\pi(G)$. Here only the least complicated case $\mathrm{char}\, R = 0$ is reviewed.

Let φ_ϱ be a W-homomorphism for G. Then G is completely reducible if and only if G_ϱ is completely reducible abelian. The latter can be tested by customary manipulations in an enveloping algebra of $N =$ `NormalGenerators`(S, φ_ϱ); see [43, Section 4]. When G is nilpotent-by-finite, G is completely reducible if and only if $N_u = 1$; when G is nilpotent, it suffices to check whether $S_u = 1$. `CRPart` is described in [44, Section 4.2]. The completely reducible part of nilpotent G is $\langle S_d \rangle$.

So we can decide whether G is completely reducible. We reiterate that although $U(G)$ may not be finitely generated, it is nilpotent, and torsion-free in characteristic zero. Consequently $U(G)$ has finite rank (see below), and some headway could be made computationally using P. Hall's methods for infinite nilpotent groups (cf. [66, pp. 30–33]).

4.6. **Finite rank linear groups.** This subsection illustrates how rank restrictions facilitate computing with finitely generated solvable-by-finite linear groups.

Recall that a group H has *finite Prüfer rank* $\mathrm{rk}(H)$ if each finitely generated subgroup can be generated by $\mathrm{rk}(H)$ elements, and $\mathrm{rk}(H)$ is the least such integer. Finite rank linear groups are solvable-by-finite (Theorem 4.3). The converse is false.

Example 4.11. The subgroup $\left\langle \mathrm{diag}(1, \mathrm{x}), \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ of $\mathrm{GL}(2, \mathbb{F}_2(\mathrm{x}))$ is solvable, but does not have finite Prüfer rank, as it contains $\begin{pmatrix} 1 & \mathrm{x}^k \\ 0 & 1 \end{pmatrix}$ for all $k \geq 1$.

Proposition 4.12 ([44, Corollary 2.5])**.** *A finitely generated subgroup of* $\mathrm{GL}(n, \mathbb{F})$ *has finite Prüfer rank if and only if it is solvable-by-finite and* $\mathbb{Q}$*-linear, i.e., isomorphic to a subgroup of* $\mathrm{GL}(m, \mathbb{Q})$ *for some* m*.*

Example 4.13. Polycyclic-by-finite groups are $\mathbb{Z}$-linear, so have finite Prüfer rank.

A group H has *finite torsion-free rank* if there is a subnormal series of finite length in H, with each factor either periodic or infinite cyclic. The number $\mathrm{h}(H)$ of infinite cyclic factors is the *torsion-free rank* or *Hirsch number* of H.

Proposition 4.14 ([44, Proposition 2.6])**.** *For a finitely generated subgroup* G *of* $\mathrm{GL}(n, \mathbb{Q})$ *the following are equivalent.*

(i) G *is solvable-by-finite.*
(ii) G *has finite Prüfer rank.*
(iii) G *has finite torsion-free rank.*

Proposition 4.15 (Cf. [44, Sections 3.2 and 4.3])**.** *Each finitely generated solvable-by-finite subgroup* G *of* $\mathrm{GL}(n, \mathbb{Q})$ *has a finitely generated subgroup* $H \leq U(G)$ *such that* $U(G) = H^G$ *and* $\mathrm{h}(H) = \mathrm{h}(U(G)) = \mathrm{rk}(U(G))$.

In Proposition 4.15, $U(G)$ is the *isolator* of H in $U(G)$: for each $g \in U(G)$ there is a positive integer m such that $g^m \in H$ (see [66, Section 2.1]).

Let $\mathbb{P}$ be a number field. To test whether $G = \langle S \rangle \leq \mathrm{GL}(n, \mathbb{P})$ has finite Prüfer rank, we just run `IsSolvableByFinite`. Suppose that G is solvable-by-finite. If G is completely reducible then it is abelian-by-finite, G_ϱ is (torsion-free) abelian, and $\mathrm{h}(G) = \mathrm{h}(G_\varrho)$. The rank of G_ϱ may be computed using algorithms to construct presentations of irreducible abelian subgroups of $\mathrm{GL}(n, \mathbb{P})$ [44, Subsections 4.1.1 and 4.5]. This gives a procedure `RankCR` that returns $\mathrm{h}(G)$ for input completely reducible G. We can find $\mathrm{h}(G)$ with similar ease when G is unipotent (see [44, Subsection 4.1.2]); call the associated procedure `RankU`. Then `RankRadical` computes $\mathrm{h}(U(G)) = \mathrm{rk}(U(G))$ as follows. First, a presentation of $\texttt{CRPart}(S)$ is employed to produce a set Y of normal generators for $U(G)$. Secondly, a generating set of H as in Proposition 4.15 is found by the method in [44, Section 4.3]; `RankU` is required and the computation initializes at Y. Then $\mathrm{h}(U(G)) = \mathrm{h}(H)$. Furthermore, since $\mathrm{h}(G) = \mathrm{h}(G/U(G)) + \mathrm{h}(U(G))$, and $G/U(G)$ is isomorphic to $\texttt{CRPart}(S)$, we obtain a procedure `HirschNumber` that accepts S and returns $\mathrm{h}(G)$.

The group $H \leq U(G)$ constructed in `RankRadical` deserves more scrutiny. It has a series $1 = H_k \lhd H_{k-1} \lhd \cdots \lhd H_0 = H$ with infinite cyclic factors H_{i-1}/H_i. Let $H_{i-1} = \langle u_i, H_i \rangle$. Then since $U(G)$ is the isolator of H, we may represent each $g \in U(G)$ uniquely as a k-tuple of canonical rational parameters $(\alpha_1, \ldots, \alpha_k)$

where $g = u_1^{\alpha_1} \cdots u_k^{\alpha_k}$; see [66, pp. 29–34]. Thus $\{u_1, \ldots, u_k\}$ serves as a 'basis' of $U(G)$.

The next theorem expands on a result by D. J. S. Robinson about finitely generated solvable groups of finite abelian ranks.

Theorem 4.16 ([44, Theorem 3.1])**.** *Let $H \leq G \leq \mathrm{GL}(n, \mathbb{F})$ where G is finitely generated and of finite Prüfer rank. Then $|G : H| < \infty$ if and only if $\mathrm{h}(H) = \mathrm{h}(G)$.*

Theorem 4.16 yields the procedure `IsOfFiniteIndex`. This accepts generating sets S_1, S_2 for solvable-by-finite subgroups G, H of $\mathrm{GL}(n, \mathbb{P})$, respectively, such that $H \leq G$; and returns `true` if and only if $\texttt{HirschNumber}(S_1) = \texttt{HirschNumber}(S_2)$.

The final decision problem that we discuss here has ties to Section 3 and the next section.

A subgroup of $\mathrm{GL}(n, \mathbb{Q})$ is *integral* if it can be conjugated into $\mathrm{GL}(n, \mathbb{Z})$. Finite subgroups of $\mathrm{GL}(n, \mathbb{Q})$ are integral [102, p. 46]. The following integrality criterion is used in one of the finiteness testing algorithms from [9] (valid for input over a quotient field $\mathbb{F}$ of a principal ideal domain).

Proposition 4.17. *Suppose that each element of $G \leq \mathrm{GL}(n, \mathbb{Q})$ has trace in $\mathbb{Z}$. Then G is integral if and only if either G is finitely generated or the enveloping algebra $\langle G \rangle_{\mathbb{Q}}$ is semisimple.*

Integrality testing may be easier when the input is solvable-by-finite.

Lemma 4.18 ([36, Lemma 4.1])**.** *Let $G \leq \mathrm{GL}(n, \mathbb{Q})$ be finitely generated solvable-by-finite, and let p be an odd prime such that φ_p is a W-homomorphism on G. Then G, $\pi(G)$, and $\pi(G_p)$ are all integral if any one of these groups is integral.*

Lemma 4.18 gives us the following procedure from [36, Section 4], applied there in arithmeticity testing (see Subsection 5.3).

`IsIntegralSF`(S)

Input: a finite subset S of $\mathrm{GL}(n, \mathbb{Q})$ such that $G = \langle S \rangle$ is solvable-by-finite.
Output: `true` if G is integral; `false` otherwise.

(1) $N := \texttt{NormalGenerators}(S, \varphi_p)$, φ_p a W-homomorphism.
(2) Return `true` if each $g \in N$ is integral (the characteristic polynomial of g has integer coefficients and $\det(g) = \pm 1$); else return `false`.

Remark 4.19. For finite G we have $N = 1$, and `IsIntegralSF` returns `true` as expected.

4.7. **Implementation.** All algorithms from Sections 3 and 4 have been implemented in MAGMA by Eamonn O'Brien and the authors. Sample experiments are given in the documentation for [41].

5. Computing with Zariski dense and arithmetic groups

5.1. **Linear groups with a non-abelian free subgroup.** Until now we have been concerned almost exclusively with virtually solvable linear groups. Since they are built up from infinite abelian and finite blocks of restricted structure, intuition might suggest that these groups are rare. Indeed, for various $\mathbb{F}$, it is unlikely that a randomly selected finite subset of $\mathrm{GL}(n,\mathbb{F})$ generates a solvable-by-finite group [1, 65, 91].

Linear groups that are not virtually solvable pose computational challenges of a different nature to those posed by virtually solvable groups. For example, although membership testing in a finitely generated solvable-by-finite subgroup of $\mathrm{GL}(n,\mathbb{Q})$ is decidable [64], there exist subgroups of $\mathrm{GL}(4,\mathbb{Z})$ in which membership testing is undecidable [78]. Hence this and related algorithmic problems in $\mathrm{GL}(n,\mathbb{Z})$ for $n \geq 4$ (e.g., subgroup conjugacy testing) are undecidable; see [79, Section 5] and [32, Section 3]. In Subsection 6.2, we note some other problems in the class of non-solvable-by-finite linear groups where decidability is unknown.

5.2. **Zariski density and arithmetic groups.** To make computation with non-solvable-by-finite linear groups feasible, we impose some natural conditions on the input (which need not generate a non-solvable-by-finite group).

First we give some definitions. A subset S of an m-dimensional $\mathbb{F}$-space V is *algebraic* if there exists nonempty $F \subseteq \mathbb{F}[\mathrm{x}_1,\ldots,\mathrm{x}_m]$ such that S is the set of zeros of all polynomials in F. The Zariski topology on V is the topology whose closed sets are the algebraic subsets. An *algebraic group* is a subgroup of $\mathrm{GL}(n,\mathbb{F})$ that is closed in the n^2-dimensional space $V = \mathrm{Mat}(n,\mathbb{F})$. The essential case for us is algebraic $\mathbb{Q}$-groups $\mathcal{G} \leq \mathrm{GL}(n,\mathbb{C})$, i.e., $\mathcal{G}$ is the set of mutual zeros of a collection of polynomials over $\mathbb{Q}$.

When $n = 2s$ is even, the symplectic group $\mathrm{Sp}(n,R)$ is defined to be

$$\{h \in \mathrm{GL}(n,R) \mid hJh^{\top} = J\} \quad \text{where} \quad J = \begin{pmatrix} 0_s & 1_s \\ -1_s & 0_s \end{pmatrix}.$$

Each of $\mathrm{GL}(n,\mathbb{C})$, $\mathrm{SL}(n,\mathbb{C})$, and $\mathrm{Sp}(n,\mathbb{C})$ is an algebraic $\mathbb{Q}$-group.

Any linear group $G \leq \mathrm{GL}(n,\mathbb{F})$ is a subgroup of some linear algebraic group; say $\mathrm{GL}(n,\mathbb{F})$ itself. The 'smallest' algebraic group in $\mathrm{GL}(n,\mathbb{F})$ containing G is its *Zariski closure* $\overline{G}$. An algorithm to compute $\overline{G}$ for finitely generated G and infinite $\mathbb{F}$ is given in [30]. We assume that G is a Zariski dense subgroup of an algebraic group $\mathcal{G}$, i.e., $\mathcal{G} = \overline{G}$. If we wish to compute with non-solvable-by-finite G then we may also assume that $\mathcal{G}$ is non-solvable.

Now we introduce an important class of dense subgroups. If $G \leq \mathrm{GL}(n,\mathbb{C})$ and R is a subring of $\mathbb{C}$ then $G_R := G \cap \mathrm{GL}(n,R)$. Let $\mathcal{G}$ be an algebraic $\mathbb{Q}$-group. We say that $H \leq \mathcal{G}_{\mathbb{Q}}$ is an *arithmetic subgroup of* $\mathcal{G}$ (or merely *arithmetic* when $\mathcal{G}$ is understood) if H is commensurable with $\mathcal{G}_{\mathbb{Z}}$, meaning that $|H : H_{\mathbb{Z}}|$ and $|\mathcal{G}_{\mathbb{Z}} : H_{\mathbb{Z}}|$ are finite. In particular, finite index subgroups of $\mathcal{G}_{\mathbb{Z}}$ are arithmetic. If

$\mathcal{G}$ is semisimple then an arithmetic subgroup $H \leq \mathcal{G}$ is not solvable-by-finite, and we call H a *semisimple arithmetic group* [72, p. 91].

By a famous result of Borel and Harish-Chandra [110, p. 134], arithmetic subgroups of algebraic $\mathbb{Q}$-groups are finitely presentable. We remark that the notion of arithmetic group may be framed in algebraic groups $\mathcal{G}$ over fields $\mathbb{F}$ other than $\mathbb{Q}$. If $\mathrm{char}\,\mathbb{F} \neq 0$ then an arithmetic subgroup need not be finitely presentable, nor even finitely generated; examples are $\mathrm{SL}(n, \mathbb{F}_q[\mathrm{x}])$ for $n = 3$, 2 respectively (see [109, p. 2981] and [110, p. 134]).

Arithmetic subgroups in $\mathcal{G}_\mathbb{Z}$ are Zariski dense. A subgroup of $\mathcal{G}_\mathbb{Z}$ that is dense but not arithmetic is a *thin matrix group* [96]. These are ubiquitous in $\mathrm{SL}(n, \mathbb{Z})$ [53, 91].

See [105, Chapters 5 and 14], [110, Chapter 1, Sections 5 and 6] for more on algebraic groups, and [60] for more on arithmetic groups.

5.3. **Decidability for arithmetic groups.** Let $\mathcal{G}$ be an algebraic $\mathbb{Q}$-group. An arithmetic group $H \leq \mathcal{G}_\mathbb{Z}$ is *explicitly given* if membership in H of each $g \in \mathcal{G}_\mathbb{Z}$ can be tested, and an upper bound on $|\mathcal{G}_\mathbb{Z} : H|$ is known. Grunewald and Segal [55, 56, 57] justified decidability of problems for explicitly given arithmetic groups. One of these is constructing a (finite) generating set of an arithmetic subgroup of $\mathcal{G}_\mathbb{Z}$. Note that the algorithm in [55] to construct a generating set from input polynomials is not always practical. Also, sometimes we will have a generating set of $\mathcal{G}_\mathbb{Z}$ *a priori*; e.g., if $\mathcal{G}_\mathbb{Z} = \mathrm{SL}(n, \mathbb{Z})$ or $\mathrm{Sp}(n, \mathbb{Z})$.

Algorithms to construct a generating set of $\mathcal{G}_\mathbb{Z}$ for unipotent or abelian $\mathcal{G}$ are given in [28, 51]. These are ingredients in the procedure `GeneratingArithmetic` from [36], which constructs a generating set of a finite index subgroup of $\mathcal{G}_\mathbb{Z}$ for a solvable algebraic $\mathbb{Q}$-group $\mathcal{G}$. Motivation for `GeneratingArithmetic` is supplied by

> (AT) *Arithmeticity testing*: if H is a finitely generated subgroup of $\mathcal{G}_\mathbb{Z}$, determine whether $|\mathcal{G}_\mathbb{Z} : H|$ is finite.

It is unknown whether (AT) is decidable for all $\mathcal{G}$. However, since $\mathcal{G}_\mathbb{Z}$ is finitely presentable, if $|\mathcal{G}_\mathbb{Z} : H|$ is finite then this can be detected by Todd–Coxeter coset enumeration (not an advisable option in practice; Todd–Coxeter may not terminate even for very small input). Thus (AT) is semidecidable as per [58, p. 149].

When $\mathcal{G}$ is solvable, arithmetic groups are polycyclic, and it was proved in [36] that (AT) is decidable.

Proposition 5.1. *Let $\mathcal{G}$ be a solvable algebraic $\mathbb{Q}$-group. A finitely generated subgroup H of $\mathcal{G}$ is arithmetic if and only if H is integral and $\mathrm{h}(H) = \mathrm{h}(\mathcal{G}_\mathbb{Z})$.*

Therefore $H \leq \mathcal{G}_\mathbb{Z}$ is arithmetic if and only if H and $\mathcal{G}_\mathbb{Z}$ have the same Hirsch number (cf. Theorem 4.16). Proposition 5.1 gives

`IsArithmeticSolvable`$(S, \mathcal{G})$

Input: a finite subset S of $\mathcal{G}_{\mathbb{Q}}$, $\mathcal{G}$ a solvable algebraic $\mathbb{Q}$-group.
Output: `true` if $H = \langle S \rangle$ is arithmetic; `false` otherwise.

(1) If $\texttt{IsIntegralSF}(S) = \texttt{false}$ then return `false`.
(2) $T := \texttt{GeneratingArithmetic}(\mathcal{G})$.
(3) If $\texttt{HirschNumber}(S) \neq \texttt{HirschNumber}(T)$ then return `false`;
else return `true`.

To test arithmeticity when $\mathcal{G}$ is unipotent we only need to compare $\texttt{HirschNumber}(S)$ and $\texttt{HirschNumber}(T)$, i.e., the first step could be omitted.

5.4. **The congruence subgroup property.** The class of arithmetic subgroups of algebraic $\mathbb{Q}$-groups—even just the semisimple ones—is very wide. A comparison of $\mathrm{SL}(n, \mathbb{Q})$ and $\mathrm{SL}(n, \mathbb{Z})$ reveals how we should limit our scope. In $\mathrm{SL}(n, \mathbb{Q})$ a proper normal subgroup is scalar and has order at most 2, whereas $\mathrm{SL}(n, \mathbb{Z})$ has a plurality of normal subgroups, e.g., the (principal) congruence subgroups $\Gamma_{n,m} := \ker \varphi_m$ for all positive integers m (terminology and notation as in Subsection 2.2). The complete inverse image of the centre of $\mathrm{SL}(n, \mathbb{Z}/m\mathbb{Z})$ in $\mathrm{SL}(n, \mathbb{Z})$ under φ_m is an example of a normal subgroup that is not a congruence subgroup. The question of whether $\mathrm{SL}(n, \mathbb{Z})$ has normal subgroups of infinite index, or more generally normal subgroups not containing any PCS, was raised as long ago as the 19th century. Fricke and Klein constructed subgroups of finite index in $\mathrm{SL}(2, \mathbb{Z})$ that do not contain any PCS (see [88]). Also $\mathrm{SL}(2, \mathbb{Z})$ has normal subgroups of infinite index: e.g., the normal closure of $\left\langle \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \right\rangle$ for $m > 5$ (see [77, p. 33]). The story is very different for degrees greater than 2.

Theorem 5.2 (Cf. [11])**.** *For $n > 2$, each normal non-central subgroup of $\mathrm{SL}(n, \mathbb{Z})$ or $\mathrm{Sp}(n, \mathbb{Z})$ contains a PCS.*

Corollary 5.3. *Each finite index subgroup of $\mathrm{SL}(n, \mathbb{Z})$ or $\mathrm{Sp}(n, \mathbb{Z})$ for $n > 2$ contains a PCS.*

Corollary 5.3 says that $\mathrm{SL}(n, \mathbb{Z})$ or $\mathrm{Sp}(n, \mathbb{Z})$ both have the *congruence subgroup property* (CSP). How prevalent is the CSP? We have seen that it does not hold for $\mathrm{SL}(2, \mathbb{Z})$. But if $n > 2$ and $\mathbb{P}$ is a number field that is not totally imaginary, then a finite index subgroup of $\mathrm{SL}(n, \mathcal{O}_{\mathbb{P}})$ or $\mathrm{Sp}(n, \mathcal{O}_{\mathbb{P}})$ contains $\Gamma_{n,\varrho}$ for some maximal ideal ϱ of $\mathcal{O}_{\mathbb{P}}$ [11]. Determining whether arithmetic subgroups of an algebraic group have the CSP is 'the congruence subgroup problem' (see [88]).

Both $\mathcal{G}_{\mathbb{Z}} = \mathrm{SL}(n, \mathbb{Z})$ and $\mathcal{G}_{\mathbb{Z}} = \mathrm{Sp}(n, \mathbb{Z})$ have the CSP for $n > 2$. With the CSP in play, an arithmetic subgroup H can be handled using our congruence homomorphism methodology. Once the level of a PCS in H is known, most of the calculations are thereby transferred to finite quotients modulo some $\Gamma_{n,m}$. So we will be computing with groups over integer residue class rings $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ rather than finite fields.

5.5. **Structure of arithmetic subgroups.**

5.5.1. *Decidability and principal congruence subgroups.* Unless stated otherwise, henceforth $\mathcal{G} = \mathrm{SL}(n, \mathbb{C})$ or $\mathrm{Sp}(n, \mathbb{C})$ for $n > 2$. Since each arithmetic group in $\mathcal{G}_{\mathbb{Q}}$ is conjugate to a group over $\mathbb{Z}$, we confine ourselves to subgroups of $\mathcal{G}_{\mathbb{Z}}$ (see [37, Section 5] for a method to compute a conjugating matrix; this uses Proposition 4.17). As we know, if H has finite index in $\mathcal{G}_{\mathbb{Z}}$ then H contains some $\Gamma_{n,m}$. We write Γ_n for $\Gamma_{n,1} = \mathrm{SL}(n, \mathbb{Z})$ or $\mathrm{Sp}(n, \mathbb{Z})$.

Let R be a commutative unital ring. A *transvection* $t \in \mathrm{SL}(n, R)$ is a unipotent matrix such that $1_n - t$ has rank 1. Denote by $t_{ij}(m)$ the transvection $1_n + e_{ij}(m)$, where $e_{ij}(m)$ has m in position (i, j) and zeros elsewhere. Define

$$E_{n,m} = \langle t_{ij}(m) \,:\, i \neq j,\, 1 \leq i, j \leq n \rangle$$

if $\Gamma_n = \mathrm{SL}(n, R)$, and

$$\begin{aligned} E_{n,m} = \; & \{t_{i,s+j}(m)t_{j,s+i}(m), t_{s+i,j}(m)t_{s+j,i}(m) \mid 1 \leq i < j \leq s\} \\ & \cup \{t_{i,s+i}(m), t_{s+i,i}(m) \mid 1 \leq i \leq s\} \end{aligned}$$

if $\Gamma_n = \mathrm{Sp}(n, R)$ where $n = 2s$. The $E_{n,m}$ are *elementary subgroups of* Γ_n *of level* m. Note that $E_{n,1} = \Gamma_n$.

Each arithmetic subgroup in Γ_n contains a unique maximal PCS. We define the *level* $M(H)$ of an arithmetic group H to be the level of its maximal PCS. For $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$ and $n \geq 3$, the normal closure $E_{n,m}^{\Gamma_n}$ is $\Gamma_{n,m}$ [37, Proposition 1.6]. Similarly, $E_{n,m}^{\Gamma_n}$ is the PCS of level m in $\Gamma_n = \mathrm{Sp}(n, \mathbb{Z})$ if $n > 2$ [11, Proposition 13.2]. So at least we have normal generators for a PCS. When $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$, a full generating set of $\Gamma_{n,m}$ is returned by `GeneratorsPCS`(m), which encodes the formula in [103]. The size of this generating set depends only on n (i.e., not on m). Although a minimal generating set of an arithmetic subgroup can be arbitrarily large (see [103] again), each arithmetic subgroup in $\mathrm{SL}(n, \mathbb{Z})$ has a 2-generator finite index subgroup [76].

Just as we do not need a full generating set of a congruence subgroup to compute with a solvable-by-finite linear group, to compute with an arithmetic group $H \leq \Gamma_n$ we do not need a full generating set for its maximal PCS. All we need is the level of H. In the first instance, decidability is then implied by the CSP.

Proposition 5.4 ([39, Proposition 2.3])**.** *Computing the level of H is decidable.*

Corollary 5.5 ([39, Corollary 2.4])**.** *Testing membership of $g \in \Gamma_n$ in H and computing an upper bound on $|\Gamma_n : H|$ are decidable.*

By Corollary 5.5, arithmetic subgroups $H \leq \Gamma_n$ are explicitly given in the sense of [55]. Hence the algorithmic problems in [55] for such H are decidable.

5.5.2. *Computing with subgroups of* $\mathrm{GL}(n,\mathbb{Z}_m)$. At the moment, algorithms for matrix groups over finite rings are less sophisticated than those for groups over finite fields. Below we sketch the approach in [37, Section 2] and [39, Section 2] to computing in $\mathrm{GL}(n,\mathbb{Z}_m)$.

Let $m = p_1^{k_1}\cdots p_t^{k_t}$ where the p_i are distinct primes and $k_i \geq 1$. By the Chinese Remainder Theorem, $\chi : \mathbb{Z}_m \to \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{k_t}}$ defined 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 $a_i \equiv a \mod p_i^{k_i}$, is a ring isomorphism.

Lemma 5.6. *The map* χ *extends to an isomorphism*

$$\mathrm{Mat}(n,\mathbb{Z}_m) \to \oplus_{i=1}^t \mathrm{Mat}\big(n,\mathbb{Z}_{p_i^{k_i}}\big)$$

which restricts to an isomorphism

$$\mathrm{GL}(n,\mathbb{Z}_m) \to \Pi_{i=1}^t \mathrm{GL}\big(n,\mathbb{Z}_{p_i^{k_i}}\big).$$

Lemma 5.7. *For* $i \geq 1$, *let* $K = \{h \in \mathrm{GL}(n,\mathbb{Z}_{p^k}) \mid h \equiv 1_n \mod p^{k-1}\}$.

(i) K *is a* p*-group, the PCS of* $\mathrm{GL}(n,\mathbb{Z}_{p^k})$ *of level* p^{k-1}.
(ii) $\mathrm{GL}(n,\mathbb{Z}_{p^k})/K \cong \mathrm{GL}(n,p)$.

Our approach rests on Lemmas 5.6 and 5.7. First we reduce to $\mathrm{GL}(n,\mathbb{Z}_{p^k})$. The second part involves computing with finite p-groups and subgroups of $\mathrm{GL}(n,p)$, for which there is an extensive apparatus [58, Sections 7.8 and 9.4]. More finely-tuned techniques may be needed; see, e.g., [39, Section 2].

5.6. **Density and computing in arithmetic subgroups.**

5.6.1. *Strong approximation.* To compute with arithmetic and dense groups we replace finite approximation by *strong approximation*.

The previous algorithms for solvable-by-finite groups took one congruence homomorphism at a time. Now we must work with congruence images modulo all maximal ideals of $\mathbb{Z}$, i.e., modulo all primes $p \in \mathbb{Z}$. This is an option if we have surjection of $H \leq \mathcal{G}_\mathbb{Z}$ onto $\varphi_p(\mathcal{G}_\mathbb{Z})$ for all but finitely many primes p; which of course may not happen with an arbitrary finitely generated subgroup of $\mathcal{G}_\mathbb{Z}$ and arbitrary $\mathcal{G}$. For example, if $m \geq 5$ then reduction modulo m does not surject $\mathrm{GL}(n,\mathbb{Z})$ onto $\mathrm{GL}(n,\mathbb{Z}_m)$. On the other hand, $\mathrm{SL}(n,\mathbb{Z})$ surjects onto $\mathrm{SL}(n,\mathbb{Z}_m)$ when $m \geq 2$. Behind these simple observations lies a deep result, the *strong approximation theorem* (SAT) [72, Window 9]. It provides conditions under which $H \leq \mathcal{G}_\mathbb{Z}$ surjects onto $\varphi_p(\mathcal{G}_\mathbb{Z})$ for almost all p. A necessary condition for SAT is that H be Zariski dense in $\mathcal{G}$. This explains why $\mathrm{GL}(n,\mathbb{Z})$ does not surject onto $\mathrm{GL}(n,p)$ for almost all primes p: $\mathrm{GL}(n,\mathbb{Z})$ is not dense in $\mathrm{GL}(n,\mathbb{C})$ because its Zariski closure consists of $g \in \mathrm{GL}(n,\mathbb{C})$ such that $\det(g)^n = 1$ [89, p. 273]. Neither does density imply SAT; e.g., $\mathrm{GL}(2,\frac{1}{2}\mathbb{Z})$ is dense in $\mathrm{GL}(2,\mathbb{C})$, but does not surject onto $\mathrm{GL}(2,p)$ modulo any prime $p \equiv 1$ modulo 8 [89, p. 273]. However, dense subgroups of Γ_n satisfy SAT.

Theorem 5.8 ([72, Window 9])**.** *If $H \leq \Gamma_n$ is dense in $\mathcal{G}$ then $\varphi_p(H) = \varphi_p(\Gamma_n)$ for almost all primes p.*

Moreover, we have

Theorem 5.9 ([71] and [72, p. 396])**.** *$H \leq \Gamma_n$ is dense if and only if $\varphi_p(H) = \varphi_p(\Gamma_n)$ for some prime $p > 3$.*

Let $\Pi(H)$ be the set of primes p such that $\varphi_p(H) \neq \mathrm{SL}(n,p)$. By Theorem 5.8, $\Pi(H)$ is finite when H is dense.

Suppose that $H \leq \Gamma_n$ is arithmetic of level M. Then $\varphi_p(H) = \varphi_p(\Gamma_n)$ for any prime p coprime to M ($\varphi_p(\Gamma_n)$ is generated by transvections, and H contains the elementary group $E_{n,M}$). Remarkably, the converse (with a tiny number of exceptions) is true as well.

Theorem 5.10 ([39, Section 2])**.** *Let $H \leq \Gamma_n$ be arithmetic of level M. Then $\varphi_p(H) = \varphi_p(\Gamma_n)$ if and only if $p \nmid M$; unless $n = 3$ or 4, $\Gamma_n = \mathrm{SL}(n,\mathbb{Z})$, $\varphi_2(H) = \varphi_2(\Gamma_n)$, and $\varphi_4(H) \neq \varphi_4(\Gamma_n)$. In the latter event, M is even.*

Theorem 5.10 pinpoints the set of prime divisors of the level of arithmetic $H \leq \Gamma_n$: barring the exceptions in Theorem 5.10, it is exactly $\Pi(H)$. This set is input for our algorithm to compute M; see Subsection 5.7.1 and [39, Section 2.4].

We can compute with dense rather than merely arithmetic groups in Γ_n. Each dense subgroup H has a unique minimal arithmetic overgroup $\mathrm{cl}(H)$the intersection of all arithmetic groups in Γ_n that contain H. The *level* of H is then defined to be the level of $\mathrm{cl}(H)$. We implemented an algorithm to compute this 'arithmetic closure' $\mathrm{cl}(H)$ [39, Section 3.3]; see Subsection 5.7. Hence, we can investigate H by applying algorithms for arithmetic groups to $\mathrm{cl}(H)$. Perhaps $\mathrm{cl}(H) = \Gamma_n$. This does happen: see [61] for examples of free subgroups H of $\mathrm{SL}(n,\mathbb{Z})$, $n > 2$, generated by n transvections, that surject onto $\mathrm{SL}(n,p)$ modulo all primes p. Since $\mathrm{SL}(n,\mathbb{Z})$ is virtually free only for $n = 2$, H has infinite index in $\mathrm{SL}(n,\mathbb{Z})$, i.e., is thin. Note that, for $n \geq 5$, the only arithmetic subgroup in Γ_n that surjects onto $\varphi_p(\Gamma_n)$ for all primes p is Γ_n itself [39, Corollary 2.14].

5.6.2. *Density testing and SAT.* While decidability of arithmeticity testing is unknown, we can test density, and this serves as an initial check along the way to settling arithmeticity of individual examples.

A Monte Carlo algorithm to test density is given in [90]. It uses

Theorem 5.11. *Suppose that $H \leq \Gamma_n$ contains non-commuting elements g_1, g_2 such that the Galois group of the characteristic polynomial of g_1 is $\mathrm{Sym}(n)$, and g_2 has infinite order. Then either H is dense, or $\mathcal{G} = \mathrm{Sp}(n,\mathbb{C})$ and the closure of H over $\mathbb{C}$ is the product of $n/2$ copies of $\mathrm{SL}(2,\mathbb{C})$.*

There are intrinsic GAP procedures to compute Galois groups and test equality with $\mathrm{Sym}(n)$. And finiteness can be tested over any field (Section 3). Elements of

Γ_n with associated Galois group equal to the symmetric group are *generic*: a 'random' element of Γ_n is likely to satisfy the criteria [90, Theorem 1.4]. Algorithm 1 of [90] is Monte Carlo, and may incorrectly report that input is not dense; but the probability of error is small due to the abundance of elements g_1 and g_2.

Another density testing algorithm in [90] accepts a finitely generated subgroup H of semisimple $\mathcal{G}$ in characteristic zero. It uses the fact that H is dense if and only if (i) H is infinite, and (ii) the adjoint representation $\mathrm{ad}(H)$ on the Lie algebra of $\mathcal{G}$ is absolutely irreducible. If $\mathcal{G} = \mathrm{SL}(n, \mathbb{C})$ then the Lie algebra consists of all matrices with zero trace, so has dimension $n^2 - 1$. If $\mathcal{G} = \mathrm{Sp}(n, \mathbb{C})$ then the algebra has dimension $(n^2 + n)/2$, and consists of all matrices of the form $\left(\begin{smallmatrix} A & B \\ C & A^\top \end{smallmatrix}\right)$ where B and C are symmetric. We construct $\mathrm{ad}(H)$ from a finite generating set for H. Checking absolute irreducibility is routine; cf. [43, p. 404]. So we have deterministic density testing, too [39, Section 5].

We get a one-way density test from Theorem 5.9, i.e., if $\varphi_p(H) = \varphi_p(\Gamma_n)$ for some prime $p > 3$ then H is dense. This raises the problem of realizing SAT computationally: for dense H, compute the set $\Pi(H)$. The problem is addressed in [39, Section 3.2] and in [40]. We label the procedures from [39, 40] for computing $\Pi(H)$ as $\texttt{PrimesForDense}(H)$.

5.7. **Algorithms for computing with dense and arithmetic groups.** In this subsection we outline procedures for dense (including arithmetic) groups in Γ_n, $n > 2$.

5.7.1. *Computing the level and related procedures.* We tailor congruence homomorphism methods to properties of arithmetic or dense groups (CSP, SAT). The core part is computing the level.

`LevelMaxPCS` accepts a finite set $S \subseteq \Gamma_n$ that generates a dense group H, and returns the level of H. To give a flavor of the computation, we quote a technical result ('stabilization lemma') from [39]. For $n > 2$ and $H \leq \Gamma_n$, set

$$\delta_H(m) = |\Gamma_n : \Gamma_{n,m} H|; \tag{*}$$

i.e., $\delta_H(m) = |\varphi_m(\Gamma_n) : \varphi_m(H)|$.

Lemma 5.12 ([39, Lemma 2.16])**.**

(i) *Suppose that $\delta_H(kp^a) = \delta_H(kp^{a+1})$ for some prime p, positive integer a, and k coprime to p. Then $\delta_H(kp^b) = \delta_H(kp^a)$ for all $b \geq a$.*

(ii) *Let p, a, and k be as in* (i)*. Then $\delta_H(lp^b) = \delta_H(lp^a)$ for all $b \geq a$ and any multiple l of k such that $\pi(l) = \pi(k)$.*

`LevelMaxPCS` is recursive, and embodies theory of dense groups as in Subsection 5.6.1. Its input includes $\texttt{PrimesForDense}(H)$. This gives the primes dividing the level of H (with some exceptions as in Theorem 5.10, which cause no difficulty in the computation). The highest power of each prime p in the prime factorization of the level is determined. Since by $(*)$ all δ-values encountered in its recursion loop are bounded, the procedure terminates.

`LevelMaxPCS` solves the following problems. We can compute $|\Gamma_n : H|$ if H is arithmetic (cf. Lemma 5.12). Membership testing is easy: $g \in \Gamma_n$ is in H if and only if $\varphi_M(g) \in \varphi_M(H)$, where $M = \texttt{LevelMaxPCS}(S)$. This extends to $\texttt{IsSubgroup}(H, L)$, which tests whether $L \leq \Gamma_n$ is contained in H. When H is arithmetic, `LevelMaxPCS` returns 1 if and only if $H = \Gamma_n$.

5.7.2. *Subnormality.* The contrast between linear groups over rings and groups over fields is stark when we look at their subnormal subgroups. We touched on this point in Subsection 5.4 and elaborate on it now.

In this subsection, $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$. Statements can be duly modified for $\Gamma_n = \mathrm{Sp}(n, \mathbb{Z})$. As in [107, p. 166], for $h = (h_{ij}) \in \Gamma_n$ we denote by $\ell(h)$ the ideal of $\mathbb{Z}$ generated by

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

i.e., the lcm of the non-diagonal entries of h and differences of the diagonal entries. Then $\ell(A) := \sum_{a \in A} \ell(a)$ for $A \subseteq \Gamma_n$. Let $Z_{n,m}$ denote the full preimage of the center (scalar subgroup) of $\mathrm{GL}(n, \mathbb{Z}_m)$ in Γ_n under φ_m. So $\ell(A)$ is the smallest ideal $m\mathbb{Z}$ such that $A \subseteq Z_{n,m}$. We define $\ell(A)$ unambiguously as the non-negative integer modulo m that generates $\ell(A)$; e.g., $\ell(Z_{n,k}) = \ell(\Gamma_{n,k}) = k$.

If $H = \langle S \rangle \leq \mathrm{GL}(n, \mathbb{Z})$ then $\ell(H) = \ell(S)$ [37, Lemma 1.22]. This gives a procedure $\texttt{El}(S)$ that returns $\ell(H)$ for $H = \langle S \rangle$.

We need the following 'sandwich theorem'.

Theorem 5.13 ([107])**.** *$H \leq \mathrm{GL}(n, \mathbb{Z})$ is subnormal if and only if $\Gamma_{n,k^e} \leq H \leq Z_{n,k}$ for some k, e. If $|\mathrm{GL}(n, \mathbb{Z}) : H| < \infty$ then $\Gamma_{n,M}$ is the maximal PCS of H, in which case H is subnormal in $\mathrm{GL}(n, \mathbb{Z})$ if and only if M divides $\ell(H)^t$ for some t.*

Corollary 5.14 ([37, Corollary 1.28])**.** *$H \trianglelefteq \mathrm{GL}(n, \mathbb{Z})$ is subnormal if and only if $\ell(H)$ is the level of H.*

So the normal closure of an arbitrary subgroup H of $\mathrm{GL}(n, \mathbb{Z})$ is $\langle H, \Gamma_{n,\ell(H)} \rangle$. The procedure `NormalClosure` accepts (finite) S for $H = \langle S \rangle$, computes $\ell = \texttt{El}(S)$, and returns the union of S and $\texttt{GeneratorsPCS}(\ell)$.

For arithmetic H, `IsSubnormal` returns `true` if there is non-negative $e \in \mathbb{Z}$ such that $M = \texttt{LevelMaxPCS}(S)$ divides $\texttt{El}(S)^e$. If $\texttt{El}(S) = 1$, i.e., $M = \texttt{El}(S)$, then the procedure $\texttt{IsNormal}(S)$ tests whether H is normal in $\mathrm{GL}(n, \mathbb{Z})$. We compute the normalizer $N_{\Gamma_n}(H)$ of arithmetic $H \leq \Gamma_n$ as the full preimage of the normalizer of a congruence image.

5.7.3. *The orbit-stabilizer problem.* Let $G \leq \mathrm{GL}(n, \mathbb{F})$, and $u, v \in \mathbb{F}^n$. The *orbit-stabilizer problem* is:

(OP) Decide whether there is $g \in G$ such that $gu = v$; if so, find g.

(SP) Compute a generating set of $\mathrm{Stab}_G(u) = \{g \in G \mid gu = u\}$.

The orbit problem (OP) is related to two other fundamental algorithmic questions, membership and conjugacy testing (see [48, 3., p. 239]). Since the conjugacy problem can be undecidable in $\mathrm{SL}(4,\mathbb{Z})$, (OP) can be undecidable. And we only attempt to solve the stabilizer problem (SP) knowing beforehand that $\mathrm{Stab}_G(u)$ is finitely generated (see [48, 6., p. 239] for a simple example where it is not).

The above difficulties steer us toward arithmetic groups H in $\Gamma_n = \mathrm{SL}(n,\mathbb{Z})$. The orbit-stabilizer problem is decidable for any explicitly given arithmetic subgroup of $\mathcal{G}$ [55]; this implies that it is decidable for H. A practical algorithm is proposed in [37, Section 4]. We first solve the orbit-stabilizer problem for subgroups of $\mathrm{GL}(n,\mathbb{Z}_m)$ acting on $\mathbb{Z}_m^n$, then solve it for $\Gamma_{n,m}$ acting on $\mathbb{Z}^n$, and patch together the two solutions. The second stage of the method uses the next theorem (see [37, Proposition 4.10 and Theorem 4.13]).

Theorem 5.15. *Non-zero elements $u = (u_1,\dots,u_n)^\top$ and $v = (v_1,\dots,v_n)^\top$ of $\mathbb{Z}^n$ are in the same $\Gamma_{n,m}$-orbit if and only if*

- *the u_i generate the same ideal $a\mathbb{Z}$ of $\mathbb{Z}$ as the v_i, and*
- *$u_i \equiv v_i \bmod am$ for $1 \le i \le n$.*

In particular, if $m = 1$ then u, v are in the same Γ_n-orbit if and only if the u_i generate the same ideal as the v_i.

A similar result is true over $\mathbb{Z}_m$, for use in the first stage.

Proposition 5.16 ([37, Proposition 4.7])**.** *Non-zero elements $u = (u_1,\dots,u_n)^\top$ and $v = (v_1,\dots,v_n)^\top$ of $\mathbb{Z}_m^n$ are in the same $\mathrm{SL}(n,\mathbb{Z}_m)$-orbit if and only if the u_i generate the same ideal of $\mathbb{Z}_m$ as the v_i.*

So we obtain a procedure `Orbit`(S,u) that returns a solution of (OP) for $H = \langle S\rangle \le \mathrm{SL}(n,\mathbb{Z})$ and $u \in \mathbb{Z}^n$, $n > 2$.

By [55, p. 744], $\mathrm{Stab}_{\Gamma_n}(u)$ is finitely generated: it is conjugate to the affine group of matrices of the form

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

Let $\sigma =$ `Orbit`(Γ_n, u). Remember that we know a generating set of Γ_n. Then $\mathrm{Stab}_{\Gamma_n}(u)$ is generated by the σ-conjugates of $t_{12}(1),\dots,t_{1n}(1)$ and $\mathrm{diag}(1,x)$ as x runs over a generating set of Γ_{n-1}. Similarly, $\mathrm{Stab}_{\Gamma_{n,m}}(u)$ is generated by the σ-conjugates of $t_{12}(m),\dots,t_{1n}(m),\mathrm{diag}(1,x)$ as x runs over a generating set of $\Gamma_{n-1,m}$ (as in [103]). This completes solution of (SP) for $G \le \mathrm{SL}(n,\mathbb{Z}_m)$ acting on $\mathbb{Z}_m^n$, hence solving the orbit-stabilizer problem for finitely generated subgroups of finite index in Γ_n.

5.8. **Experiments.** The algorithms from this section are joint work with Alexander Hulpke, and have been implemented in GAP. Below is a small sample of experiments conducted with the software (see [38]).

One set of test groups come from low-dimensional topology. These were evidence supporting the conjecture of Lubotzky on 2-generator arithmetic subgroups, verified in [76] (see Subsection 5.5.1). Let

$$\mathcal{C} = \langle x, y, z \mid zxz^{-1} = xy,\ zyz^{-1} = yxy \rangle,$$

the fundamental group of the figure-eight knot complement. A representation $\beta_T : \mathcal{C} \to \mathrm{SL}(3, \mathbb{Z})$ for $T \in \mathbb{Z} \setminus \{0\}$ is given in [68], where $H_T = \langle \beta_T(x), \beta_T(y) \rangle$ is shown to be arithmetic. Finding $|\mathrm{SL}(3, \mathbb{Z}) : H_T|$ was an open problem in [68]. We can compute the level and the index using `PrimesForDense` and `LevelMaxPCS`; see [37, Section 6] and [39, Section 4]. For example, it took 892.6 seconds to find the level $2^7 5^6 29 \cdot 67 \cdot 193$ and index $2^{42} 3^5 5^{25} 7^4 13 \cdot 31^2 67 \cdot 1783$ for $T = 100$.

Another batch of test groups comes from an intermingling of group theory, differential equations, and theoretical physics. Let $G(d, k) = \langle U, T \rangle$ where

$$U = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ d & d & 1 & 0 \\ 0 & -k & -1 & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

There are 14 pairs (d, k) such that $G(d, k) \leq \mathrm{Sp}(4, \mathbb{Z})$ is the monodromy group of a hypergeometric ordinary differential equation associated to Calabi-Yau threefolds. Of those, seven are arithmetic and the rest are thin [100]. We can study $G(d, k)$ by first locating an arithmetic group in $\mathrm{Sp}(4, \mathbb{Z})$ containing $G(d, k)$; see [21]. Our procedures complete all computations quickly, and find the minimal arithmetic overgroup of $G(d, k)$ (some of these for the first time) [39, Section 4.2].

6. Where to next?

We have used our methodology for computing with finitely generated linear groups to solve a variety of algorithmic problems. Other problems await a similarly satisfactory treatment.

6.1. **Solvable-by-finite groups.** One of the foremost open computational problems for solvable-by-finite groups $G \leq \mathrm{GL}(n, \mathbb{F})$ is subgroup membership testing. This problem is decidable for $\mathbb{F} = \mathbb{Q}$ [64], so it is decidable for finitely generated linear groups of finite rank (Proposition 4.12). However, as yet we do not have a practical algorithm. One hurdle to overcome is that the unipotent radical $U(G)$ may not be finitely generated. However, $U(G)$ has finite rank (and is polyrational), so we could attempt to design an algorithm using methods from Subsections 4.5 and 4.6. This would amount to a computational realization of Hall's theory of infinite nilpotent groups, including calculation of Hall polynomials. With an eye on practicality, we note another technique: replace computing in the torsion-free nilpotent group $U(G)$ by computing in related Lie algebras (see, e.g., [3]).

Partial classes of solvable-by-finite linear groups offer fresh opportunities. Constructing (faithful) linear representations of polycyclic-by-finite groups falls under

this heading. An algorithm to solve this problem for finitely generated torsion-free nilpotent groups is given in [84]. More ambitiously, we would seek an algorithm to construct a representation over $\mathbb{Q}$ of a finitely generated finite rank subgroup of $\mathrm{GL}(n, \mathbb{F})$.

6.2. **Non-solvable-by-finite groups.** Let G be a finitely generated non-solvable-by-finite subgroup of $\mathrm{GL}(n, \mathbb{F})$. The procedure `IsSolvableByFinite` from Subsection 4.3 only attests to the existence of a free group in G, without constructing one. Taking advantage of the ubiquity of free subgroups in non-solvable-by-finite linear groups [1, 49], we could try picking a 'random' finitely generated subgroup and testing whether it is free (here 'random' has several interpretations [92]). This runs into the open problem of testing whether finitely generated linear groups are free. The difficulty of freeness testing is evinced by

$$H(x) := \left\langle \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \right\rangle \leq \mathrm{GL}(2, \mathbb{C}).$$

This group is free for $|x| \geq 2$, and for some x such that $|x| < 2$. However, often it is still not known whether $H(x)$ is free (see [16]).

Construction of 'large' free subgroups would be interesting. For a non-solvable-by-finite subgroup H of an algebraic group $\mathcal{G}$ (say $\mathcal{G} = \overline{H}$), 'large' means Zariski dense. If $n > 2$, $\mathcal{G} = \mathrm{Sp}(n, \mathbb{C})$ or $\mathrm{SL}(n, \mathbb{C})$, and $H = \mathcal{G}_{\mathbb{Z}}$, then such free subgroups are plentiful and provide examples of thin matrix groups. A related problem is construction of strongly dense subgroups of $\mathcal{G}$, i.e., free dense subgroups H in which each non-cyclic subgroup is again dense. See [20] for insights on the importance of strongly dense subgroups, their existence, and a link to the Banach–Tarski paradox.

The group $\mathrm{SL}(3, \mathbb{Z})$ is a source of exciting open problems. As usual, subgroup membership testing is crucial: it is not known whether this problem is decidable in $\mathrm{SL}(3, \mathbb{Z})$. We also mention (i) the Howson property: is the intersection of two finitely generated subgroups of $\mathrm{SL}(3, \mathbb{Z})$ finitely generated? (ii) coherence: is every finitely generated subgroup of $\mathrm{SL}(3, \mathbb{Z})$ finitely presentable? Computer experimentation may help to answer these questions; cf. [68] and [39, Section 4.1]. The questions have a negative answer in degrees greater than 3 and a positive answer in degree 2.

We pointed to arithmeticity testing as a significant open problem; cf. Section 5.3 and [96]. Constructing presentations of (finitely presentable) arithmetic groups can be hard; a practical algorithm even for finite index subgroups of $\mathrm{SL}(n, \mathbb{Z})$ is lacking. Recent progress is [23], which gives algorithms to compute a presentation of the unit group of an order in a semisimple $\mathbb{Q}$-algebra. The problem of computing linear representations of finitely generated abstract groups resurfaces (especially finitely presented groups that are not necessarily solvable-by-finite [87]). Here we note the achievements of [69, 70] in constructing faithful representations of triangle groups.

Acknowledgments. A. S. Detinko was supported by a Marie Skłodowska-Curie Individual Fellowship grant H2020 MSCA-IF-2015, No. 704910 (EU Framework Programme for Research and Innovation). D. L. Flannery was funded by the Irish Research Council (New Foundations 2015).

REFERENCES

1. R. Aoun, *Random subgroups of linear groups are free*, Duke Math. J. **160** (2011), no. 1, 117–173.
2. M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), no. 3, 469–514.
3. B. Assmann, *Algorithmic use of the Mal'cev correspondence*, Groups St Andrews 2005. Vol. 1, London Math. Soc. Lecture Note Ser. **339**, Cambridge Univ. Press, Cambridge, 2007, pp. 158–169.
4. B. Assmann and B. Eick, Polenta—Polycyclic presentations for matrix groups, `http://www.gap-system.org/Packages/polenta.html`
5. B. Assmann and B. Eick, *Computing polycyclic presentations for polycyclic rational matrix groups*, J. Symbolic Comput. **40** (2005), no. 6, 1269–1284.
6. B. Assmann and B. Eick, *Testing polycyclicity of finitely generated rational matrix groups*, Math. Comp. **76** (2007), 1669–1682.
7. H. Bäärnhielm, D. Holt, C. R. Leedham-Green, and E. A. O'Brien, *A practical model for computation with matrix groups*, J. Symbolic Comput. **68** (2015), 27–60.
8. L. Babai, *Deciding finiteness of matrix groups in Las Vegas polynomial time*, Proceedings of the Third Annual ACM-SIAM Symposium on Discrete Algorithms (Orlando, FL, 1992) (New York), ACM, 1992, pp. 33–40.
9. L. Babai, R. Beals, and D. N. Rockmore, *Deciding finiteness of matrix groups in deterministic polynomial time*, Proc. of International Symposium on Symbolic and Algebraic Computation ISSAC '93 (ACM Press), 1993, pp. 117–126.
10. L. Babai, R. Beals, and Á. Seress, *Polynomial-time theory of matrix groups*, STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing, ACM, New York, 2009, pp. 55–64.
11. H. Bass, J. Milnor, and J.-P. Serre, *Solution of the congruence subgroup problem for* SL_n $(n \geq 3)$ *and* Sp_{2n} $(n \geq 2)$, Inst. Hautes Études Sci. Publ. Math. (1967), no. 33, 59–137.
12. G. Baumslag, F. Cannonito, D. J. S. Robinson, and D. Segal, *The algorithmic theory of polycyclic-by-finite groups*, J. Algebra **142** (1991), no. 1, 118–149.
13. R. Beals, GRIM: Groups of Rational and Integer Matrices, `http://www.gap-system.org/Gap3/Packages3/grim.html`
14. R. Beals, *Algorithms for matrix groups and the Tits alternative*, J. Comput. System Sci. **58** (1999), no. 2, 260–279, 36th IEEE Symposium on the Foundations of Computer Science (Milwaukee, WI, 1995).
15. R. Beals, *Improved algorithms for the Tits alternative*, Groups and Computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 63–77.
16. A. F. Beardon, *Pell's equation and two generator free Möbius groups*, Bull. London Math. Soc. **25** (1993), 527–532.
17. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.
18. C. Brav and H. Thomas, *Thin monodromy in* $\mathrm{Sp}(4)$, Compos. Math. **150** (2014), no. 3, 333–343.
19. E. Breuillard, *A strong Tits alternative*, `https://arxiv.org/abs/0804.1395v1`

20. E. Breuillard, B. Green, R. Guralnick, and T. Tao, *Strongly dense free subgroups of semisimple algebraic groups*, Israel J. Math. **192** (2012), 347–379.
21. Y. Chen, Y. Yang, and N. Yui, *Monodromy of Calabi–Yau differential equations* (with an appendix by Cord Erdenberger), J. Reine Angew. Math. **616** (2008), 167–203.
22. A. M. Cohen, S. Haller, and S. H. Murray, *Computing in unipotent and reductive algebraic groups*, LMS J. Comput. Math. **11** (2008), 343–366 (electronic).
23. R. Coulangeon, G. Nebe, O. Braun, and S. Schönnenbeck, *Computing in arithmetic groups with Voronoi's algorithm*, J. Algebra **435** (2015), no. 1, 263–285.
24. W. A. de Graaf, `http://www.science.unitn.it/~degraaf/arith.html`
25. W. A. de Graaf, *Lie algebras: Theory and Algorithms*, North-Holland, Amsterdam, 2000.
26. W. A. de Graaf, *Constructing algebraic groups from their Lie algebras*, J. Symbolic Comput. **44** (2009), 1223–1233.
27. W. A. de Graaf, *Computation with Linear Algebraic Groups*, Chapman & Hall/CRC, Boca Raton, FL, 2017.
28. W. A. de Graaf and A. Pavan, *Constructing arithmetic subgroups of unipotent groups*, J. Algebra **322** (2009), 3950–3970.
29. K. Dekimpe and B. Eick, *AClib, Almost Crystallographic Groups - a library and algorithms*, `http://www.gapsystem.org/Packages/aclib.html`
30. H. Derksen, E. Jeandel, and P. Koiran, *Quantum automata and algebraic groups*, J. Symbolic Comput. **39** (2005), no. 3-4, 357–371.
31. A. S. Detinko, *On deciding finiteness for matrix groups over fields of positive characteristic*, LMS J. Comput. Math. **4** (2001), 64–72 (electronic).
32. A. S. Detinko, B. Eick, and D. L. Flannery, *Computing with matrix groups over infinite fields*, Groups St Andrews 2009 in Bath. Volume 1, London Math. Soc. Lecture Note Ser. **387**, Cambridge Univ. Press, Cambridge, 2011, pp. 256–270.
33. A. S. Detinko and D. L. Flannery, *Computing in nilpotent matrix groups*, LMS J. Comput. Math. **9** (2006), 104–134 (electronic).
34. A. S. Detinko and D. L. Flannery, *Algorithms for computing with nilpotent matrix groups over infinite domains*, J. Symbolic Comput. **43** (2008), no. 1, 8–26.
35. A. S. Detinko and D. L. Flannery, *On deciding finiteness of matrix groups*, J. Symbolic Comput. **44** (2009), no. 8, 1037–1043.
36. A. S. Detinko, D. L. Flannery, and W. A. de Graaf, *Integrality and arithmeticity of solvable linear groups*, J. Symbolic Comput. **68** (2015), 138–145.
37. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Algorithms for arithmetic groups with the congruence subgroup property*, J. Algebra **421** (2015), 234–259.
38. A. S. Detinko, D. L. Flannery, and A. Hulpke, *GAP functionality for Zariski dense groups*, Oberwolfach Preprints, OWP 2017-22.
39. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Zariski density and computing in arithmetic groups*, Math. Comp. **87** (2018), 967–986.
40. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Algorithms for experimenting with Zariski dense subgroups*, Exp. Math., in press.
41. A. S. Detinko, D. L. Flannery, and E. A. O'Brien, `http://magma.maths.usyd.edu.au/magma/handbook/matrix_groups_over_infinite_fields`
42. A. S. Detinko, D. L. Flannery, and E. A. O'Brien, *Deciding finiteness of matrix groups in positive characteristic*, J. Algebra **322** (2009), no. 11, 4151–4160.
43. A. S. Detinko, D. L. Flannery, and E. A. O'Brien, *Algorithms for the Tits alternative and related problems*, J. Algebra **344** (2011), 397–406.
44. A. S. Detinko, D. L. Flannery, and E. A. O'Brien, *Algorithms for linear groups of finite rank*, J. Algebra **393** (2013), 187–196.

45. A. S. Detinko, D. L. Flannery, and E. A. O'Brien, *Recognizing finite matrix groups over infinite fields*, J. Symbolic Comput. **50** (2013), 100–109.
46. J. D. Dixon, *The Tits alternative*, http://people.math.carleton.ca/~jdixon/Titsalt.pdf
47. J. D. Dixon, *The Structure of Linear Groups*, Van Nostrand Reinhold, London, 1971.
48. J. D. Dixon, *The orbit-stabilizer problem for linear groups*, Canad. J. Math. **37** (1985), no. 2, 238–259.
49. D. B. A. Epstein, *Almost all subgroups of a Lie group are free*, J. Algebra **19** (1971), 261–262.
50. T. Ericson and V. Zinoviev, *Codes on Euclidean Spheres*, North-Holland, Amsterdam, 2001.
51. P. Faccin, W. A. de Graaf, and W. Plesken, *Computing generators of the unit group of an integral abelian group ring*, J. Algebra **373** (2013), 441–452.
52. W. Feit, *The current situation in the theory of finite simple groups*. Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1, pp. 55–93. Gauthier-Villars, Paris, 1971.
53. E. Fuchs, *The ubiquity of thin groups*, Thin groups and superstrong approximation, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014, pp. 73–92.
54. The GAP Group, *GAP – Groups, Algorithms, and Programming*, http://www.gapsystem.org
55. F. Grunewald and D. Segal, *Some general algorithms. I. Arithmetic groups*, Ann. of Math. (2) **112** (1980), no. 3, 531–583.
56. F. Grunewald and D. Segal, *Some general algorithms. II. Nilpotent groups*, Ann. of Math. (2) **112** (1980), no. 3, 585–617.
57. F. Grunewald and D. Segal, *Decision problems concerning S-arithmetic groups*, J. Symbolic Logic **50** (1985), no. 3, 743–772.
58. D. F. Holt, B. Eick, and E. A. O'Brien, *Handbook of Computational Group Theory*, Chapman & Hall/CRC, Boca Raton, FL, 2005.
59. A. Hulpke, *Notes on Computational Group Theory*, http://www.math.colostate.edu/~hulpke/CGT/cgtnotes.pdf
60. J. E. Humphreys, *Arithmetic Groups*, Lecture Notes in Math., vol. 789, Springer, Berlin, 1980.
61. S. P. Humphries, *Free subgroups of* $\mathrm{SL}(n,\mathbb{Z})$*,* $n > 2$*, generated by transvections*, J. Algebra **116** (1988), 155–162.
62. G. Ivanyos, *Deciding finiteness for matrix semigroups over function fields over finite fields*, Israel J. Math. **124** (2001), 185–188.
63. C. Jordan, *Traité des substitutions et des équations algébriques*, Les Grands Classiques Gauthier-Villars. [Gauthier-Villars Great Classics], Éditions Jacques Gabay, Sceaux, 1989.
64. V. M. Kopytov, *The solvability of the occurrence problem in finitely generated solvable matrix groups over an algebraic number field*, Algebra i Logika **7** (1968), no. 6, 53–63.
65. M. J. Larsen and A. Shalev, *A probabilistic Tits alternative and probabilistic identities*, Algebra Number Theory **10** (2016), no. 6, 1359–1371.
66. J. C. Lennox and D. J. S. Robinson, *The Theory of Infinite Soluble Groups*, Oxford University Press, Oxford, 2004.
67. E. H. Lo and G. Ostheimer, *A practical algorithm for finding matrix representations for polycyclic groups*, J. Symbolic Comput. **28** (1999), no. 3, 339–360.
68. D. D. Long and A. W. Reid, *Small subgroups of* $\mathrm{SL}(3,\mathbb{Z})$, Exp. Math. **20** (2011), no. 4, 412–425.
69. D. D. Long, A. W. Reid, and M. Thistlethwaite, *Zariski dense surface subgroups in* $\mathrm{SL}(3,\mathbb{Z})$, Geom. Topol. **15** (2011), 1–9.
70. D. D. Long and M. B. Thistlethwaite, *Zariski dense surface subgroups in* $\mathrm{SL}(4,\mathbb{Z})$, Exp. Math. **27** (2018), no. 1, 82–92.
71. A. Lubotzky, *One for almost all: generation of* $\mathrm{SL}(n,p)$ *by subsets of* $\mathrm{SL}(n,\mathbb{Z})$, Contemp. Math. **243**, 125–128, 1999.

72. A. Lubotzky and D. Segal, *Subgroup Growth*, Birkhäuser, Basel, 2003.
73. E. M. Luks, *Computing in solvable matrix groups*, Proc. 33rd IEEE Symposium on Foundations of Computer Science, pp. 111–120, 1992.
74. Maple. Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario, `http://www.maplesoft.com`
75. Mathematica, Wolfram Research, Inc., Champaign, Illinois, `http://www.wolfram.com/mathematica/`
76. C. Meiri, Generating pairs for finite index subgroups of $\mathrm{SL}(n, \mathbb{Z})$, *J. Algebra* **470** (2017), 420–424.
77. J. L. Mennicke, *Finite factor groups of the unimodular group*, Ann. of Math. (2) **81** (1965), 31–37.
78. K. A. Mihaĭlova, *The occurrence problem for direct products of groups*, Dokl. Akad. Nauk SSSR **119** (1958), 1103–1105.
79. C. F. Miller, III, *Decision problems for groups: survey and reflections*. Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989), 1–59, Math. Sci. Res. Inst. Publ., 23, Springer, New York, 1992.
80. A. Myasnikov, V. Shpilrain, and A. Ushakov, *Non-commutative Cryptography and Complexity of Group-theoretic Problems*, Mathematical Surveys and Monographs, vol. 177, American Mathematical Society, Providence, RI, 2011.
81. G. Nebe and W. Plesken, *Finite Rational Matrix Groups*, Mem. Amer. Math. Soc. **116** (1995), no. 556, American Mathematical Society, Providence, RI.
82. M. Neunhöffer, Á. Seress, et al., *Recog: a collection of group recognition methods*, `http://gap-packages.github.io/recog/`
83. M. Newman, *Integral Matrices*, Academic Press, New York, 1972.
84. W. Nickel, *Matrix representations for torsion-free nilpotent groups by Deep Thought*, J. Algebra **300** (2006), no. 1, 376–383.
85. E. A. O'Brien, *Algorithms for matrix groups*, Groups St Andrews 2009 in Bath. Vol. 2, London Math. Soc. Lecture Note Ser. **388**, Cambridge Univ. Press, Cambridge, 2011, pp. 297–323.
86. G. Ostheimer, *Practical algorithms for polycyclic matrix groups*, J. Symbolic Comput. **28** (1999), no. 3, 361–379.
87. W. Plesken, *Presentations and representations of groups*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 423–434.
88. M. S. Raghunathan, *The congruence subgroup problem*, Proc. Indian Acad. Sci. (Math. Sci.) **114** (2004), no. 4, 299–308.
89. A. S. Rapinchuk, *Strong approximation for algebraic groups*, Thin groups and superstrong approximation, Math. Sci. Res. Inst. Publ., vol. 61, Cambridge Univ. Press, Cambridge, 2014, pp. 269–298.
90. I. Rivin, *Large Galois groups with applications to Zariski density*, `http://arxiv.org/abs/1312.3009v4`
91. I. Rivin, *Zariski density and genericity*, Int. Math. Res. Not. IMRN 2010, no. 19, 3649–3657.
92. I. Rivin, *How to pick a random integer matrix? (and other questions)*, Math. Comp. **85** (2016), no. 298, 783–797.
93. D. N. Rockmore, K.-S. Tan, and R. Beals, *Deciding finiteness for matrix groups over function fields*, Israel J. Math. **109** (1999), 93–116.
94. L. Rónyai, *Computations in associative algebras*, Groups and computation (New Brunswick, NJ, 1991), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, RI, 1993, pp. 221–243.
95. SageMath, the Sage Mathematics Software System, The Sage Developers, `http://www.sagemath.org`

96. P. Sarnak, *Notes on thin matrix groups*, Thin groups and superstrong approximation, 343–362, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014.
97. Á. Seress, *An introduction to computational group theory*, Notices Amer. Math. Soc. **44** (1997), no. 6, 671–679.
98. M. Shirvani and B. A. F. Wehrfritz, *Skew Linear Groups*, London Math. Soc. Lecture Note Ser., vol. 118, Cambridge Univ. Press, Cambridge, 1986.
99. C. C. Sims, *Computation with Finitely Presented Groups*, Encyclopedia of Mathematics and its Applications, vol. 48, Cambridge Univ. Press, Cambridge, 1994.
100. S. Singh and T. Venkataramana, *Arithmeticity of certain symplectic hypergeometric groups*, Duke Math. J. **163** (2014), no. 3, 591–617.
101. R. Steinwandt, *On computing a separating transcendence basis*, SIGSAM Bull. **34** (2000), no. 4, 3–6.
102. D. A. Suprunenko, *Matrix Groups*, Translations of Mathematical Monographs, vol. 45, American Mathematical Society, Providence, R.I., 1976.
103. B. Sury and T. N. Venkataramana, *Generators for all principal congruence subgroups of* $\mathrm{SL}(n, Z)$ *with* $n \geq 3$, Proc. Amer. Math. Soc. **122** (1994), no. 2, 355–358.
104. J. Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972), 250–270.
105. B. A. F. Wehrfritz, *Infinite Linear Groups*, Springer-Verlag, New York, 1973.
106. B. A. F. Wehrfritz, *Conditions for linear groups to have unipotent derived subgroups*, J. Algebra **323** (2010), 3147–3154.
107. J. S. Wilson, *The normal and subnormal structure of general linear groups*, Proc. Cambridge Philos. Soc. **71** (1972), 163–177.
108. A. E. Zalesskii, *Linear groups*, Russian Math. Surveys **36** (1981), no. 5, 63–128.
109. A. E. Zalesskii, *Linear groups*, translated from Itogi Nauki i Tekhniki, Seriya Algebra, Topologiya, Geometriya **21** (1983), 135–182 (2974–3004).
110. A. E. Zalesskii, *Linear groups*, Algebra, IV, Encyclopaedia Math. Sci., vol. 37, Springer, Berlin, 1993, pp. 97–196.

SCHOOL OF COMPUTER SCIENCE, UNIVERSITY OF ST ANDREWS, NORTH HAUGH, ST ANDREWS KY16 9SX, UK

E-mail address: ad271@st-andrews.ac.uk

SCHOOL OF MATHEMATICS, STATISTICS AND APPLIED MATHEMATICS, NATIONAL UNIVERSITY OF IRELAND GALWAY, GALWAY H91TK33, IRELAND

E-mail address: dane.flannery@nuigalway.ie