ALGORITHMS FOR THE TITS ALTERNATIVE AND RELATED PROBLEMS

A. S. DETINKO, D. L. FLANNERY, AND E. A. O'BRIEN

ABSTRACT. We present an algorithm to decide whether a finitely generated linear group over an infinite field is solvable-by-finite, thereby obtaining a computationally effective version of the Tits alternative. We also give algorithms to decide whether the group is nilpotent-by-finite, abelian-by-finite, or central-by-finite. Implementations of the algorithms are publicly available in MAGMA.

1. INTRODUCTION

The *Tits alternative*, established by Tits [28], states that a finitely generated linear group over a field either is solvable-by-finite, or it contains a non-cyclic free subgroup. This theorem partitions finitely generated linear groups into two very different classes, which require separate treatment. Consequently, one of the first questions that must be settled for such a group is to determine the class of the Tits alternative to which it belongs. In the class of groups with non-cyclic free subgroups, some basic computational problems are undecidable in general; whereas solvable-by-finite groups are more amenable to computation (see [16, Section 3]). For further discussion of the Tits alternative, and its influence on other areas of group theory, we refer to [18].

Algorithms to decide the Tits alternative over the rational field $\mathbb{Q}$ were proposed in [6, 7]. Drawing on results of [17], a different approach was considered in [24]. Another algorithm for the Tits alternative in $\mathrm{GL}(n, \mathbb{Q})$, as well as practical algorithms to test solvability and polycyclicity of rational matrix groups, appeared in [1, 2, 3]. We are not aware of implementations of these algorithms to decide the Tits alternative over $\mathbb{Q}$.

This paper gives a practical algorithm to decide whether a finitely generated linear group over an arbitrary field is solvable-by-finite. Additionally, we can test whether the group is solvable. Our method uses congruence homomorphism techniques (see [16, Section 4]), which were applied previously to special cases of the problems mentioned above; namely, deciding finiteness and nilpotency [11, 12, 13, 14]. We also rely on two other recent developments. The first is a description by Wehrfritz [30] of congruence subgroups of solvable-by-finite linear groups. The second is the development of effective algorithms to construct presentations of matrix groups over finite fields (see [4, 23]).

If the field is $\mathbb{Q}$, our algorithm to test virtual solvability is a refinement and extension of that in [1]. However, we consider finitely generated linear groups defined over an arbitrary field (albeit possibly with a finite number of exceptions in positive characteristic). We also solve the related problems of deciding whether a group defined over a field of characteristic zero is virtually nilpotent, virtually abelian, or central-by-finite. The resulting algorithms are practical, and implementations are publicly available in MAGMA [8].

Detinko and Flannery were supported by Science Foundation Ireland grants 07/MI/007 and 08/RFP/MTH1331. O'Brien was supported by the Marsden Fund of New Zealand grant UOA 1015. He thanks the Department of Mathematics, National Cheng Kung University, Taiwan, for its hospitality while this work was completed. Most importantly, we are very much indebted to Professor B. A. F. Wehrfritz, who kindly provided us with his new results [30] on congruence subgroups of solvable-by-finite linear groups.

Date: April 11, 2012.

We emphasize that this paper demonstrates that the various problems of testing virtual properties are *decidable* for finitely generated groups over a wide range of fields. Solvability testing was previously known to be decidable for groups over number fields [21].

Section 2 sets up the background theory for our congruence homomorphism techniques. In Section 3 we present an algorithm to decide virtual solvability. Section 4 deals with the special case where the group is completely reducible. In Section 5 we outline algorithms to decide whether a group in characteristic zero is nilpotent-by-finite, abelian-by-finite, or central-by-finite. Finally, we report on the MAGMA implementation of our algorithms.

2. CONGRUENCE HOMOMORPHISMS AND COMPUTING IN SOLVABLE-BY-FINITE GROUPS

We start by fixing some notation. Let $G = \langle S \rangle \leq \mathrm{GL}(n, \mathbb{F})$, where $S = \{g_1, \ldots, g_r\}$ and $\mathbb{F}$ is an infinite field. Denote the integral domain generated by the entries of the matrices in $S \cup S^{-1}$ by R. Recall that R/ρ is a finite field if ρ is a maximal ideal of R [29, 4.1, p. 50]. Let ρ be an ideal of a subring Δ of $\mathbb{F}$; then natural projection $\Delta \to \Delta/\rho$ extends to a group homomorphism $\mathrm{GL}(n, \Delta) \to \mathrm{GL}(n, \Delta/\rho)$ and a ring homomorphism $\mathrm{Mat}(n, \Delta) \to \mathrm{Mat}(n, \Delta/\rho)$. We denote all these homomorphisms by ψ_ρ. The kernel of ψ_ρ on G is denoted G_ρ, and is called a *congruence subgroup* of G.

2.1. **Congruence subgroups of solvable-by-finite groups.** Each solvable-by-finite linear group has a triangularizable normal subgroup of finite index [27, Theorem 7, p. 135]; in particular, its Zariski connected component is unipotent-by-abelian. Proving that G is solvable-by-finite is therefore equivalent to proving that G has a unipotent-by-abelian normal subgroup of finite index. So to apply congruence homomorphism techniques to computing in the first class of the Tits alternative, we should first answer the following question: if G is solvable-by-finite, for which ideals $\rho \subseteq R$ is G_ρ unipotent-by-abelian? We summarize recent results of Wehrfritz [30, Theorems 1–3] that describe such ideals (as usual, H' is the commutator subgroup $[H, H]$ of a group H).

Theorem 2.1. *Suppose that $G \leq \mathrm{GL}(n, \Delta)$ is solvable-by-finite, where Δ is an integral domain.*

(i) *Let ρ be an ideal of Δ. If $\mathrm{char}\,\Delta = p > n$, or $\mathrm{char}\,\Delta = 0$ and $\mathrm{char}(\Delta/\rho) = p > n$, then G'_ρ is unipotent.*

(ii) *Suppose that Δ is a Dedekind domain of characteristic zero, and ρ is a maximal ideal of Δ. If $p \in \mathbb{Z}$ is an odd prime such that $p \in \rho \setminus \rho^{p-1}$, then G_ρ is connected; hence G'_ρ is unipotent.*

We call $\psi_\rho : \mathrm{GL}(n, \Delta) \to \mathrm{GL}(n, \Delta/\rho)$ a *W-homomorphism* if Δ/ρ is finite and G'_ρ is unipotent whenever $G \leq \mathrm{GL}(n, \Delta)$ is solvable-by-finite.

2.2. **Construction of W-homomorphisms.** We may assume that $\mathbb{F}$ is finitely generated over its prime subfield, and is the field of fractions of R. Then it suffices to let $\mathbb{F}$ be one of

I. the rationals $\mathbb{Q}$,
II. a number field,
III. a function field $\mathbb{P}(x_1, \ldots, x_m)$, or
IV. a finite extension of $\mathbb{P}(x_1, \ldots, x_m)$,

where $\mathbb{P}$ is a number field or finite field in III–IV. See [16, Section 4] for more details.

In each case I–IV we explain below how to construct W-homomorphisms on $\mathrm{GL}(n, R)$. Note that if $\mathbb{F}$ has positive characteristic at most n, then in general we cannot construct a W-homomorphism.

For a subring Δ of a field, $\frac{1}{\mu}\Delta$ denotes the localization $\{x\mu^{-i} \mid x \in \Delta, i \geq 0\}$ of Δ at a non-zero element μ.

2.2.1. *The rational field.* (Cf. [17, Lemma 9].) Let $\mathbb{F} = \mathbb{Q}$. Then $R = \frac{1}{\mu}\mathbb{Z}$ for some $\mu \in \mathbb{Z} \setminus \{0\}$ determined by the denominators of entries in the elements of $S \cup S^{-1}$. By Theorem 2.1 (ii), if $p \in \mathbb{Z}$ is an odd prime not dividing μ, then reduction mod p is a W-homomorphism from $\mathrm{GL}(n, R)$ onto $\mathrm{GL}(n, p)$. We denote this homomorphism by $\Psi_1 = \Psi_{1,p}$.

2.2.2. *Number fields.* Let $\mathbb{F} = \mathbb{Q}(\alpha)$ where α is an algebraic integer. We may take $R = \frac{1}{\mu}\mathbb{Z}[\alpha]$, $\mu \in \mathbb{Z} \setminus \{0\}$. Let $f(t) = a_0 + \cdots + a_{k-1}t^{k-1} + t^k \in \mathbb{Z}[t]$ be the minimal polynomial of α. For a prime $p \in \mathbb{Z}$ not dividing μ, define $\psi_{2,p} : R \to \mathbb{Z}_p(\bar{\alpha})$ by

$$\psi_{2,p} : \textstyle\sum_{i=0}^{k-1} b_i\alpha^i \mapsto \sum_{i=0}^{k-1} \bar{b}_i\bar{\alpha}^i$$

where $\bar{b}_i$ denotes the reduction of b_i mod p, and $\bar{\alpha}$ is a root of $\bar{f}(t) = \bar{a}_0 + \cdots + \bar{a}_{k-1}t^{k-1} + t^k$.

Lemma 2.2. (i) *Let $p \in \mathbb{Z}$ be an odd prime dividing neither μ nor the discriminant of $f(t)$. Then $\psi_{2,p}$ is a W-homomorphism.*

(ii) *Let $p \in \mathbb{Z}$ be a prime greater than n not dividing μ. Then $\psi_{2,p}$ is a W-homomorphism.*

Proof. Let $\mathcal{O}$ be the ring of integers of $\mathbb{F}$. Select an irreducible factor $\bar{f}_j(t)$ of $\bar{f}(t)$, and let $f_j(t)$ be a pre-image of $\bar{f}_j(t)$ in $\mathbb{Z}[t]$. The ideal ρ of $\frac{1}{\mu}\mathcal{O}$ generated by p and $f_j(\alpha)$ is maximal, and $p \notin \rho^2$ (see [20, Proposition 3.8.1, Theorem 3.8.2]). Since the kernel of $\psi_{2,p}$ on $\mathrm{GL}(n, R)$ is contained in the kernel of ψ_ρ on $\mathrm{GL}(n, \frac{1}{\mu}\mathcal{O})$, Theorem 2.1 (ii) implies that $\psi_{2,p}$ is a W-homomorphism. The second part is immediate from Theorem 2.1 (i). □

For example, let $\mathbb{F}$ be the cth cyclotomic field; if p is an odd prime not dividing $\mathrm{lcm}(\mu, c)$, then $\psi_{2,p}$ is a W-homomorphism.

We denote the W-homomorphism $\psi_{2,p}$ for p as in Lemma 2.2 by $\Psi_2 = \Psi_{2,p}$.

2.2.3. *Function fields.* Let $\mathbb{F} = \mathbb{P}(x_1, \ldots, x_m)$, so $R \subseteq \frac{1}{\mu}\mathbb{P}[x_1, \ldots, x_m]$ for some $\mathbb{P}$-polynomial $\mu = \mu(x_1, \ldots, x_m)$. Suppose that $\alpha = (\alpha_1, \ldots, \alpha_m)$ is a non-root of μ, where the α_i are in the algebraic closure $\overline{\mathbb{P}}$ of $\mathbb{P}$. Note that if $\mathbb{P}$ is infinite then α can always be chosen in $\mathbb{P}^m$. Define $\psi_{3,\alpha}$ to be the substitution homomorphism that replaces x_i by α_i, $1 \leq i \leq m$.

Let $\mathrm{char}\, R = 0$. Set $\Psi_3 = \Psi_{3,\alpha,p} = \Psi_{i,p} \circ \psi_{3,\alpha}$, where $p > n$, $i = 1$ if $\mathbb{P} = \mathbb{Q}$, and $i = 2$ if $\mathbb{P} \neq \mathbb{Q}$ is a number field.

If $\mathrm{char}\, R = p > n$ then set $\Psi_3 = \Psi_{3,\alpha} = \psi_{3,\alpha}$.

In all cases Ψ_3 is a W-homomorphism by Theorem 2.1 (i).

2.2.4. *Algebraic function fields.* Let $\mathbb{F} = \mathbb{L}(\beta)$ where $\mathbb{L} = \mathbb{P}(x_1, \ldots, x_m)$, $|\mathbb{F}/\mathbb{L}| = e$ and β has minimal polynomial $f(t) = a_0 + \cdots + a_{e-1}t^{e-1} + t^e$. Then $R \subseteq \frac{1}{\mu}\mathbb{L}_0[\beta]$ for some $\mu \in \mathbb{L}_0 = \mathbb{P}[x_1, \ldots, x_m]$. We may assume that $f(t) \in \mathbb{L}_0[t]$.

Define $\psi_{4,\alpha}$ on $\mathrm{GL}(n, R)$ as follows. Let $\alpha \in \overline{\mathbb{P}}^m$, $\mu(\alpha) \neq 0$; and let $\tilde{\beta}$ be a root of $\tilde{f}(t) = \tilde{a}_0 + \cdots + \tilde{a}_{e-1}t^{e-1} + t^e$ where $\tilde{a}_i := \psi_{3,\alpha}(a_i)$. Each element of R may be uniquely expressed as $\sum_{i=0}^{e-1} c_i\beta^i$ for some $c_i \in \frac{1}{\mu}\mathbb{L}_0$. Then

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

where $\tilde{c}_i = \psi_{3,\alpha}(c_i)$.

Suppose that $\operatorname{char} R = 0$, so we can choose $\alpha \in \mathbb{P}^m$. Set $\Psi_4 = \Psi_{4,\alpha,p} = \Psi_{i,p} \circ \psi_{4,\alpha}$ where $p > n$, $i = 1$ if $\mathbb{P} = \mathbb{Q}$ and $\tilde{\beta} \in \mathbb{Q}$, and $i = 2$ otherwise.

If $\operatorname{char} R = p > n$ then set $\Psi_4 = \psi_{4,\alpha}$.

By Theorem 2.1 (i), Ψ_4 is a W-homomorphism.

Remark 2.3. An *SW-homomorphism* on $\mathrm{GL}(n, R)$ is a congruence homomorphism with finite image such that every torsion element of its congruence subgroup is unipotent (see [29, 4.8, p. 56] and [16, Section 4]). This property of the congruence subgroup is crucial to the algorithms of [14] for finiteness testing and structural analysis of finite matrix groups over infinite fields. The W-homomorphisms Ψ_i are SW-homomorphisms; moreover, this remains true for Ψ_3 and Ψ_4 without requiring that $p > n$.

3. Testing virtual solvability

3.1. **Preliminaries.** If ψ_ρ is a W-homomorphism on $\mathrm{GL}(n, R)$, then G is solvable-by-finite if and only if G'_ρ is unipotent. In this subsection we develop procedures to test whether a finitely generated subgroup of $\mathrm{GL}(n, R)$ is unipotent-by-abelian. Denote the $\mathbb{F}$-enveloping algebra of $M \subseteq \mathrm{Mat}(n, \mathbb{F})$ by $\langle M \rangle_{\mathbb{F}}$, and the $\mathbb{F}$-linear span of M by $\mathrm{span}_{\mathbb{F}}(M)$.

Lemma 3.1. *Let $H \leq \mathrm{GL}(n, \mathbb{F})$ be unipotent-by-abelian. Then $gh - hg \in \mathrm{Rad}\langle H \rangle_{\mathbb{F}}$ for all $g, h \in H$.*

Proof. (Cf. [17, p. 256] and [1, Lemma 5].) Since H' is unipotent, $h_1 = [g, h] - 1_n$ is nilpotent. For every $a \in \langle H \rangle_{\mathbb{F}}$, the matrix ah_1 is nilpotent (as H is triangularizable), and so $h_1 \in \mathrm{Rad}\langle H \rangle_{\mathbb{F}}$. Thus $gh - hg = hgh_1 \in \mathrm{Rad}\langle H \rangle_{\mathbb{F}}$. ☐

Lemma 3.2. *Let $H \trianglelefteq G$ where H is unipotent-by-abelian. If $x \in \mathrm{Rad}\langle H \rangle_{\mathbb{F}}$ then there is a non-zero G-module in the nullspace of x.*

Proof. The hypotheses on H ensure that $x^g \in \mathrm{Rad}\langle H \rangle_{\mathbb{F}}$ for all $g \in G$. Thus, the nullspace of $\mathrm{Rad}\langle H \rangle_{\mathbb{F}}$ is a (non-zero) G-module in the nullspace of x. ☐

In [13, p. 4155] we describe a simple recursive procedure $\texttt{ModuleViaNullSpace}(S, x)$ that finds, in no more than n iterations, a G-module U in the nullspace of $x \in \mathrm{Mat}(n, \mathbb{F})$ that contains every such G-module. Hence, if x is as in Lemma 3.2 then U is non-zero.

We now establish a convention. For a subset $K = \{h_1, \ldots, h_k\}$ of $\mathrm{Mat}(n, \mathbb{F})$, define

$$K^G = \{h_1^g, \ldots, h_k^g \mid g \in G\}.$$

If $K \subseteq G$ then $\langle K^G \rangle$ is the normal closure of $\langle K \rangle$ in G, which is usually denoted $\langle K \rangle^G$.

We next state a procedure that will be needed in several places later.

$\texttt{BasisAlgebraClosure}(K, S)$

Input: finite subsets K and $S = \{g_1, \ldots, g_r\}$ of $\mathrm{GL}(n, \mathbb{F})$.
Output: A basis of the $\mathbb{F}$-enveloping algebra of $\langle K^G \rangle$, where $G = \langle S \rangle$.

(1) $\mathcal{A} := K \cup K^{-1}$.
(2) While $\exists\, g \in S \cup S^{-1}$ and $A \in \mathcal{A}$ such that $g^{-1}Ag \notin \mathrm{span}_{\mathbb{F}}(\mathcal{A})$, do
   $\mathcal{A} := \mathcal{A} \cup \{g^{-1}Ag\}$.

(3) 'Spin up' to construct a basis $\mathcal{B}$ of the $\mathbb{F}$-enveloping algebra of $\langle \mathcal{A} \rangle$.
(4) Return $\mathcal{B}$.

`BasisAlgebraClosure` terminates in at most n^2 iterations. For a discussion of the well-known 'spinning up' method in step (3), see, e.g., [12, Section 3.1]. One feature of `BasisAlgebraClosure` is that the basis $\mathcal{B}$ returned consists of elements of $\langle K^G \rangle$.

Remark 3.3. If $K \subseteq \mathrm{Mat}(n, \mathbb{F})$ contains non-invertible elements, then the obvious modifications should be made to `BasisAlgebraClosure`. That is, $\mathcal{A}$ is initialized to K in step (1); and in step (3) a basis of $\langle \mathcal{A} \rangle_{\mathbb{F}}$ is constructed (by the same spinning up as before). The output of this modified procedure, which we name `BasisAlgebraClosure`*, is a basis of $\langle K^G \rangle_{\mathbb{F}}$.

3.2. **Testing virtual solvability.** Let U be a H-submodule of $V := \mathbb{F}^n$, where $H \leq \mathrm{GL}(n, \mathbb{F})$. Extend a basis of U to one of V, with respect to which H has block triangular form. We denote the projection homomorphism of H onto the corresponding block diagonal group in $\mathrm{GL}(n, \mathbb{F})$ by π_U. The kernel of π_U is a unipotent normal subgroup of H.

`NormalGenerators` is a procedure that accepts S and a W-homomorphism $\Psi = \psi_\rho$ as input, and returns *normal generators* for G_ρ, i.e., generators for a subgroup whose normal closure in G is G_ρ. This procedure first finds a presentation $\mathcal{P}$ of $\Psi(G)$ on the generating set $\Psi(g_1), \ldots, \Psi(g_r)$. Such presentations can be computed using algorithms from [4, 23]. The relators in $\mathcal{P}$ are then evaluated by replacing each occurrence of $\Psi(g_i)$ in each relator by g_i, $1 \leq i \leq r$. The resulting words in the g_i constitute the output of `NormalGenerators`.

We also need the following recursive procedure.

`ExploreBasis`$(\mathcal{A}, T)$

Input: finite subsets $\mathcal{A}, T$ of $\mathrm{GL}(m, \mathbb{F})$, where $\mathcal{A} \subseteq \langle T \rangle$.
Output: `true` or `false`.

(1) If $[A_i, A_j] = 1_m \ \forall\, A_i, A_j \in \mathcal{A}$ then return `true`.
(2) $U_1 :=$ `ModuleViaNullSpace`$(T, A_iA_j - A_jA_i)$ where $[A_i, A_j] \neq 1_m$.
If $U_1 = \{0\}$ then return `false`.
(3) $\pi := \pi_{U_1}$, $U_2 := V/U_1$.
(4) For $\ell = 1, 2$ do
$\mathcal{A}_\ell := \{\pi(A_j)_{|U_\ell} \mid A_j \in \mathcal{A}\}$, $T_\ell := \{\pi(h_j)_{|U_\ell} \mid h_j \in T\}$;
if `ExploreBasis`$(\mathcal{A}_\ell, T_\ell) =$ `false` then return `false`.
(5) Return `true`.

Now we can assemble our algorithm to decide the Tits alternative.

`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 and `false` otherwise.

(1) $K :=$ `NormalGenerators`(S, Ψ), Ψ a W-homomorphism on $\mathrm{GL}(n, R)$.
(2) $\mathcal{A} :=$ `BasisAlgebraClosure`(K, S).
(3) Return `ExploreBasis`$(\mathcal{A}, S)$.

Remark 3.4. When $\mathbb{F} = \mathbb{Q}$, `IsSolvableByFinite` is similar to the algorithm of [1, p. 1280]—but see the first paragraph of [1, Section 10.1].

`IsSolvableByFinite` terminates in no more than n iterations at step (3). A report of `false` is correct by Lemmas 3.1 and 3.2. Note that if `true` is returned at the first pass through step (1) of `ExploreBasis`, then G is abelian-by-finite.

Algorithms to test solvability of matrix groups over finite fields are implemented in [3, 8]. We can augment `IsSolvableByFinite` by checking solvability of $\Psi(G)$ during step (1), and thus obtain a solvability testing algorithm for finitely generated subgroups of $\mathrm{GL}(n, \mathbb{F})$. Moreover, when $R = \mathbb{Z}$, these algorithms decide whether G is polycyclic or polycyclic-by-finite (cf. [5, Theorem 4.2]).

We now point out some further additions to our basic method for deciding virtual solvability.

First suppose that $\mathrm{char}\,\mathbb{F} = 0$. Sometimes we can quickly detect that G is not solvable-by-finite, by means of the following observations. A classical theorem of Jordan states that there is a function $f : \mathbb{N} \to \mathbb{N}$ (independent of $\mathbb{F}$) such that if G is a finite subgroup of $\mathrm{GL}(n, \mathbb{F})$, then G has an abelian normal subgroup of index bounded by $f(n)$. It follows from [29, 10.11, p. 142] that if G is solvable-by-finite, then the solvable radical of $\Psi(G)$ has index bounded by $f(n)$. To apply this criterion, we use an algorithm described in [19, Section 4.7.5] to compute the index of the solvable radical of a matrix group over a finite field, and then we compare this index with $f(n)$. Collins [9] has found the optimal function f for all n. In particular, $f(n) = (n + 1)!$ for $n \geq 71$.

Next, recall that if $\Psi = \psi_\rho$ is $\Psi_{3,\alpha,p}$ or $\Psi_{4,\alpha,p}$, then p must be greater than n by definition. However, with extra restrictions in place, it is possible to test virtual solvability in characteristic $p \leq n$ too. Suppose that ρ is a proper ideal of R such that either (i) $\mathrm{char}\,R = 0$, $\mathrm{char}(R/\rho) > 0$ and G_ρ is generated by unipotent elements; or (ii) $\mathrm{char}\,R > 0$ and G_ρ is generated by diagonalizable elements. Then G is solvable-by-finite if and only if G'_ρ is unipotent: this follows from the last paragraph of [30, Section 1], and [30, Theorem 1 (d)]. We can determine whether (i) or (ii) holds by checking whether each normal generator of G_ρ is unipotent or diagonalizable.

4. Completely reducible groups

Some of our problems coincide in an important special case.

Lemma 4.1. *Suppose that $G \leq \mathrm{GL}(n, \mathbb{F})$ is completely reducible, where $\mathbb{F}$ is any field. Then the following are equivalent:*

(i) *G is solvable-by-finite;*
(ii) *G is nilpotent-by-finite;*
(iii) *G is abelian-by-finite.*

Proof. Trivially (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i). If G is solvable-by-finite, then a normal unipotent-by-abelian subgroup of G must be abelian, because a completely reducible unipotent group is trivial. Thus (i) implies (iii). □

Motivated by Lemma 4.1, we consider how to decide whether a solvable-by-finite group G is completely reducible. Let ψ_ρ be a W-homomorphism on $\mathrm{GL}(n, R)$. If G_ρ is completely reducible (hence abelian) and $\mathrm{char}\,R$ does not divide $|G : G_\rho|$, then G is completely reducible by [27, Theorem 1, p. 122]. Therefore, in characteristic zero, G is completely reducible if and only if the elements of $\texttt{BasisAlgebraClosure}(K, S)$ commute pairwise and are all diagonalizable, where $K = \texttt{NormalGenerators}(S, \psi_\rho)$. If $\operatorname{char} R = p > 0$ divides $|G : G_\rho|$, then we cannot decide complete reducibility of G; otherwise we apply the characteristic zero criterion.

A finitely generated solvable linear group may not be finitely presentable [29, 4.22, p. 66]. However, if G is both solvable-by-finite and completely reducible, then G_ρ is a finitely generated abelian normal subgroup of finite index. So we can compute presentations of G_ρ and $\psi_\rho(G)$, and combine them as explained in [1, 4], to obtain a finite presentation of G.

5. Testing virtual nilpotency and related algorithms

We now consider the problems of deciding whether a finitely generated linear group is nilpotent-by-finite, abelian-by-finite, or central-by-finite. Algorithms for nilpotency testing and computing with finitely generated nilpotent groups over arbitrary fields are given in [10, 11].

Henceforth $\operatorname{char} \mathbb{F} = 0$ unless stated otherwise.

5.1. **Preliminaries.**

Lemma 5.1. *Let $H \leq \mathrm{GL}(n, \mathbb{F})$ be nilpotent-by-finite (resp. abelian-by-finite), $\mathbb{F}$ any field. If H is connected then H is nilpotent (resp. abelian).*

Proof. (Cf. [17, Lemma 9].) Let $N \leq H$ be nilpotent (resp. abelian) of finite index. Then the Zariski closure of N in H is nilpotent (resp. abelian) and contains the connected component of H; see [29, Chapter 5]. The lemma follows. □

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

Proof. This follows from Theorem 2.1 (ii) and Lemma 5.1. □

Denote by $g_d, g_u \in \mathrm{GL}(n, \mathbb{F})$ the diagonalizable and unipotent parts of $g \in \mathrm{GL}(n, \mathbb{F})$, i.e., $g = g_d g_u = g_u g_d$ is the Jordan decomposition of g. For $X \subseteq \mathrm{GL}(n, \mathbb{F})$ we put

$$X_d = \{x_d \mid x \in X\} \qquad \text{and} \qquad X_u = \{x_u \mid x \in X\}.$$

Proposition 5.3. *Let $H = \langle K^G \rangle$, where K is a finite subset of G. Then H is nilpotent and H' is unipotent if and only if $\langle K_d^G \rangle$ is abelian, $\langle K_u^G \rangle$ is unipotent, and $[K_d^G, K_u^G] = \{1_n\}$.*

Proof. If $\langle K_d^G \rangle$ is abelian, $\langle K_u^G \rangle$ is unipotent, and these groups centralize each other, then the group L that they generate is unipotent-by-abelian and nilpotent. Hence the same is true for $H \leq L$.

Now suppose that H is unipotent-by-abelian and nilpotent. Then $f_d : H \to H_d$, $f_u : H \to H_u$ defined by

$$f_d : h \mapsto h_d, \qquad f_u : h \mapsto h_u$$

are homomorphisms by [26, Proposition 3, p. 136]. Thus

$$H_d = \langle f_d(K^G) \rangle \qquad \text{and} \qquad H_u = \langle f_u(K^G) \rangle.$$

Now $h^g = h_d^g h_u^g$ and h_d^g, h_u^g are diagonalizable, unipotent respectively. Uniqueness of the Jordan decomposition implies that $h_d^g = (h^g)_d$ and $h_u^g = (h^g)_u$, so

$$H_d = \langle K_d^G \rangle \qquad \text{and} \qquad H_u = \langle K_u^G \rangle.$$

Thus $\langle K_u^G \rangle$ is unipotent. Since H is nilpotent, $[K_d^G, K_u^G] = \{1_n\}$ (see [26, Proposition 3, p. 136] again). Finally, since $\langle K_d^G \rangle = H_d$ is unipotent-by-abelian and completely reducible, it must be abelian. □

5.2. **Nilpotent-by-finite and abelian-by-finite groups.** Our algorithms for deciding whether G is nilpotent-by-finite or abelian-by-finite require that G be defined over a Dedekind domain R. Hence they apply, for example, when $\mathbb{F}$ is $\mathbb{Q}$, a number field, or (a finite extension of) a univariate function field.

Lemma 5.4. *Let $K \subseteq \mathrm{GL}(n, \mathbb{F})$, and $\widetilde{K} := \{h - 1_n \mid h \in K \cup K^{-1}\}$. Then $H = \langle K \rangle$ is unipotent if and only if $\langle \widetilde{K} \rangle_{\mathbb{F}}$ is nilpotent.*

Proof. Observe that $\langle \widetilde{K} \rangle_{\mathbb{F}} = \mathrm{span}_{\mathbb{F}}(\{h - 1_n \mid h \in H\})$. Therefore, if H is unipotent then H^x is unitriangular for some $x \in \mathrm{GL}(n, \mathbb{F})$, so $\langle \widetilde{K} \rangle_{\mathbb{F}}$ is nilpotent. Conversely, if $\langle \widetilde{K} \rangle_{\mathbb{F}}$ is nilpotent then $h - 1_n$ is nilpotent for all $h \in H$, i.e., H is unipotent. □

Let K be a finite subset of $\mathrm{GL}(n, \mathbb{F})$. The procedure `IsAbelianClosure` determines whether $\langle K^G \rangle$ is abelian by testing whether the elements of `BasisAlgebraClosure`(K, S) commute pairwise. Another auxiliary procedure is the following (recall Remark 3.3).

`IsUnipotentClosure`(K, S)

Input: finite subsets $K = \{h_1 \ldots, h_k\}$ and S of $\mathrm{GL}(n, \mathbb{F})$, where the h_i are unipotent.
Output: `true` if $\langle K^G \rangle$ is unipotent, `false` otherwise, where $G = \langle S \rangle$.

(1) $\widetilde{K} := \{h_j - 1_n \mid 1 \leq j \leq k\}$.
(2) $\mathcal{B} :=$ `BasisAlgebraClosure`$^*(\widetilde{K}, S)$.
(3) If $|\mathcal{B}| > n(n-1)/2$, or B is not nilpotent for some $B \in \mathcal{B}$ (i.e., $B^n \neq 0_n$), then return `false`.
(4) If $\langle B + 1_n : B \in \mathcal{B} \rangle$ is unipotent then return `true`; else return `false`.

Remark 5.5. Lemma 5.4 guarantees correctness of `IsUnipotentClosure`. See [10, Section 2.1] for a procedure to test whether a finitely generated linear group is unipotent.

Let Ψ be a W-homomorphism as in Corollary 5.2. By Proposition 5.3, we have the following algorithm to test virtual nilpotency.

`IsNilpotentByFinite`(S)

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

(1) $K := \{h_1, \ldots, h_k\} =$ `NormalGenerators`(S, Ψ).
(2) $K_d := \{(h_i)_d \mid 1 \leq i \leq k\}$, $K_u := \{(h_i)_u \mid 1 \leq i \leq k\}$.
(3) If not `IsUnipotentClosure`(K_u, S) or not `IsAbelianClosure`(K_d, S) or $[K_d^G, K_u^G] \neq \{1_n\}$ then return `false`; else return `true`.

Remark 5.6. In step (3) we use the fact that $[K_d^G, K_u^G] = \{1_n\}$ if and only if the elements of $\texttt{BasisAlgebraClosure}(K_d, S)$ commute with the elements of $\texttt{BasisAlgebraClosure}(K_u, S)$ (these two bases are already computed in this step).

Similarly, for Dedekind domains R of characteristic zero, the algorithm $\texttt{IsAbelianByFinite}(S)$ decides whether G is abelian-by-finite: it returns $\texttt{IsAbelianClosure}(K, S)$, where as usual K is $\texttt{NormalGenerators}(S, \Psi)$.

If either of $\texttt{IsNilpotentByFinite}(S)$ or $\texttt{IsAbelianByFinite}(S)$ returns `true`, then we can decide complete reducibility of G: now G is completely reducible if and only if $K_u = \{1_n\}$.

5.3. **Central-by-finite groups.** In this subsection, instead of a W-homomorphism we may use more generally an SW-homomorphism (see Remark 2.3).

Lemma 5.7. *Let H be a group such that H' is finite. If A is a torsion-free normal subgroup of H, then A is central.*

Proof. Since $[A, H] \leq A \cap H' = \{1\}$, this is clear. □

Corollary 5.8. *Let $\mathbb{F}$ be any field of characteristic zero, and let $\Psi = \psi_\rho$ be an SW-homomorphism on $\mathrm{GL}(n, R)$. Then $G \leq \mathrm{GL}(n, \mathbb{F})$ is central-by-finite if and only if G_ρ is central.*

Proof. If G is central-by-finite then G' is finite by a result of Schur [25, 10.1.4, p. 287]. Since G_ρ is torsion-free, it is central by Lemma 5.7. The other direction is trivial because $|G : G_\rho|$ is finite. □

Corollary 5.8 underpins a simple procedure $\texttt{IsCentralByFinite}(S)$ which returns `true` if $[K, S] = \{1_n\}$, where $G_\rho = \langle K^G \rangle$; else it returns `false`. Here $\mathbb{F}$ is any field of characteristic zero. The same procedure works for the fields $\mathbb{F}$ of positive characteristic in Sections 2.2.3–2.2.4, provided that Ψ is a W-homomorphism as defined there and G_ρ is completely reducible (hence torsion-free).

We could also decide whether G is central-by-finite by checking whether the 'adjoint' representation that arises from the conjugation action of G on $\langle G \rangle_\mathbb{F}$ has finite image (using, e.g., the algorithms of [14]), as suggested in [7]. While this approach is valid for all fields $\mathbb{F}$, it may involve computing with matrices of dimension n^2.

6. IMPLEMENTATION AND PERFORMANCE

We have implemented our algorithms as part of the MAGMA package INFINITE [15]. We use the COMPOSITIONTREE package [4, 23] to study congruence images and construct their presentations.

In practice, the single most expensive task is evaluating relators to obtain normal generators for the kernel of a W-homomorphism.

We describe below sample outputs covering the main domains and types of groups. The experiments were performed using MAGMA V2.17-2 on a 2GHz machine. The examples are randomly conjugated so that generators are not sparse, and matrix entries are typically large. All (algebraic) function fields $\mathbb{F}$ in these examples are univariate, and if they have zero characteristic are over $\mathbb{Q}$. Since random selection plays a role in some of the algorithms, times have been averaged over three runs. The complete examples are available in the INFINITE package.

(1) $G_1 \leq \mathrm{GL}(7, \mathbb{F})$ where $\mathbb{F}$ is a function field of characteristic zero. It is conjugate to an infinite monomial subgroup of $\mathrm{GL}(7, \mathbb{Q})$. We decide that this 4-generator group is abelian-by-finite in 82s.

(2) $G_2 \leq \mathrm{GL}(40, \mathbb{F})$ where $\mathbb{F}$ is an algebraic function field of characteristic zero. It is conjugate to an infinite completely reducible nilpotent subgroup of $\mathrm{GL}(40, \mathbb{Q})$. We decide that this 4-generator group is central-by-finite in 30s.
(3) $G_3 \leq \mathrm{GL}(56, \mathbb{F})$ where $\mathbb{F}$ is an algebraic function field of characteristic zero. It is conjugate to the Kronecker product of an infinite reducible nilpotent subgroup of $\mathrm{GL}(8, \mathbb{Q})$ with a primitive complex reflection group from the Shephard-Todd list. We decide that this 7-generator group is nilpotent-by-finite in 219s.
(4) $G_4 \leq \mathrm{GL}(18, \mathbb{F})$ where $\mathbb{F}$ is a function field over $\mathrm{GF}(19)$. It is conjugate to the Kronecker product of a solvable subgroup of $\mathrm{GL}(6, 19)$ with an infinite triangular subgroup of $\mathrm{GL}(3, \mathbb{F})$. We decide that this 13-generator group is solvable in 80s.
(5) $G_5 \leq \mathrm{GL}(32, \mathbb{F})$ where $\mathbb{F}$ is the fifth cyclotomic field. It is conjugate to the Kronecker product of an infinite solvable subgroup of $\mathrm{GL}(8, \mathbb{Q})$ from [3] with a primitive complex reflection group from the Shephard-Todd list. We decide that this 8-generator group is solvable-by-finite in 90s.
(6) $G_6 \leq \mathrm{GL}(12, \mathbb{F})$ where $\mathbb{F}$ is a function field of characteristic zero. It is conjugate to $\mathrm{SL}(12, \mathbb{Z})$. We decide that this 3-generator group is not solvable-by-finite in 10s.
(7) $G_7 \leq \mathrm{GL}(32, \mathbb{F})$ where $\mathbb{F}$ is a number field of degree 4 over $\mathbb{Q}$. It is conjugate to the Kronecker product of $\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \rangle$ with an infinite reducible nilpotent rational matrix group. We decide that this 4-generator group is not solvable-by-finite in 56s.

REFERENCES

1. B. Assmann and B. Eick, *Computing polycyclic presentations for polycyclic rational matrix groups*, J. Symbolic Comput. **40** (2005), no. 6, 1269–1284.
2. ______, *Testing polycyclicity of finitely generated rational matrix groups*, Math. Comp. **76** (2007), 1669–1682.
3. ______, Polenta. A refereed GAP 4 package, `www.gap-system.org/Packages/polenta.html` (2007).
4. H. Bäärnhielm, D. F. Holt, C.R. Leedham-Green, and E.A. O'Brien, *A new model for computation with matrix groups*, preprint (2011).
5. G. Baumslag, F. B. Cannonito, D. J. S. Robinson, and D. Segal, *The algorithmic theory of polycyclic-by-finite groups*, J. Algebra **142** (1991), no. 1, 118–149.
6. 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).
7. ______, *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.
8. 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.
9. M. J. Collins, *On Jordan's theorem for complex linear groups*, J. Group Theory **10** (2007), 411–423.
10. A. S. Detinko and D. L. Flannery, *Computing in nilpotent matrix groups*, LMS J. Comput. Math. **9** (2006), 104–134 (electronic).
11. ______, *Algorithms for computing with nilpotent matrix groups over infinite domains*, J. Symbolic Comput. **43** (2008), 8–26.
12. ______, *On deciding finiteness of matrix groups*, J. Symbolic Comput. **44** (2009), 1037–1043.
13. A. S. Detinko, D. L. Flannery, and E. A. O'Brien, *Deciding finiteness of matrix groups in positive characteristic*, J. Algebra **322** (2009), 4151–4160.
14. ______, *Recognizing finite matrix groups over infinite fields*, preprint (2011).
15. ______, The MAGMA package INFINITE, `http://magma.maths.usyd.edu.au/magma/` (2011).
16. A. S. Detinko, B. Eick, and D. L. Flannery, *Computing with matrix groups over infinite fields*, London Math. Soc. Lecture Note Ser. **387** (2011), 256–270.

17. J. D. Dixon, *The orbit-stabilizer problem for linear groups*, Canad. J. Math. **37** (1985), no. 2, 238–259.
18. J. D. Dixon, *The Tits alternative*, preprint, `http://math.carleton.ca/~jdixon/Titsalt.pdf`
19. D. F. Holt, B. Eick, and E. A. O'Brien, *Handbook of computational group theory*, Chapman and Hall/CRC, London, 2005.
20. H. Koch, *Number theory. Algebraic numbers and functions*, Graduate Studies in Mathematics, vol. 24, American Mathematical Society, Providence, RI, 2000.
21. 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 (Russian).
22. E. A. O'Brien, *Towards effective algorithms for linear groups*, Finite geometries, groups, and computation, Walter de Gruyter, Berlin, 2006, pp. 163–190.
23. E. A. O'Brien, *Algorithms for matrix groups*, London Math. Soc. Lecture Note Ser. **388** (2011), 297–323.
24. G. Ostheimer, *Practical algorithms for polycyclic matrix groups*, J. Symbolic Comput. **28** (1999), no. 3, 361–379.
25. D. J. S. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996.
26. D. Segal, *Polycyclic groups*, Cambridge University Press, Cambridge, 1983.
27. D. A. Suprunenko, *Matrix groups*, Transl. Math. Monogr., vol. 45, American Mathematical Society, Providence, RI, 1976.
28. J. Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972), 250–270.
29. B. A. F. Wehrfritz, *Infinite linear groups*, Springer-Verlag, 1973.
30. ______, *Conditions for linear groups to have unipotent derived subgroups*, J. Algebra **323** (2010), 3147–3154.

SCHOOL OF MATHEMATICS, STATISTICS AND APPLIED MATHEMATICS, NATIONAL UNIVERSITY OF IRELAND, GALWAY, IRELAND
E-mail address: `alla.detinko@nuigalway.ie`

SCHOOL OF MATHEMATICS, STATISTICS AND APPLIED MATHEMATICS, NATIONAL UNIVERSITY OF IRELAND, GALWAY, IRELAND
E-mail address: `dane.flannery@nuigalway.ie`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF AUCKLAND, PRIVATE BAG 92019, AUCKLAND, NEW ZEALAND
E-mail address: `e.obrien@auckland.ac.nz`