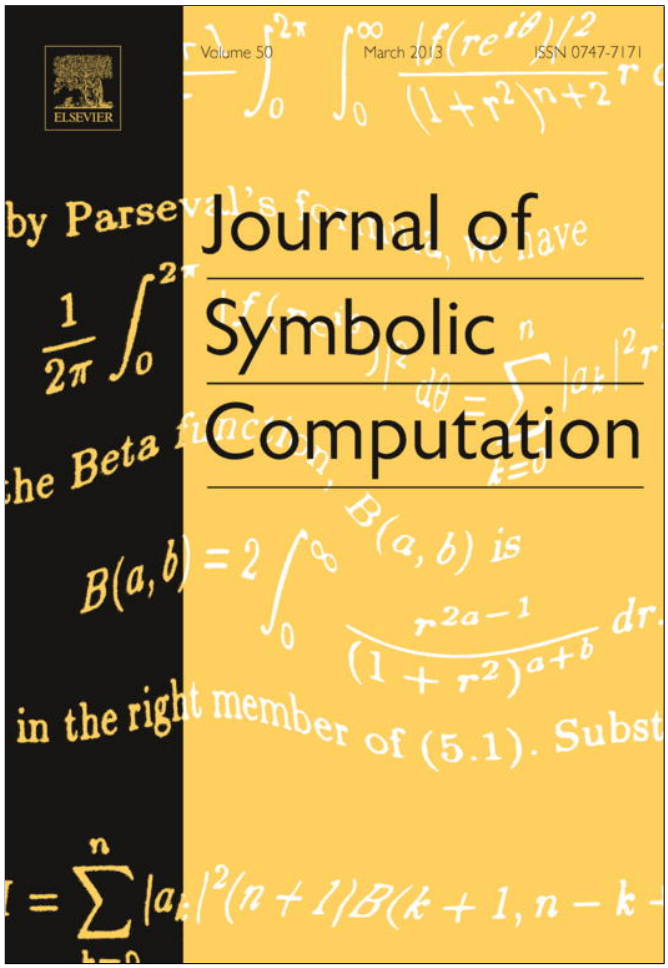

Journal of Symbolic Computation 50 (2013) 100–109

Contents lists available at SciVerse ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Recognizing finite matrix groups over infinite fields ☆

A.S. Detinko [a], D.L. Flannery [a], E.A. O'Brien [b]

[a] School of Mathematics, Statistics and Applied Mathematics, National University of Ireland, Galway, Ireland
[b] Department of Mathematics, The University of Auckland, Private Bag 92019, Auckland, New Zealand

ARTICLE INFO

Article history:
Received 12 January 2012
Accepted 10 April 2012
Available online 15 June 2012

Keywords:
Finitely generated linear group
Finite linear group
Decision problem
Algorithm

ABSTRACT

We present a uniform methodology for computing with finitely generated matrix groups over any infinite field. As one application, we completely solve the problem of deciding finiteness in this class of groups. We also present an algorithm that, given such a finite group as input, in practice successfully constructs an isomorphic copy over a finite field, and uses this copy to investigate the group's structure. Implementations of our algorithms are available in MAGMA.

1. Introduction

This paper establishes a uniform methodology for computing with finitely generated linear groups over any infinite field. Our techniques constitute a computational analogue of 'finite approximation' (Wehrfritz, 1973, Chapter 4), which is a major tool in the study of finitely generated linear groups. It relies on the fact that each finitely generated linear group G is residually finite. Moreover, G is approximated by matrix groups of the same degree over finite fields (Zalesskii, 1993, Theorem A, p. 151). We also use the fundamental result that G has a normal subgroup of finite index with every torsion element unipotent (Wehrfritz, 1973, 4.8, p. 56). For computational purposes, the key objective is to determine a congruence homomorphism whose kernel has this property, and whose image is defined over a finite field.

The first problem that we solve is a natural and obvious candidate for an application of our methodology: testing finiteness of finitely generated linear groups. This problem has been investigated

☆ 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. We are grateful to the referees for many useful comments and suggestions.

E-mail addresses: alla.detinko@nuigalway.ie (A.S. Detinko), dane.flannery@nuigalway.ie (D.L. Flannery), e.obrien@auckland.ac.nz (E.A. O'Brien).

0747-7171/$ – see front matter
http://dx.doi.org/10.1016/j.jsc.2012.04.002

previously, but only for groups over specific domains. Algorithms for testing finiteness over the rational field $\mathbb{Q}$ are given in Babai et al. (1993). One of these, based on integrality testing, is exploited as part of the default procedures in GAP (The GAP Group, 2012) and Magma (Bosma et al., 1997) to decide finiteness over $\mathbb{Q}$. Groups over a characteristic zero function field are considered in Rockmore et al. (1999). However, the algorithm there possibly involves squaring dimensions. Function fields are also dealt with in Detinko (2001), Detinko and Flannery (2009), Detinko et al. (2009), Ivanyos (2001), where computing in matrix algebras plays a central role. While the algorithms from Detinko and Flannery (2009), Detinko et al. (2009) have been implemented in Magma, we know of no implementations of those from Detinko (2001), Ivanyos (2001), Rockmore et al. (1999).

In this paper, we design a new finiteness testing algorithm that may be employed, for the first time, over any infinite field. The algorithm is concise and practical. Our implementation is distributed with Magma, and we demonstrate that it performs well for a range of inputs.

If a group G is finite then, in practice, we can often construct an isomorphic copy of G over some finite field. As a consequence, drawing on recent progress in computing with matrix groups over finite fields (Bäärnhielm et al., 2011; O'Brien, 2011), we obtain the first algorithms to answer many structural questions about G. These include: computing $|G|$; testing membership in G; computing Sylow subgroups, a composition series, and the solvable and unipotent radicals of G.

We emphasize that this paper provides a framework for the solution of broader computational problems than the testbed ones treated here. SW-homomorphisms (defined below) are used in Detinko and Flannery (2008) to test nilpotency over certain fields. In Detinko et al. (2011b), these are extended to decide virtual properties of finitely generated linear groups. The present paper gives a comprehensive account of our techniques that is valid in all settings. For further discussion of how these ideas have been developed, see the survey (Detinko et al., 2011).

Briefly, the paper is organized as follows. Sections 2 and 3 set up our computational analogue of finite approximation. The algorithms are presented and justified in Section 4. In the final section, we report on our Magma implementation.

2. Congruence homomorphisms of finitely generated linear groups

Let ρ be a proper ideal of an (associative, unital) ring Δ. The natural surjection $\Delta \to \Delta/\rho$ induces an algebra homomorphism $\mathrm{Mat}(n,\Delta) \to \mathrm{Mat}(n,\Delta/\rho)$, which restricts to a group homomorphism $\mathrm{GL}(n,\Delta) \to \mathrm{GL}(n,\Delta/\rho)$. All these congruence homomorphisms will be denoted by ϕ_ρ. The *principal congruence subgroup* Γ_ρ is the kernel of ϕ_ρ in $\mathrm{GL}(n,\Delta)$.

We fix some more notation, used throughout. Let $S = \{g_1, \ldots, g_r\} \subseteq \mathrm{GL}(n,\mathbb{F})$, where $\mathbb{F}$ is a field. Denote $\langle S\rangle$ by G. Then $G \leqslant \mathrm{GL}(n,R)$, where $R \subseteq \mathbb{F}$ is the (Noetherian) ring generated by the entries of the matrices g_i, g_i^{-1}, $1 \leqslant i \leqslant r$. Recall that R/ρ is a finite field if ρ is a maximal ideal (see Wehrfritz, 1973, p. 50). For the purpose of studying G, we may assume without loss of generality that $\mathbb{F}$ is the field of fractions of R, and is a finitely generated extension of its prime subfield.

Each finitely generated linear group possesses a normal subgroup N of finite index whose torsion elements are all unipotent; so N is torsion-free if $\mathrm{char}\, R = 0$. A proof of this result, due to Selberg (1960) and Wehrfritz (1970), can be found in Wehrfritz (1973, 4.8, p. 56); a short new proof is supplied by Proposition 2.1 and Corollary 2.2 below. We call such a normal subgroup N of a given linear group an *SW-subgroup*. If ρ is an ideal of R such that Γ_ρ is an SW-subgroup of $\mathrm{GL}(n,R)$, then ϕ_ρ is an *SW-homomorphism*. We now formulate conditions that enable us to construct SW-homomorphisms.

Proposition 2.1. *Let Δ be a Noetherian integral domain, and ρ be a maximal ideal of Δ. If Γ_ρ has a non-trivial torsion element h, then $p := \mathrm{char}(\Delta/\rho) > 0$ and $|h|$ is a power of p.*

Proof. Set $|h| = q$. Since $\phi_\rho(h) = 1_n$, we have $h = 1_n + b$ where $b \in \mathrm{Mat}(n,\rho)$, $b \neq 0_n$. Hence $(1_n + b)^q = 1_n$, so that

$$qb + \binom{q}{2} b^2 + \cdots + b^q = 0_n. \qquad (\dagger)$$

For $k \geqslant 2$, denote the (i, j)th entry of b^k by $b_{ij}^{(k)}$; then $b_{ij}^{(k)} \in \rho^k$. By the Krull Intersection Theorem (Isaacs, 1993, 27.8, p. 437), $\bigcap_{k=1}^{\infty} \rho^k = \{0\}$. Hence there exists a positive integer c such that $b_{ij} \in \rho^c$ for all i, j, but $b_{rs} \notin \rho^{c+1}$ for some r, s. This implies that $b_{ij}^{(k)} \in \rho^{kc}$. Now

$$qb_{rs} + \binom{q}{2} b_{rs}^{(2)} + \cdots + b_{rs}^{(q)} = 0$$

by (†), so $qb_{rs} \in \rho^{2c} \subseteq \rho^{c+1}$.

Suppose that $q \notin \rho$. Since Δ/ρ is a field, there exist $x \in \Delta$ and $y \in \rho$ such that $1 = qx + y$. Then

$$b_{rs} = qb_{rs}x + b_{rs}y$$

and so, because $b_{rs} \in \rho^c$ and $qb_{rs} \in \rho^{c+1}$, we get $b_{rs} \in \rho^{c+1}$. This contradiction proves that $q \in \rho$. Thus q must be a power of p. For if not, we could have begun with h of prime order different to p, and then ρ would contain two different prime integers and so would contain 1. □

Corollary 2.2. *Let ρ, ρ_1, and ρ_2 be maximal ideals of the Noetherian integral domain Δ.*

(i) *If* $\operatorname{char}(\Delta/\rho) = 0$ *then Γ_ρ is torsion-free.*
(ii) *Suppose that* $\operatorname{char}\Delta = 0$, *and* $\operatorname{char}(\Delta/\rho_1) \neq \operatorname{char}(\Delta/\rho_2)$. *Then $\Gamma_{\rho_1} \cap \Gamma_{\rho_2}$ is a torsion-free subgroup of* $\mathrm{GL}(n, \Delta)$. *In particular, if $\Delta = R$ then $\Gamma_{\rho_1} \cap \Gamma_{\rho_2}$ is an SW-subgroup of* $\mathrm{GL}(n, R)$.
(iii) *Suppose that* $\operatorname{char}\Delta = p > 0$. *Then each torsion element of Γ_ρ is unipotent. In particular, if $\Delta = R$ then Γ_ρ is an SW-subgroup of* $\mathrm{GL}(n, R)$.

Proof. Clear from Proposition 2.1. □

Note that parts (i) and (ii) of Corollary 2.2 contribute to a solution of the problem posed on p. 70 of Suprunenko (1976).

By Corollary 2.2(ii), if $\operatorname{char} R = 0$ then an SW-subgroup can be constructed as the intersection of two congruence subgroups. Since this may not be convenient, we mention one more result.

Proposition 2.3. *Suppose that Δ is a Dedekind domain of characteristic zero, and ρ is a maximal ideal of Δ such that* $\operatorname{char}(\Delta/\rho) = p > 2$. *If $p \notin \rho^2$ then Γ_ρ is torsion-free.*

Proof. See Suprunenko (1976, Theorem 4, p. 70). □

3. Construction of SW-homomorphisms

We now outline methods to construct both congruence homomorphisms and SW-homomorphisms, given the assumptions on $\mathbb{F}$ made in the second paragraph of Section 2.

Since $\mathbb{F}$ is a finitely generated extension of its prime subfield, there is a subfield $\mathbb{P} \subseteq \mathbb{F}$ of finite degree over the prime subfield, and elements $x_1, \ldots, x_m$ $(m \geqslant 0)$ algebraically independent over $\mathbb{P}$, such that $\mathbb{F}$ is a finite extension of $\mathbb{L} = \mathbb{P}(x_1, \ldots, x_m)$; say $|\mathbb{F} : \mathbb{L}| = e \geqslant 1$. Here $|\mathbb{P} : \mathbb{Q}| = k \geqslant 1$ if $\operatorname{char}\mathbb{F} = 0$, and if $\operatorname{char}\mathbb{F} = p > 0$ then $\mathbb{P}$ is the field $\mathbb{F}_q$ of size q.

Each type of field is considered in its own section below. For an integral domain Δ and $\mu \in \Delta \setminus \{0\}$, let $\frac{1}{\mu}\Delta$ denote the ring of fractions with denominators in the multiplicative submonoid of Δ generated by μ.

3.1. The rational field

Let $\mathbb{F} = \mathbb{Q}$. Then $R = \frac{1}{\mu}\mathbb{Z}$ where μ is the least common multiple of the denominators of the entries in the matrices g_i, g_i^{-1}, $1 \leqslant i \leqslant r$. For a prime $p \in \mathbb{Z}$ not dividing μ, define $\phi_1 = \phi_{1,p} : \mathrm{GL}(n, R) \to \mathrm{GL}(n, p)$ to be entry-wise reduction modulo p. If $p > 2$ then we denote $\phi_{1,p}$ by $\Phi_1 = \Phi_{1,p}$. By Proposition 2.3, Φ_1 is an SW-homomorphism.

3.2. Number fields

Let $\mathbb{F}$ be a number field, so that $\mathbb{F} = \mathbb{Q}(\alpha)$ for some algebraic number α. Let $f(t)$ be the minimal polynomial of α, of degree k. Multiplying α by a common multiple of the denominators of the coefficients of $f(t)$, if necessary, we may assume that α is an algebraic integer; that is, $f(t) \in \mathbb{Z}[t]$.

We have $R \subseteq \frac{1}{\mu}\mathbb{Z}[\alpha] \subseteq \frac{1}{\mu}\mathcal{O}$ for some $\mu \in \mathbb{Z}$, where $\mathcal{O}$ is the ring of integers of $\mathbb{F}$. We define an SW-homomorphism on R as the restriction of a congruence homomorphism on the Dedekind domain $\frac{1}{\mu}\mathcal{O}$.

Let $p \in \mathbb{Z}$ be a prime not dividing μ, and denote by $\bar{f}(t)$ the polynomial obtained by mod p reduction of the coefficients of $f(t)$. Further, let $\bar{\alpha}$ be a root of $\bar{f}(t)$, so that $\bar{\alpha}$ is a root of some $\mathbb{Z}_p$-irreducible factor $\bar{f}_j(t)$ of $\bar{f}(t)$. Each $b \in R$ may be expressed uniquely in the form $b = \sum_{i=0}^{k-1} c_i \alpha^i$ where $c_i \in \frac{1}{\mu}\mathbb{Z}$. Thus the assignment $\phi_{2,p} : b \mapsto \sum_{i=0}^{k-1} \phi_{1,p}(c_i)\bar{\alpha}^i$ is well-defined. Moreover, $\phi_{2,p}$ is a ring homomorphism $R \to \mathbb{Z}_p(\bar{\alpha}) = \mathbb{F}_{p^l}$, say. Thus we have an induced congruence homomorphism $\phi_{2,p} : \mathrm{GL}(n, R) \to \mathrm{GL}(n, p^l)$.

Next, we state criteria under which $\phi_2 = \phi_{2,p}$ is an SW-homomorphism.

Lemma 3.1. *Suppose that $p \in \mathbb{Z}$ is an odd prime dividing neither μ nor the discriminant of $f(t)$. Then the kernel of $\phi_{2,p}$ on $\mathrm{GL}(n, R)$ is torsion-free.*

Proof. Let $f_j(t)$ be a preimage of $\bar{f}_j(t)$ in $\mathbb{Z}[t]$. The ideal ρ generated by p and $f_j(\alpha)$ in $\frac{1}{\mu}\mathcal{O}$ is maximal, by Koch (2000, Theorem 3.8.2). Hence $\rho \cap R$ is a maximal ideal of R. Also $p \notin \rho^2$ by Koch (2000, Proposition 3.8.1, Theorem 3.8.2). The lemma then follows from Proposition 2.3. □

Lemma 3.2. *There are no non-trivial p-subgroups of $\mathrm{GL}(n, \mathbb{F})$ if $p > nk + 1$.*

Proof. Let $g \in \mathrm{GL}(n, \mathbb{Q})$ be of order p. Since the characteristic polynomial of g has a primitive pth root of unity as a root, it is divisible by the pth cyclotomic polynomial. Thus $p - 1 \leqslant n$. The general claim holds because each subgroup of $\mathrm{GL}(n, \mathbb{F})$ is isomorphic to a subgroup of $\mathrm{GL}(nk, \mathbb{Q})$. □

Corollary 3.3. *Suppose that Δ is a Noetherian subring of $\mathbb{F}$, and ρ is a maximal ideal of Δ such that $\mathrm{char}(\Delta/\rho) = p > nk + 1$. Then Γ_ρ is torsion-free.*

Proof. This is a consequence of Proposition 2.1 and Lemma 3.2. □

Let $p \in \mathbb{Z}$ be a prime not dividing μ. We denote $\phi_{2,p}$ by $\Phi_2 = \Phi_{2,p}$ if one of the following extra conditions on p is satisfied: p is odd and does not divide the discriminant of the minimal polynomial of α; or $p > nk + 1$. The preceding discussion shows that Φ_2 is an SW-homomorphism.

Example 3.4. Suppose that $\mathbb{F}$ is a cyclotomic field, say $\mathbb{F} = \mathbb{Q}(\zeta)$ where ζ is a primitive cth root of unity, $c > 2$. If $p > 2$ and p does not divide $\mathrm{lcm}(\mu, c)$, then $\phi_{2,p}$ is an SW-homomorphism by Lemma 3.1.

3.3. Function fields

Let $\mathbb{F} = \mathbb{P}(x_1, \ldots, x_m)$, $m \geqslant 1$, where $\mathbb{P}$ is $\mathbb{Q}$, a number field, or $\mathbb{F}_q$. We have $R \subseteq \frac{1}{\mu}\mathbb{P}[x_1, \ldots, x_m]$ for some $\mu = \mu(x_1, \ldots, x_m)$ determined by $S \cup S^{-1}$.

Let $a = (a_1, \ldots, a_m)$ be a non-root of μ. If $\mathrm{char}\,\mathbb{F} = 0$, then $a_i \in \mathbb{P}$ for all i; if $\mathbb{F}$ has positive characteristic, then the a_i are in $\mathbb{P}$ or some finite extension. Define $\phi_3 = \phi_{3,a}$ to be the map that substitutes a_i for x_i, $1 \leqslant i \leqslant m$. Corollary 2.2(i) implies that $\phi_3 : \mathrm{GL}(n, R) \to \mathrm{GL}(n, \mathbb{P})$ is a homomorphism with torsion-free kernel if $\mathrm{char}\,\mathbb{F} = 0$. We then obtain an SW-homomorphism in zero characteristic by setting $\Phi_3 = \Phi_{3,a,p} = \Phi_{i,p} \circ \phi_{3,a}$, where $i = 1$ or 2 if $\mathbb{P} = \mathbb{Q}$ or $\mathbb{P}$ is a number field, respectively. If $\mathbb{P} = \mathbb{F}_q$

then $\Phi_3 = \phi_3$ is an SW-homomorphism by Corollary 2.2(iii). Notice that $\Phi_{3,a,p}$ is defined for all but a finite number of a and p when $m = 1$; otherwise, $\Phi_{3,a,p}$ is defined for infinitely many a and p.

3.4. Algebraic function fields

For $m \geqslant 1$, let $\mathbb{L} = \mathbb{P}(x_1, \ldots, x_m)$ and $\mathbb{L}_0 = \mathbb{P}[x_1, \ldots, x_m]$, where again $\mathbb{P}$ is $\mathbb{Q}$, a number field, or $\mathbb{F}_q$. We assume that $\mathbb{F} = \mathbb{L}(\alpha)$ is a simple extension of $\mathbb{L}$ of degree $e > 1$. For instance, we can stipulate that $\mathbb{F}$ is a separable extension of $\mathbb{L}$ (e.g., in characteristic p this is assured if $p \nmid e$). Let $f(t) \in \mathbb{L}_0[t]$ be the minimal polynomial of α. We have $R \subseteq \frac{1}{\mu}\mathbb{L}_0[\alpha]$ for some $\mu \in \mathbb{L}_0$ determined in the usual way by the input S.

Suppose that $a = (a_1, \ldots, a_m)$ is a non-root of μ, where the a_i are in $\mathbb{P}$ or a finite extension. Denote by $\bar{f}(t)$ the polynomial obtained by substitution of a in the coefficients of $f(t)$. Define $\bar{c} = \phi_{3,a}(c)$ for $c \in \frac{1}{\mu}\mathbb{L}_0$ similarly. Let $\bar{\alpha}$ be a root of $\bar{f}(t)$. Define $\phi_4 = \phi_{4,a} : R \to \mathbb{P}(\bar{\alpha})$ by $\phi_4 : \sum_{i=0}^{e-1} c_i\alpha^i \mapsto \sum_{i=0}^{e-1} \bar{c}_i\bar{\alpha}^i$. Therefore, if $\operatorname{char}\mathbb{F} = 0$ then we get an induced congruence homomorphism $\phi_4 : \mathrm{GL}(n, R) \to \mathrm{GL}(n, \mathbb{P}(\bar{\alpha}))$, whose kernel is torsion-free by Corollary 2.2(i). Set $\Phi_4 = \Phi_{4,a,p} = \Phi_{i,p} \circ \phi_{4,a}$, where $i = 1$ if $\mathbb{P}(\bar{\alpha}) = \mathbb{Q}$, and $i = 2$ if $\mathbb{P}(\bar{\alpha})$ is a number field. If $\operatorname{char}\mathbb{F} > 0$ then we set $\Phi_4 = \phi_4$. In all cases Φ_4 is an SW-homomorphism. As with $\Phi_{3,a,p}$, the homomorphism $\Phi_{4,a,p}$ is defined for infinitely many a and p, and for all but a finite number of a, p when $m = 1$.

Remark 3.5. Fields $\mathbb{F}$ as in Sections 3.1–3.4 are the main ones supported by GAP and Magma.

Remark 3.6. SW-homomorphisms are used in Detinko et al. (2011b, Section 5.3) to test whether $G \leqslant \mathrm{GL}(n, \mathbb{F})$ is central-by-finite; indeed, each 'W-homomorphism' defined in that paper is a special kind of SW-homomorphism. They also feature in the nilpotency testing algorithm of Detinko and Flannery (2008).

3.5. Analyzing congruence homomorphisms

We now prove some results that will be helpful in the analysis of our algorithms.

Lemma 3.7. *Let Δ be a Dedekind domain, and let G be a finitely generated subgroup of $\mathrm{GL}(n, \Delta)$. For all but a finite number of maximal ideals ρ of Δ, the following are true*:

(i) *if G is finite then ϕ_ρ is an isomorphism of G onto $\phi_\rho(G)$*;
(ii) *if G is infinite, and ν is a positive integer, then $\phi_\rho(G)$ contains an element of order greater than ν.*

Proof. (Cf. Wehrfritz, 1973, p. 51 and Detinko and Flannery, 2009, Lemma 3.) Note that a non-zero element a of Δ is contained in only finitely many maximal ideals of Δ. To see this, let $a\Delta = \rho_1^{e_1} \cdots \rho_c^{e_c}$, where the ρ_i are maximal ideals. If ρ is a maximal ideal of Δ containing a, then $\rho_1^{e_1} \cdots \rho_c^{e_c} \subseteq \rho$, so $\rho = \rho_i$ for some i.

Next, let $M = \{h_1, \ldots, h_d\} \subseteq \mathrm{Mat}(n, \Delta)$, and for each pair $l, k \in \{1, \ldots, d\}$, $l \neq k$, choose (i, j) such that $h_l(i, j) - h_k(i, j) \neq 0$. Denote the product of all differences $h_l(i, j) - h_k(i, j)$ by a_M. If ρ is an ideal of Δ not containing a_M, then $|\phi_\rho(M)| = |M|$.

Taking M to be the set of elements of G, part (i) is now clear.

If G is infinite then G contains an element g of infinite order, by a result of Schur (Suprunenko, 1976, Theorem 5, p. 181). Thus, taking M to be $\{g, \ldots, g^\nu, g^{\nu+1}\}$, we get (ii). □

To utilize Lemma 3.7 in our context, let $\mathbb{F}$ be one of $\mathbb{Q}$, a number field, $\mathbb{P}(x)$, or a finite extension of $\mathbb{P}(x)$. The relevant SW-homomorphism Φ on $\mathrm{GL}(n, R)$ is the restriction of a congruence homomorphism ϕ_ρ on $\mathrm{GL}(n, \Delta)$, where Δ is a Dedekind domain with maximal ideal ρ. Hence for $G \leqslant \mathrm{GL}(n, R)$ and all but a finite number of choices in the definition of ϕ_ρ, the following hold: (a) if G is finite, then Φ is an isomorphism on G; (b) if G is infinite, then $\Phi(G)$ contains an element of order greater

than any given positive integer ν. For the other fields $\mathbb{F}$ where R may not be contained in a Dedekind domain (function fields with more than one indeterminate or finite extensions thereof), it is still true that there are infinitely many SW-homomorphisms Φ such that (a) and (b) hold. This follows from the definition of Φ in each case, and arguing as in the proof of Lemma 3.7.

4. Finiteness algorithms for matrix groups

4.1. Preliminaries: asymptotic bounds

We continue with the notation of the previous section: $|\mathbb{F}:\mathbb{L}| = e \geqslant 1$, $\mathbb{L} = \mathbb{P}(x_1, \ldots, x_m)$, $m \geqslant 0$, and $|\mathbb{P}:\mathbb{Q}| = k \geqslant 1$ or $\mathbb{P} = \mathbb{F}_q$.

Suppose first that $\operatorname{char}\mathbb{F} = 0$. Put $n_0 = nke$.

Lemma 4.1. *A finite subgroup G of $\mathrm{GL}(n, \mathbb{F})$ is isomorphic to a subgroup of $\mathrm{GL}(n_0, \mathbb{Q})$.*

Proof. Certainly G is isomorphic to a subgroup of $\mathrm{GL}(ne, \mathbb{L})$, and a subgroup of $\mathrm{GL}(ne, \mathbb{P})$ is isomorphic to a subgroup of $\mathrm{GL}(nke, \mathbb{Q})$. The lemma follows from Suprunenko (1976, p. 69, Corollary 4). □

It is well-known that the order of a finite subgroup of $\mathrm{GL}(n, \mathbb{Q})$ is bounded by a function of n (see, e.g., Feit, 1995; Friedland, 1997). Hence by Lemma 4.1 there are functions $\nu_1 = \nu_1(n_0)$ and $\nu_2 = \nu_2(n_0)$ bounding the order of a finite subgroup of $\mathrm{GL}(n, \mathbb{F})$ and the order of a torsion element of $\mathrm{GL}(n, \mathbb{F})$, respectively. For $n_0 > 10$ or $n_0 = 3, 5$ we may take $\nu_1 = 2^{n_0}(n_0)!$ by Feit (1995, Theorem A); for the remaining n_0, values of ν_1 are also listed there. A suitable function ν_2 is given by the next lemma.

Lemma 4.2. *If g is a torsion element of $\mathrm{GL}(n, \mathbb{F})$, then $|g| \leqslant 2^{s+1}3^{\lfloor n_0/2 \rfloor}$ where 2^s is the largest power of 2 dividing n_0.*

Proof. Let $\mathbb{F} = \mathbb{Q}$. If $|g|$ is odd then $|g| \leqslant 3^{\lfloor n/2 \rfloor}$ by Friedland (1997, p. 3519). Suppose that g is a 2-element. Then g is conjugate to a monomial matrix over $\mathbb{Q}$ (see Leedham-Green and Plesken, 1986, IV.4). Since the order of a 2-element in $\mathrm{Sym}(n)$ is bounded by the largest power 2^t of 2 dividing n, $|g| \leqslant 2^{t+1}$. Lemma 4.1 now implies the result in the general case $\mathbb{F} \supseteq \mathbb{Q}$. □

Here is one more useful condition to detect infinite groups in characteristic zero.

Lemma 4.3. *If $G \leqslant \mathrm{GL}(n, \mathbb{F})$ is finite and $p > n_0 + 1$ then $p \nmid |G|$.*

Proof. This follows from Lemmas 3.2 and 4.1. □

Now suppose that $\operatorname{char}\mathbb{F} > 0$. The order of a finite subgroup of $\mathrm{GL}(n, \mathbb{F})$ can be arbitrarily large. On the other hand, the orders of torsion elements of $\mathrm{GL}(n, \mathbb{F})$ are bounded. The next lemma furnishes such a bound.

Lemma 4.4. *Let $n_0 = ne$. If g is a torsion element of $\mathrm{GL}(n, \mathbb{F})$ then $|g| \leqslant q^{n_0} - 1$.*

Proof. The proof is essentially the same as that of Rockmore et al. (1999, Theorem 3.3, Corollary 3.4). We recap the main points. It suffices to assume that $\mathbb{F} = \mathbb{L}$. By Zalesskii (1966), g is conjugate to a block upper triangular matrix, where the (irreducible) blocks are $\mathbb{F}_q$-matrices. Hence the characteristic polynomial of g has $\mathbb{F}_q$-coefficients. It follows that the dimension of $\langle g \rangle_{\mathbb{F}_q}$ is at most n, and so every invertible element of this enveloping algebra has order at most $q^n - 1$. □

4.2. Testing finiteness

Using Section 3, we can construct a congruence image $\phi_\rho(G)$ of $G \leqslant \mathrm{GL}(n, \mathbb{F})$ over a finite field such that the torsion elements of $G_\rho := G \cap \Gamma_\rho$ are unipotent. Thus, to decide finiteness of G, we merely test whether G_ρ is trivial ($\mathrm{char}\,\mathbb{F} = 0$), or whether G_ρ is unipotent ($\mathrm{char}\,\mathbb{F} > 0$). Both tasks can be accomplished using only *normal generators* of G_ρ: generators for a subgroup whose normal closure in G is G_ρ—that is, we do not need to construct the full congruence subgroup. Normal generators are found by a standard method (Holt et al., 2005, pp. 299–300) that requires a presentation of $\phi_\rho(G)$ as input. Since it is a matrix group over a finite field, we can compute a presentation of $\phi_\rho(G)$ using the algorithms described in Bäärnhielm et al. (2011), O'Brien (2011). We refer to such an algorithm as `Presentation`. Let `SWImage` be an algorithm that constructs a congruence image over a finite field. The congruence homomorphism in question is one of the SW-homomorphisms $\Phi = \Phi_i$, $1 \leqslant i \leqslant 4$, defined in Sections 3.1–3.4. The following procedure tests finiteness along the lines just explained (see Section 4.1 for definitions of n_0 and ν_1).

`IsFiniteMatrixGroup`

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

(1) $H := \mathtt{SWImage}(G) = \langle \Phi(g_1), \ldots, \Phi(g_r) \rangle$.
(2) If $\mathrm{char}\,\mathbb{F} = 0$ and either $|H| > \nu_1$ or p divides $|H|$ for some prime $p > n_0 + 1$, then return `false`.
(3) $\mathtt{Presentation}(H) := \langle \Phi(g_1), \ldots, \Phi(g_r) \mid w_j(\Phi(g_1), \ldots, \Phi(g_r)) = 1; 1 \leqslant j \leqslant t \rangle$.
(4) $K := \{w_j(g_1, \ldots, g_r) \mid 1 \leqslant j \leqslant t\}$.
(5) If $\mathrm{char}\,\mathbb{F} = 0$ and $K = \{1_n\}$, or $\mathrm{char}\,\mathbb{F} > 0$ and $\mathtt{IsUnipotent}(\langle K \rangle^G)$, then return `true`. Else return `false`.

Step (2) is justified by Lemma 4.3 and the comments before Lemma 4.2. For example, if $\mathbb{F}$ is a number field then Lemma 3.7 suggests that the initial check in this step will usually identify that G is infinite. We test unipotency of the congruence subgroup $\langle K \rangle^G$ in step (5) using the normal generating set K. A procedure for doing this, based on computation in enveloping algebras, is given in Detinko et al. (2011b, Section 5.2). Also note that we can apply a conjugation isomorphism as in Glasby and Howlett (1997) to write the SW-image over the smallest possible finite field of the chosen characteristic.

Next we consider the special but very important case that G is a cyclic group: testing whether $g \in \mathrm{GL}(n, \mathbb{F})$ has finite order. Let ν_2 be an upper bound on the order of a torsion element of $\mathrm{GL}(n, \mathbb{F})$. See Lemmas 4.2 and 4.4 for values of ν_2.

`IsFiniteCyclicMatrixGroup`

Input: $g \in \mathrm{GL}(n, \mathbb{F})$.
Output: `true` if g has finite order; `false` otherwise.

(1) $h := \mathtt{SWImage}(g)$.
(2) $d := \mathtt{Order}(h)$.
(3) If $d > \nu_2$, or $\mathrm{char}\,\mathbb{F} = 0$ and $p \mid d$ for some prime $p > n_0 + 1$, then return `false`.
(4) If $\mathrm{char}\,\mathbb{F} = 0$ and $g^d = 1_n$, or $\mathrm{char}\,\mathbb{F} > 0$ and $\mathtt{IsUnipotent}(g^d)$, then return `true`. Else return `false`.

Note that g^d is unipotent in characteristic $p > 0$ if and only if its order divides $p^{\lceil \log_p n \rceil}$ (see Suprunenko, 1976, p. 192). Also, if $\mathrm{char}\,\mathbb{F} = 0$ and `IsFiniteCyclicMatrixGroup` returns `true`, then the order d of g is calculated in step (2). In the situations covered by Lemma 3.7, if $|g|$ is infinite then $d > \nu_2$ for all but a finite number of choices of Φ. That is, we expect that infiniteness of $|g|$ will be detected at step (3) of `IsFiniteCyclicMatrixGroup`.

Recall that an infinite group $G \leqslant \mathrm{GL}(n, \mathbb{F})$ has an infinite order element. Hence, as a precursor to running `IsFiniteMatrixGroup`, we check via `IsFiniteCyclicMatrixGroup` whether 'random' elements of G, produced by a variation of the product replacement algorithm (Celler et al., 1995), have infinite order; cf. Babai et al. (1993, Section 8.2).

4.3. Recognizing finite matrix groups

Suppose that $G \leqslant \mathrm{GL}(n, \mathbb{F})$ is finite. We describe how to find an isomorphic copy of G in some $\mathrm{GL}(n, q)$ and carry out further computations with G.

If $\mathrm{char}\,\mathbb{F} = 0$ then $\mathtt{SWImage}(G) = \Phi(G)$ is isomorphic to G. If $\mathrm{char}\,\mathbb{F} > 0$ then the congruence subgroup may be non-trivial. We repeat the construction of normal generators of the congruence subgroup for different choices of Φ, until we find a Φ for which all these generators are trivial. By the discussion at the end of Section 3.5, if $m = 1$ (there is just one indeterminate) then in a finite number of iterations we will get an isomorphic copy of G by Lemma 3.7. Otherwise, there are infinitely many isomorphisms Φ, and the procedure will terminate if the set of maximal ideals is recursively enumerable. In our many experiments the procedure always succeeded in finding an isomorphic copy of G.

Once we have an isomorphic copy, algorithms for matrix groups over finite fields (see Bäärnhielm et al., 2011 and Holt et al., 2005, Chapter 10) are used to investigate the structure and properties of G. In particular, we can

- compute a composition series and short presentation for G;
- compute $|G|$;
- compute the solvable and unipotent radicals, the derived subgroup, center, and Sylow subgroups of G;
- test membership of $x \in \mathrm{GL}(n, \mathbb{F})$ in G.

Where feasible, the computation is undertaken directly in the isomorphic copy, and the result is 'lifted' by means of the known isomorphism to G. Sometimes this involves additional work. For instance, membership testing requires that we construct a new isomorphic copy; namely, of $\langle G, x\rangle$.

5. Implementation and performance

The algorithms have been implemented in Magma as part of our package Infinite (Detinko et al., 2011a). We use machinery from the CompositionTree package (Bäärnhielm et al., 2011; O'Brien, 2011) to study congruence images and construct their presentations.

We implemented SW-homomorphisms in full, as per Sections 3.1–3.4. When selecting a prime p subject to various conditions (see Sections 3.1 and 3.2), our default choice is the smallest valid one. In Sections 3.3 and 3.4 we need to find a non-root a of a collection of polynomials $\{f_1, \ldots, f_s\} \subseteq \mathbb{P}[X_1, \ldots, X_m]$. For example, if $\mathbb{P} = \mathbb{F}_q$ then we could choose $a = (a_1, \ldots, a_1)$ where $a_1 \in \mathbb{F}_{q^l}$, $l > \max_j \deg(f_j)$, and a_1 does not lie in a proper subfield of $\mathbb{F}_{q^l}$. To avoid working with potentially large field extensions, we instead generate random m-tuples of elements of (increasing extensions of) $\mathbb{F}_q$ to obtain a. A similar strategy of generating random m-tuples is employed in characteristic 0.

The SW-homomorphisms are applied in Infinite to solve specific problems, such as testing finiteness, virtual properties, and nilpotency (the latter over an arbitrary field, significantly enhancing Detinko and Flannery, 2008). Here we report on the algorithms of Sections 4.2 and 4.3.

In our implementation of `IsFiniteMatrixGroup` and `IsFiniteCyclicMatrixGroup`, we construct (at least) two SW-homomorphisms and determine the orders of the images of G under these. If G is finite and $\mathrm{char}\,\mathbb{F} = 0$, then the orders must be identical. In positive characteristic, the least common multiple of the orders of two images of an element of finite G must be at most ν_2. The single most expensive task is evaluating relations to obtain normal generators for the kernel of an SW-homomorphism, since this may lead to blow-up in the size of matrix entries. Hence we first check the orders of images under several SW-homomorphisms before we evaluate relations.

In Detinko et al. (2009) we proposed an alternative algorithm to decide finiteness for groups defined over function fields of positive characteristic. This is an option in INFINITE; it avoids evaluation of relations over the field of definition, and is sometimes faster than `IsFiniteMatrixGroup` for such groups.

We now describe sample outputs that illustrate the efficiency and scope of our implementation. The examples chosen cover the main domains and a variety of groups. Our experiments were performed using MAGMA V2.17-2 on a 2GHz machine. All examples are randomly conjugated, so that generators are not sparse, and matrix entries (numerators and denominators) are large. Since random selection plays a role in some of the COMPOSITIONTREE algorithms, times stated are averages over three runs. The complete examples are available in the INFINITE package.

(1) $G_1 \leqslant \mathrm{GL}(24, \mathbb{Q}(\zeta_{17}))$ is a conjugate of the monomial group $\langle \zeta_{17} \rangle \wr \mathrm{Sym}(24)$. It has order $17^{24}24!$, the maximum possible for a finite subgroup of $\mathrm{GL}(24, \mathbb{Q}(\zeta_{17}))$ by Feit (1995). We decide finiteness of this 3-generator group and determine its order in 1435s; compute a Sylow 3-subgroup in 22s; and the derived group in 57s.
(2) $G_2 \leqslant \mathrm{GL}(12, \mathbb{F})$ where $\mathbb{F} = \mathbb{P}(x)$ and $\mathbb{P} = \mathbb{Q}(\sqrt{2})$. It is conjugate to $H_1 \wr H_2$ where H_1 is `RationalMatrixGroup`$(4, 2)$ and $H_2 =$ `PrimitiveSubgroup`$(3, 1)$, both from standard MAGMA databases. We decide finiteness of this 7-generator group in 18s; compute its order $2^{16}3^7$ in 1435s; its center in 3s; and its Fitting subgroup in 3s.
(3) $G_3 \leqslant \mathrm{GL}(20, \mathbb{F})$ where $\mathbb{F}$ is a degree 2 extension of the function field $\mathbb{Q}(x)$. It is conjugate to the derived subgroup of the monomial group $\langle -1 \rangle \wr \mathrm{Sym}(20)$ in $\mathrm{GL}(20, \mathbb{F})$. We decide finiteness and compute the order of this 31-generator group in 1090s; and construct a Sylow 7-subgroup in 5s.
(4) $G_4 \leqslant \mathrm{GL}(100, \mathbb{Q}(\zeta_{19}))$. We prove that this 14-generator group is infinite in 9s.
(5) $G_5 \leqslant \mathrm{GL}(30, \mathbb{F})$ where $\mathbb{F}$ is an algebraic function field of degree 3 over $\mathbb{Q}(x)$. We prove that this 4-generator group is infinite in 1024s.
(6) $G_6 \leqslant \mathrm{GL}(6, \mathbb{F})$ where $\mathbb{F}$ is an algebraic function field of degree 2 over $\mathbb{F}_9(x)$. It is conjugate to $\mathrm{GL}(6, 3^2)$. We find the order of this 2-generator group in 18s; its unipotent radical in 15s; a Sylow 3-subgroup H in 18s; and compute the normalizer in G_6 of H in 42s.
(7) $G_7 \leqslant \mathrm{GL}(16, \mathbb{F})$ where $\mathbb{F}$ is a degree 3 extension of $\mathbb{F}_2(x)$. It is conjugate to the Kronecker product of $\mathrm{GL}(8, 2)$ with a unipotent subgroup of $\mathrm{GL}(2, \mathbb{F}_2(x))$. We decide finiteness of this 8-generator group in 16s; we compute its order $16 \cdot |\mathrm{GL}(8, 2)|$ and an isomorphic copy in 488s; and determine the Fitting subgroup in 12s.
(8) $G_8 \leqslant \mathrm{GL}(12, \mathbb{F})$ where $\mathbb{F}$ is a function field with two indeterminates over $\mathbb{F}_5$. We prove that this 8-generator group is infinite in 6s.
(9) $G_9 \leqslant \mathrm{GL}(12, \mathbb{F})$ where $\mathbb{F}$ is a degree 2 extension of a univariate function field over $\mathbb{F}_5$. We prove that this 8-generator group is infinite in 10s.

References

Bäärnhielm, H., Holt, D.F., Leedham-Green, C.R., O'Brien, E.A., 2011. A practical model for computation with matrix groups. Preprint.

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

Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I. The user language. J. Symbolic Comput. 24 (3–4), 235–265.

Celler, F., Leedham-Green, C.R., Murray, S.H., Niemeyer, A.C., O'Brien, E.A., 1995. Generating random elements of a finite group. Comm. Algebra 23, 4931–4948.

Detinko, A.S., 2001. On deciding finiteness for matrix groups over fields of positive characteristic. LMS J. Comput. Math. 4, 64–72 (electronic).

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

Detinko, A.S., Flannery, D.L., 2008. Algorithms for computing with nilpotent matrix groups over infinite domains. J. Symbolic Comput. 43, 8–26.

Detinko, A.S., Flannery, D.L., 2009. On deciding finiteness of matrix groups. J. Symbolic Comput. 44, 1037–1043.

Detinko, A.S., Flannery, D.L., O'Brien, E.A., 2009. Deciding finiteness of matrix groups in positive characteristic. J. Algebra 322, 4151–4160.

Detinko, A.S., Flannery, D.L., O'Brien, E.A., 2011a. http://magma.maths.usyd.edu.au/magma/handbook/text/617.

Detinko, A.S., Flannery, D.L., O'Brien, E.A., 2011b. Algorithms for the Tits alternative and related problems. J. Algebra 344, 397–406.
Feit, W., 1995. The orders of finite linear groups. Preprint.
Friedland, S., 1997. The maximal orders of finite subgroups in $GL_n(\mathbb{Q})$. Proc. Amer. Math. Soc. 125, 3519–3526.
The GAP Group, 2012. GAP – Groups, Algorithms, and Programming, Version 4.5.4. http://www.gap-system.org.
Glasby, S.P., Howlett, R.B., 1997. Writing representations over minimal fields. Comm. Algebra 25 (6), 1703–1711.
Holt, D.F., Eick, B., O'Brien, E.A., 2005. Handbook of Computational Group Theory. Chapman and Hall/CRC, London.
Isaacs, I. Martin, 1993. Algebra: a Graduate Course, 1st ed. Brooks Cole, Pacific Grove, CA.
Ivanyos, G., 2001. Deciding finiteness for matrix semigroups over function fields over finite fields. Israel J. Math. 124, 185–188.
Koch, H., 2000. Number Theory. Algebraic Numbers and Functions. Grad. Stud. Math., vol. 24. American Mathematical Society, Providence, RI.
Leedham-Green, C.R., Plesken, W., 1986. Some remarks on Sylow subgroups of general linear groups. Math. Z. 191, 529–535.
O'Brien, E.A., 2011. Algorithms for matrix groups. London Math. Soc. Lecture Note Ser. 388, 297–323.
Rockmore, D.N., Tan, K.-S., Beals, R., 1999. Deciding finiteness for matrix groups over function fields. Israel J. Math. 109, 93–116.
Suprunenko, D.A., 1976. Matrix Groups. Transl. Math. Monogr., vol. 45. American Mathematical Society, Providence, RI.
Wehrfritz, B.A.F., 1973. Infinite Linear Groups. Springer-Verlag, New York.
Zalesskii, A.E., 1966. Maximal periodic subgroups of the full linear group over a field with positive characteristic. Vesci Akad. Navuk BSSR Ser. Fiz.-Mat. Navuk 1966 (2), 121–123 (in Russian).
Zalesskii, A.E., 1993. Linear groups. In: Algebra IV. In: Encyclopaedia Math. Sci., vol. 37. Springer, Berlin.