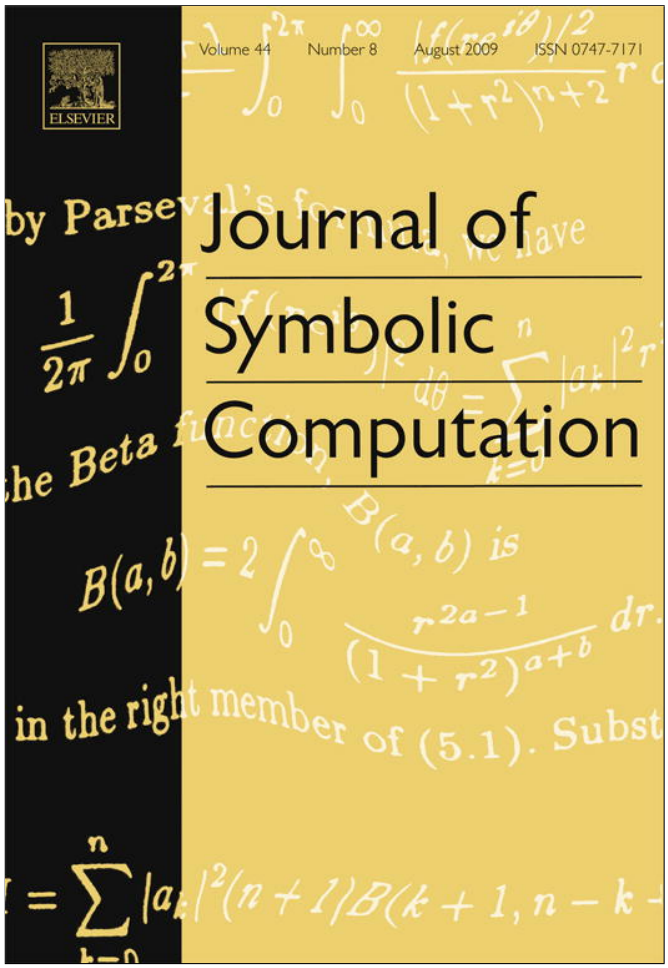

Journal of Symbolic Computation 44 (2009) 1037–1043

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

On deciding finiteness of matrix groups☆

A.S. Detinko, D.L. Flannery [1]

School of Mathematics, Statistics and Applied Mathematics, National University of Ireland, Galway, Ireland

ARTICLE INFO

Article history:
Received 29 June 2008
Accepted 16 February 2009
Available online 27 February 2009

Keywords:
Matrix group
Function field
Finiteness problem
Algorithm

ABSTRACT

We provide a new, practical algorithm for deciding finiteness of matrix groups over function fields of zero characteristic. The algorithm has been implemented in GAP. Experimental results and extensions of the algorithm to any field of zero characteristic are discussed.

1. Introduction

In any class of potentially infinite groups, deciding finiteness is a fundamental computational problem. For arbitrary classes of groups, finiteness may not even be decidable (see Lyndon and Schupp (2001, p. 192)). However, for matrix groups, the outlook is more optimistic. Several authors (Babai, 1992; Babai et al., 1993) have developed algorithms (both deterministic and randomized) for deciding finiteness of matrix groups over the rational field $\mathbb{Q}$. Algorithms from Babai et al. (1993) have been implemented, and finiteness testing of groups over $\mathbb{Q}$ is available in the computer algebra systems GAP (The GAP group) and MAGMA (Bosma et al., 1997). A standard reduction achieved by representing algebraic numbers as matrices over $\mathbb{Q}$ then enables finiteness testing over number fields.

Deciding finiteness of groups over function fields is considered in Detinko (2001), Ivanyos (2001), Rockmore et al. (1999). Although polynomial-time algorithms in both zero and positive characteristic were proposed, they involve a lot of computing over function fields, and so may be practicable only for small input. In particular, the ideas presented in Rockmore et al. (1999, Section 2) for zero characteristic rely on computing an enveloping algebra basis over the ground field as a first step, and then constructing a representation of the input group in possibly squared dimension. No

☆ Supported in part by Science Foundation Ireland, grant 08/RFP/MTH1331.
E-mail addresses: alla.detinko@nuigalway.ie (A.S. Detinko), dane.flannery@nuigalway.ie (D.L. Flannery).
[1] Tel.: +353 91 492332; fax: +353 91 494542.

0747-7171/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2009.02.001

implementations of the algorithms from Detinko (2001), Ivanyos (2001), Rockmore et al. (1999) are publicly available.

An essentially different technique for deciding finiteness is described in Detinko and Flannery (2008). That technique, which is based on changing the ground domain via congruence homomorphism, can be applied uniformly over any domain. It was used in Detinko and Flannery (2008) for deciding finiteness of nilpotent matrix groups. Algorithms from Detinko and Flannery (2008) have been implemented as part of the GAP package 'Nilmat' (Detinko et al., 2007). Experimental evidence points to the efficiency of the Nilmat functions `IsFiniteNilpotentMatGroup` and `SizeOfNilpotentMatGroup`, which test finiteness and compute orders of nilpotent groups over $\mathbb{Q}$ in very large degrees, where other available functions for these purposes fail. In smaller degrees where the GAP function `IsFinite` terminates successfully, `IsFiniteNilpotentMatGroup` is much faster.

This paper employs the technique of Detinko and Flannery (2008) to develop a new and practical algorithm for deciding finiteness of matrix groups over function fields of zero characteristic. As a consequence of the main algorithm, we are able to solve another basic computational problem; namely, computing the order of a finite input group (cf. O'Brien (2006, Section 2). We mention incidentally that one of our approaches to the order problem is by means of finding a faithful representation of the input group over a finite field.) Furthermore, we outline how this paper, together with Babai et al. (1993), yield a practical solution to the finiteness and order problems for matrix groups defined over any field of zero characteristic.

We have implemented our main algorithm in GAP. Section 4 contains experimental results obtained from the implementation.

Although attention is restricted in this paper to zero characteristic, our ideas also carry over to function fields of positive characteristic. However, extra difficulties arise in the latter case. Some remarks on this case are given in Section 5.

2. Deciding finiteness via congruence homomorphisms

This section sets up some theoretical preliminaries and notation used throughout the paper.

Let Δ be an integral domain and ϱ be an ideal of Δ. Denote the natural ring epimorphism $\Delta \to \Delta/\varrho$ by φ_ϱ. Recall that Δ/ϱ is an integral domain (respectively field) if and only if ϱ is prime (respectively maximal). Also, if Δ is finitely generated and ϱ is maximal, then Δ/ϱ is a finite field (see Wehrfritz (1973, 4.1, p. 50)). We get a ring homomorphism $\mathrm{Mat}(n, \Delta) \to \mathrm{Mat}(n, \Delta/\varrho)$ by entrywise extension, and then a group homomorphism $\mathrm{GL}(n, \Delta) \to \mathrm{GL}(n, \Delta/\varrho)$ by restriction. With a slight abuse of notation, we denote each of these homomorphisms by φ_ϱ as well. The map φ_ϱ on $\mathrm{GL}(n, \Delta)$ is a *congruence homomorphism* (with respect to ϱ). The kernel $\mathcal{G}_\varrho$ of φ_ϱ on $\mathrm{GL}(n, \Delta)$ is called a (principal) congruence subgroup. We write the congruence subgroup $G \cap \mathcal{G}_\varrho$ of $G \leq \mathrm{GL}(n, \Delta)$ as G_ϱ. The reader is referred to Suprunenko (1976, Chapter III, Section 11) for background on the use of congruence homomorphisms in linear group theory.

Let $\mathbb{F}$ be a field, $\mathcal{S}$ be a subset $\{S_1, \ldots, S_r\}$ of $\mathrm{GL}(n, \mathbb{F})$, and $G = \langle \mathcal{S} \rangle$. Then $G \leq \mathrm{GL}(n, R)$ where R is the integral domain generated by the entries of the matrices in $\mathcal{S} \cup \mathcal{S}^{-1}$. We are concerned in this paper with the case that $\mathbb{F} = \mathbb{P}(X_1, \ldots, X_m)$, where the X_i are algebraically independent indeterminates, $m > 0$, and $\mathbb{P}$ is a number field. Let μ be the least common multiple of the denominators of the generators of R. Then $R \subseteq \Delta = \mu^{-1}\mathbb{P}[X_1, \ldots, X_m]$, the ring of fractions with denominators in the monoid generated by μ. Note that Δ is a UFD (unique factorization domain).

If G is finite then by a result of Mal'cev (Wehrfritz, 1973, 4.2, p. 51), there exists an ideal ϱ of R such that φ_ϱ is an isomorphism $G \to \varphi_\varrho(G)$. To use this result in practice, we need a way of selecting a suitable ideal ϱ i.e. such that G_ϱ is trivial. The first lemma lists criteria for a suitable ideal. Generalizations of this lemma to positive characteristic, and to Dedekind domains, are given in Detinko and Flannery (2008, Section 3).

Lemma 1 (*Suprunenko, 1976, Theorem 3, p. 68*). *Let Δ be a UFD of characteristic zero. Suppose that $\varrho = \lambda\Delta$, where λ is an irreducible element of Δ such that λ does not divide 2, and λ^2 does not divide p for any prime $p \in \mathbb{Z}$. Then $\mathcal{G}_\varrho$ is torsion-free.*

We denote the ideal of Δ generated by elements $\eta_1, \ldots, \eta_t$ as $\langle \eta_1, \ldots, \eta_t \rangle$.

Corollary 2. *Let Δ be a UFD of characteristic zero. Suppose that there exist elements $\lambda_0 = 0, \lambda_1, \ldots, \lambda_m$ of Δ such that, for $\varrho_j := \langle \lambda_0, \lambda_1, \ldots, \lambda_j \rangle$ and all i, $1 \leq i \leq m$,*

(i) *Δ/ϱ_{i-1} is a UFD of characteristic zero;*
(ii) *$\lambda_i + \varrho_{i-1}$ is an irreducible element of Δ/ϱ_{i-1} such that $\lambda_i + \varrho_{i-1}$ does not divide $2 + \varrho_{i-1}$, and $(\lambda_i + \varrho_{i-1})^2$ does not divide $p + \varrho_{i-1}$ for any prime $p \in \mathbb{Z}$.*

Then $\mathcal{G}_{\varrho_m}$ is torsion-free.

Proof. Lemma 1 and the hypotheses imply that $\mathcal{G}_{\varrho_i/\varrho_{i-1}}$ is torsion-free for all $i \leq m$. Since the composite of group homomorphisms, each of which has torsion-free kernel, also has torsion-free kernel, the result follows. □

Now we explain how to construct an ideal $\varrho = \varrho_m$ as per Corollary 2 in our situation $\Delta = \mu^{-1}\mathbb{P}[X_1, \ldots, X_m]$. We say that $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{P}^m$ is *admissible* if $\mu(\alpha) \neq 0$. Since $\mathbb{P}$ is infinite, there exist infinitely many admissible α. Let $\alpha = (\alpha_1, \ldots, \alpha_m)$ be admissible, and define $\lambda_i = X_i - \alpha_i$, $\varrho = \varrho(\alpha) = \langle \lambda_1, \ldots, \lambda_m \rangle \subseteq \Delta$. By Corollary 2, $\mathcal{G}_\varrho$ is torsion-free. Generators for the image $\varphi_\varrho(G)$ are found simply by substituting α_i for X_i in entries of the S_j, $1 \leq i \leq m$, $1 \leq j \leq r$. Thus $\varphi_\varrho(G) \leq \mathrm{GL}(n, \mathbb{P})$.

If G is infinite then $\varphi_{\varrho(\alpha)}(G)$ may be finite. We consider this possibility in the next lemma.

Lemma 3. *Let $G \leq \mathrm{GL}(n, \Delta)$ be infinite. Then there are infinitely many admissible α such that $\varphi_{\varrho(\alpha)}(G)$ is infinite. If $m = 1$, then $\varphi_{\varrho(\alpha)}(G)$ is finite only for finitely many admissible α.*

Proof. The orders of finite subgroups of $\mathrm{GL}(n, \mathbb{P})$ are bounded above (see the first paragraph of Rockmore et al. (1999, Section 3.2)). So there is a positive integer ν such that every torsion element of $\mathrm{GL}(n, \mathbb{P})$ has order dividing ν. Since a periodic linear group is locally finite (Suprunenko, 1976, Theorem 5, p. 181), G must have an element g of infinite order. Hence, either there exist i, j, $i \neq j$, such that the (i, j)th entry $g_{ij}^{(\nu)}$ of g^ν is non-zero, or there exists k such that $g_{kk}^{(\nu)} \neq 1$. Now there are infinitely many $\alpha \in \mathbb{P}^m$ such that $g_{ij}^{(\nu)}(\alpha) \neq 0$ (and infinitely many α such that $g_{kk}^{(\nu)}(\alpha) \neq 1$). Hence for any such α, $\varphi_{\varrho(\alpha)}(g)$ has infinite order. If $m = 1$, then α may be chosen subject to a finite set of exclusions (i.e. excluding α such that $g_{ij}^{(\nu)}(\alpha) = 0$ or $g_{kk}^{(\nu)}(\alpha) = 1$). □

3. An algorithm for deciding finiteness over function fields in zero characteristic

The results of the previous section suggest the following strategy for deciding finiteness of a given subgroup G of $\mathrm{GL}(n, \Delta)$. First, we select an admissible α and construct $\varphi_\varrho(G) \leq \mathrm{GL}(n, \mathbb{P})$, where $\varrho = \varrho(\alpha)$. (Admissibility of α just means that $\varphi_\varrho(S)$ is defined for all $S \in \mathcal{S} \cup \mathcal{S}^{-1}$.) Then we test whether $\varphi_\varrho(G)$ is finite; if so, we test whether G_ϱ is trivial. In this section we provide a method for solving the latter problem. One advantage of our method is that it avoids computation of the congruence subgroup G_ϱ (in contrast to Detinko and Flannery (2008, Section 4.3)), which can be a difficult task.

3.1. Deciding finiteness via computing with enveloping algebras over the coefficient field

Let $G = \langle \mathcal{S} \rangle$, where $\mathcal{S} = \{S_1, \ldots, S_r\} \subseteq \mathrm{GL}(n, \mathbb{F})$, $\mathbb{F} = \mathbb{P}(X_1, \ldots, X_m)$. We denote the $\mathbb{P}$-enveloping algebra and $\mathbb{P}$-linear span of a subset U of $\mathrm{Mat}(n, \mathbb{F})$ by $\langle U \rangle_\mathbb{P}$ and $\mathrm{span}_\mathbb{P}(U)$, respectively. If $\langle G \rangle_\mathbb{P}$ has finite dimension then a basis of $\langle G \rangle_\mathbb{P}$ can be found by the following well-known procedure (cf. Detinko (2001, p. 70)), which we will refer to as `BasisEnvAlgebra`$(\mathcal{S})$. Define subsets $\mathcal{S}^k$ of $\mathrm{GL}(n, \mathbb{F})$ by $\mathcal{S}^1 = \mathcal{S}$ and $\mathcal{S}^k = \cup_{S_j \in \mathcal{S}}(\mathcal{S}^{k-1} S_j)$ for $k > 1$. That is, $\mathcal{S}^k$ is the set of all length k products of elements drawn from $\mathcal{S}$. Let $A_1 = I_n$, and suppose that we have a $\mathbb{P}$-linearly independent set $\mathcal{A} = \{A_1, \ldots, A_e\} \subseteq \mathrm{GL}(n, \mathbb{F})$ such that for each i, $1 < i \leq e$, $A_i \in \mathcal{S}^k$ for some $k < e$. If there are $A_i \in \mathcal{A}$ and $S_j \in \mathcal{S}$ such that $A_i S_j \notin \mathrm{span}_\mathbb{P}(\mathcal{A})$, then we update $\mathcal{A}$ by adding $A_i S_j$. We repeat this basic step until eventually we get a $\mathbb{P}$-linearly independent set $\mathcal{A} = \{A_1, \ldots, A_d\}$ such that $A_i S_j \in \mathrm{span}_\mathbb{P}(\mathcal{A})$ for all $A_i \in \mathcal{A}$ and $S_j \in \mathcal{S}$. The set $\mathcal{A}$ at this point is the output of `BasisEnvAlgebra`$(\mathcal{S})$: it is a basis of $\langle \mathcal{S} \rangle_\mathbb{P}$ consisting of elements of G. If G is finite then this will be a basis of $\langle G \rangle_\mathbb{P}$; otherwise, we obtain a basis of $\langle G \rangle_\mathbb{P}$ merely by replacing $\mathcal{S}$ in the procedure by $\mathcal{S} \cup \mathcal{S}^{-1}$.

Under the assumptions $\Delta = \mu^{-1}\mathbb{P}[X_1, \ldots, X_m]$ and $\varrho = \varrho(\alpha)$ for admissible $\alpha \in \mathbb{P}^m$, we have that φ_ϱ acts identically on the elements of $\mathbb{P}$. Hence φ_ϱ induces a surjective homomorphism of $\mathbb{P}$-algebras $\langle G\rangle_{\mathbb{P}} \to \langle \varphi_\varrho(G)\rangle_{\mathbb{P}}$.

The next two results are vital.

Lemma 4. *Let $A_1, \ldots, A_\ell$ be elements of $\mathrm{Mat}(n, \Delta)$ such that $\varphi_\varrho(A_1), \ldots, \varphi_\varrho(A_\ell)$ are linearly independent over $\varphi_\varrho(\Delta) = \mathbb{P}$. Then the following hold.*

(i) *$A_1, \ldots, A_\ell$ are linearly independent over $\mathbb{P}$.*
(ii) *If $A \in \mathrm{Mat}(n, \Delta)$, $\varphi_\varrho(A) = \sum_{i=1}^{\ell} \beta_i \varphi_\varrho(A_i)$, $\beta_i \in \mathbb{P}$, and $A \in \mathrm{span}_{\mathbb{P}}(A_1, \ldots, A_\ell)$, then $A = \sum_{i=1}^{\ell} \beta_i A_i$.*

Proof. Obvious, since $\varphi_\varrho|_{\mathbb{P}}$ is the identity map. □

Theorem 5. *Suppose that $\varphi_\varrho(G)$ is finite. Then the following are equivalent.*

(i) *G is finite.*
(ii) *$\varphi_\varrho : \langle G\rangle_{\mathbb{P}} \to \langle \varphi_\varrho(G)\rangle_{\mathbb{P}}$ is an isomorphism.*
(iii) *$\dim_{\mathbb{P}}\langle \varphi_\varrho(G)\rangle_{\mathbb{P}} = \dim_{\mathbb{P}}\langle G\rangle_{\mathbb{P}}$.*

Proof. (i) $\Longleftrightarrow$ (ii): Suppose that G is finite. Since G is completely reducible, $\langle G\rangle_{\mathbb{P}}$ is conjugate to a subalgebra of $\mathrm{Mat}(n, \mathbb{K})$ for some number field $\mathbb{K}$, by Dixon (1971, Theorem 3.4B, p. 54). Hence for each $h \in \langle G\rangle_{\mathbb{P}}$, the characteristic polynomial $f(t)$ of h has all coefficients in $\mathbb{K} \cap \Delta = \mathbb{P}$. Since its coefficients are φ_ϱ-invariant, $f(t)$ is the characteristic polynomial of $\varphi_\varrho(h)$. So if $\varphi_\varrho(h) = 0_n$ then $f(t) = t^n$, and then $h^n = 0_n$. This shows that the kernel of φ_ϱ on $\langle G\rangle_{\mathbb{P}}$ is contained in the radical J of $\langle G\rangle_{\mathbb{P}}$. However $J = \{0\}$ because G is completely reducible; thus φ_ϱ is an isomorphism. The other direction is trivial.

(ii) $\Longleftrightarrow$ (iii): A $\mathbb{P}$-algebra isomorphism is a $\mathbb{P}$-vector space isomorphism, so (ii) $\Rightarrow$ (iii) is clear. If (iii) holds then φ_ϱ maps a basis of $\langle G\rangle_{\mathbb{P}}$ to a basis of $\langle \varphi_\varrho(G)\rangle_{\mathbb{P}}$, so is injective. □

Before proceeding to the statement of our algorithm, we make some observations relating to the last step in the algorithm: testing finiteness of G if $\varphi_\varrho(G)$ is finite. Suppose that φ_ϱ is one-to-one on $\mathcal{S} \cup \mathcal{S}^{-1} = \{S_1, \ldots, S_r\}$, and set $\varphi_\varrho(S_i) = \bar{S}_i$. Then given any element $\bar{A} = \bar{S}_{k_1} \cdots \bar{S}_{k_t}$ of $\langle \varphi_\varrho(G)\rangle_{\mathbb{P}}$, we are able to define a canonical pre-image $A = S_{k_1} \cdots S_{k_t}$ in $\langle G\rangle_{\mathbb{P}}$. Thus, if we have a basis $\bar{\mathcal{A}} = \{\bar{A}_1, \ldots, \bar{A}_d\}$ of $\langle \varphi_\varrho(G)\rangle_{\mathbb{P}}$ computed via `BasisEnvAlgebra`, then we readily gain $\mathcal{A} = \{A_1, \ldots, A_d\} \subseteq \langle G\rangle_{\mathbb{P}}$. By Lemma 4 (i), $\mathcal{A}$ is linearly independent. Theorem 5 shows that to test whether G is finite, it suffices to compare the dimensions of $\langle \varphi_\varrho(G)\rangle_{\mathbb{P}}$ and $\langle G\rangle_{\mathbb{P}}$. By Lemma 4 and Theorem 5, we should not compute a basis of $\langle G\rangle_{\mathbb{P}}$ (moreover, $\langle G\rangle_{\mathbb{P}}$ may be infinite-dimensional), but only check whether $\bar{A}_i\bar{S}_j = \sum_{k=1}^{d} \beta_k \bar{A}_k$, $\beta_k \in \mathbb{P}$, implies that $A_iS_j = \sum_{k=1}^{d} \beta_k A_k$.

We summarize all of the above in the following algorithm.

`IsFiniteMatGroupFuncNF`($\mathcal{S}$)

Input: a finite subset $\mathcal{S}$ of $\mathrm{GL}(n, \mathbb{F})$, where $\mathbb{F} = \mathbb{P}(X_1, \ldots, X_m)$, $\mathbb{P}$ a number field.

Output: a message 'true' meaning that $G = \langle \mathcal{S}\rangle$ is finite, or a message 'false' otherwise.

(I) Let $\mathcal{S} := \mathcal{S} \cup \mathcal{S}^{-1}$.
Find $\alpha \in \mathbb{P}^m$ admissible for $\mathcal{S}$, and compute $\bar{\mathcal{S}} := \{\bar{S}_i := \varphi_\varrho(S_i) \mid S_i \in \mathcal{S}\}$, $\varrho := \varrho(\alpha)$.
(II) If $\bar{S}_i = \bar{S}_j$ for some $i \neq j$ then return 'false'.
(III) If $\varphi_\varrho(G) = \langle \bar{\mathcal{S}}\rangle \leq \mathrm{GL}(n, \mathbb{P})$ is infinite then return 'false'.
(IV) Construct $\bar{\mathcal{A}} := $ `BasisEnvAlgebra`$(\bar{\mathcal{S}}) := \{\bar{A}_1, \ldots, \bar{A}_d\}$, and find $\mathcal{A} := \{A_1, \ldots, A_d\}$.
For $\bar{A}_i \in \bar{\mathcal{A}}$, $\bar{S}_j \in \bar{\mathcal{S}}$, find $\beta_k \in \mathbb{P}$ such that $\bar{A}_i\bar{S}_j = \sum_{k=1}^{d} \beta_k \bar{A}_k$.
If for some i, j we have $A_iS_j \neq \sum_{k=1}^{d} \beta_k A_k$, then return 'false'; else return 'true'.

We now comment on the practicality of `IsFiniteMatGroupFuncNF`. For further discussion along these lines, see Section 4.

A significant computational advantage of the algorithm is that most of its operations are performed over $\mathbb{P}$ rather than $\mathbb{P}(X_1, \ldots, X_m)$. Over the latter field, only matrix multiplication and calculating a few $\mathbb{P}$-linear combinations may be required.

Step III requires deciding finiteness over $\mathbb{P}$. To do this we may use any of the available implementations (in e.g. GAP or MAGMA) of the algorithms in Babai et al. (1993); then the efficiency of `IsFiniteMatGroupFuncNF` would depend on the efficiency of the chosen implementation (here we refer to Babai et al. (1993, Section 8) for relevant complexity estimates). For nilpotent groups we could even use the Nilmat function `IsFiniteNilpotentMatGroup`.

Apart from the above, the most time-consuming part of `IsFiniteMatGroupFuncNF` (if it is reached) is Step IV, i.e. computing a basis of $\langle \varphi_\varrho(G) \rangle_{\mathbb{P}}$. The transitive closure algorithm `BasisEnvAlgebra` is a frequently used tool in computing with matrix groups. Complexity estimates for such algorithms are given in Babai et al. (1993, Section 8) and Rockmore et al. (1999, Section 3.4.1). We stress that `BasisEnvAlgebra` is invoked only over the coefficient field, not over the original function field of definition. If G is finite then Step IV is unavoidable. If G is infinite then by Lemma 3 we expect Step IV would not be reached, especially when $m = 1$; that is, infiniteness of the input would be detected at an earlier stage of the algorithm. Therefore we expect `IsFiniteMatGroupFuncNF` to be a simpler process for an infinite rather than finite input group.

3.2. Related algorithms

3.2.1. Computing orders

In addition to deciding finiteness, `IsFiniteMatGroupFuncNF` leads to a solution of one more important computational problem: determining the order of a finite subgroup of $\mathrm{GL}(n, \mathbb{F})$. Suppose that G is finite (as recognized by `IsFiniteMatGroupFuncNF`); then $|G| = |\varphi_\varrho(G)|$. Since $\varphi_\varrho(G) \leq \mathrm{GL}(n, \mathbb{P})$, and orders over $\mathbb{Q}$ may be computed using standard procedures (e.g. the GAP function `Order`), this settles the problem. Here is another approach. We have $\varphi_\varrho(G) \leq \mathrm{GL}(n, \Delta/\varrho)$ where Δ/ϱ is a finitely generated Dedekind domain. So, as in Lemma 1, we may choose a maximal ideal σ of Δ/ϱ such that $\varphi_\varrho(G)$ has trivial congruence subgroup with respect to φ_σ (see Detinko and Flannery (2008, Section 3)). Thus we find $|G|$ by calculating the order of an isomorphic copy of G in some $\mathrm{GL}(n, q)$. In particular, if $g \in \mathrm{GL}(n, \mathbb{F})$ has finite order, then $|g|$ may be calculated by the preceding and the algorithm of Celler and Leedham-Green (O'Brien, 2006, Section 2).

3.2.2. Deciding finiteness in zero characteristic

We now describe how solution of the finiteness decision problem may be generalized to any field of zero characteristic. The key idea is to represent input data in a form that allows us to apply `IsFiniteMatGroupFuncNF` and the algorithm of Babai et al. (1993). First note that if we have an algorithm for deciding finiteness over a field $\mathbb{K}$, and $\mathbb{L}$ is a finite degree extension of $\mathbb{K}$, then we can test finiteness of $G \leq \mathrm{GL}(n, \mathbb{L})$ after expressing entries from $\mathbb{L}$ as matrices over $\mathbb{K}$ (according to the multiplication action of elements of $\mathbb{L}$ on a $\mathbb{K}$-basis of $\mathbb{L}$). Suppose that $\mathrm{char}\,\mathbb{L} = 0$. Then since $G \leq \mathrm{GL}(n, R)$ where $R \subseteq \mathbb{L}$ is finitely generated and contains a copy of $\mathbb{Z}$, by elementary structure theory of finitely generated field extensions we can replace $\mathbb{L}$ by a suitable finite extension of $\mathbb{K} = \mathbb{Q}(X_1, \ldots, X_m)$. The above reduction gives $H \leq \mathrm{GL}(s, \mathbb{K})$ for some $H \cong G$ and s divisible by n, and then `IsFiniteMatGroupFuncNF` can be applied to H to decide finiteness of G. In this way it is possible to test (for example) finiteness of finitely generated subgroups of $\mathrm{GL}(n, \mathbb{R})$ and $\mathrm{GL}(n, \mathbb{C})$. Matrix entries are handled symbolically, dispensing with the need for floating point representation of numbers.

4. Implementation and experimental results

We have implemented `IsFiniteMatGroupFuncNF` in GAP (The GAP group). In this section we present computational results that characterize the practicality of `IsFiniteMatGroupFuncNF`, depending on the main input parameters.

As noted previously, when the image $\bar{G}$ of G under a congruence homomorphism is finite, the algorithm will proceed to the most computationally intensive stage. In turn, the time for completion

Table 1
Experimental results for `IsFiniteMatGroupFuncNF`.

G	n	No. of generators	$\lvert\bar{G}\rvert$	Runtime ($\bar{G}$)	Runtime (G)
G_{11}	10	3	$2^{10}10!$	00 : 02.438	00 : 05.547
G_{12}	10	3	$2^{10}10!$	"	01 : 31.781
G_{21}	20	3	$2^{20}20!$	00 : 03.063	17 : 40.703
G_{22}	20	3	$2^{20}20!$	"	19 : 06.547
G_{31}	36	12	648	00 : 03.172	02 : 02.469
G_{32}	36	12	648	"	16 : 59.078

of that stage will depend on whether or not the input group G is finite. To address these issues, we performed experiments for groups with extremal properties. Specifically, we tested groups G such that (a) both G and $\bar{G}$ are absolutely irreducible, so give the largest dimension n^2 of $\langle \bar{G} \rangle_{\mathbb{P}}$; and (b) $\bar{G}$ has order $2^n n!$, which is an upper bound on the order of finite subgroups of $\mathrm{GL}(n, \mathbb{Q})$ for $n \geq 10$ (see Rockmore et al. (1999, Section 3.2)). Some results, for $\mathbb{F} = \mathbb{Q}(X)$, are displayed in Table 1. The experiments were carried out on a Pentium 4 running at 1.73 GHz under Windows. CPU time is in the format minutes : seconds.milliseconds.

The groups G_{i1} are infinite, whereas the G_{i2} are finite, $1 \leq i \leq 3$. For each i, the image groups $\bar{G}_{i1}$ and $\bar{G}_{i2}$ are conjugate subgroups of $\mathrm{GL}(n, \mathbb{Q})$. For $i = 1, 2$, $\bar{G}_{i1}$ and $\bar{G}_{i2}$ are conjugate to full monomial subgroups of $\mathrm{GL}(n, \mathbb{Q})$. The groups $\bar{G}_{3i}$ are finite nilpotent, and were constructed using the function `MonomialNilpotentMatGroup` of Detinko et al. (2007). The runtime of Step III of `IsFiniteMatGroupFuncNF` (deciding finiteness of $\bar{G}_{ij} \leq \mathrm{GL}(n, \mathbb{Q})$) is shown in column 5 of Table 1. This may be compared with the total runtime, in the last column. We observed similar runtimes for one indeterminate as for other reasonably small numbers of indeterminates.

To monitor how size of input matrix entries affects the speed of `IsFiniteMatGroupFuncNF`, we took the entries of generators of G_{12} to be integral polynomials of degree up to 30, with coefficients up to 2,000,000. Other groups in Table 1 have matrix entries of much more moderate size, so for those groups this parameter did not affect runtimes.

5. Remarks on the positive characteristic case

The methods of this paper may also be used to decide finiteness of matrix groups in positive characteristic i.e. groups over function fields $\mathbb{F} = \mathbb{F}_q(X_1, \ldots, X_m)$, $\mathbb{F}_q$ the finite field of size q. However, this case is much more complicated. Some sources of difficulty are that the order of a finite subgroup G of $\mathrm{GL}(n, \mathbb{F})$ can be arbitrarily large, and G need not be completely reducible. Furthermore, $\mathbb{F}_q$ may not contain α_i such that $\alpha = (\alpha_1, \ldots, \alpha_m)$ is admissible and $\varphi_{\varrho(\alpha)}$ acts on G as an isomorphism, for $\varrho(\alpha)$ defined as in Section 2. So in general it is necessary to work over extensions of $\mathbb{F}_q$. As the finiteness problem in positive characteristic has an essentially different nature to the problem in zero characteristic, it is the subject of separate investigation.

Acknowledgment

The authors are grateful to Professor Eamonn O'Brien, who recently implemented `IsFiniteMatGroupFuncNF` in Magma, and obtained much improved runtimes over those reported in Table 1.

References

Babai, L., 1992. Deciding finiteness of matrix groups in Las Vegas polynomial time. In: Proceedings of the Third Annual ACM–SIAM Symposium on Discrete Algorithms (Orlando, FL, 1992). ACM, New York, pp. 33–40.

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.

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., 2007. Nilmat—Computing with nilpotent matrix groups. A refereed GAP 4 package; see http://www.gap-system.org/Packages/nilmat.html.
Detinko, A.S., Flannery, D.L., 2008. Algorithms for computing with nilpotent matrix groups over infinite domains. J. Symbolic Comput. 43, 8–26.
Dixon, J.D., 1971. The Structure of Linear Groups. Van Nostrand Reinhold, London.
The GAP group. GAP - Groups, Algorithms, and Programming, Version 4.4.10 http://www.gap-system.org.
Ivanyos, G., 2001. Deciding finiteness for matrix semigroups over function fields over finite fields. Israel J. Math. 124, 185–188.
Lyndon, R.C., Schupp, P.E., 2001. Combinatorial Group Theory. Springer.
O'Brien, E.A., 2006. Towards effective algorithms for linear groups. In: Finite Geometries, Groups, and Computation. Walter de Gruyter, Berlin, pp. 163–190.
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. In: Transl. Math. Monogr., vol. 45. American Mathematical Society, Providence, RI.
Wehrfritz, B.A.F., 1973. Infinite Linear Groups. Springer-Verlag.