Volume 322, Issue 11, December 1, 2009 ISSN 0021-8693

ELSEVIER

JOURNAL OF
ALGEBRA
COMPUTATIONAL ALGEBRA

Journal of Algebra 322 (2009) 4151–4160

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Deciding finiteness of matrix groups in positive characteristic ☆

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, University of Auckland, Auckland, New Zealand

ARTICLE INFO

Article history:
Received 29 June 2009
Available online 1 October 2009
Communicated by Derek Holt

Keywords:
Matrix group
Function field
Finiteness problem
Order problem
Algorithm

ABSTRACT

We present a new algorithm to decide finiteness of matrix groups defined over a field of positive characteristic. Together with previous work for groups in zero characteristic, this provides the first complete solution of the finiteness problem for finitely generated matrix groups over a field. We also give an algorithm to compute the order of a finite matrix group over a function field of positive characteristic by constructing an isomorphic copy of the group over a finite field. Our implementations of these algorithms are publicly available in MAGMA.

1. Introduction

Deciding finiteness is a fundamental problem for any class of potentially infinite groups. For matrix groups over a field of zero characteristic, the algorithms of [1,6] provide a solution of this problem, and their implementations perform satisfactorily for reasonably large input (cf. [6, Section 4]). Deciding finiteness over a purely transcendental extension $\mathbb{F}$ of a finite field was considered by several authors [3,9,10]. The approach taken in [10] relies on the fact that a subgroup G of $\mathrm{GL}(n, \mathbb{F})$ is finite if and only if, for every finite subfield $\mathbb{F}_q$ of $\mathbb{F}$, the enveloping algebra $\langle G\rangle_{\mathbb{F}_q}$ is finite. Since the $\mathbb{F}_q$-dimension of $\langle G\rangle_{\mathbb{F}_q}$ may depend exponentially on n (see [10, Theorem 3.3]), this leads to exponential-time algorithms. The polynomial-time algorithms of [3,9] involve significant computing over function fields, and so we expect that they are practical only for small input. We know of no implementations of the algorithms of [3,9,10].

☆ Supported in part by Science Foundation Ireland, grants 07/MI/007 and 08/RFP/MTH1331, and by the Marsden Fund of New Zealand, grant UOA 721.

* Corresponding author.
E-mail address: dane.flannery@nuigalway.ie (D.L. Flannery).

0021-8693/$ – see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2009.08.020

A uniform approach to deciding finiteness of matrix groups over an infinite field via congruence homomorphisms was proposed in [5, Section 4.3], and applied to nilpotent groups. We implemented this approach, for rational nilpotent groups, in the computer algebra systems Magma [2] and GAP (see the 'Nilmat' package [4]). Its performance is usually much better than existing procedures in GAP and Magma.

The idea of using congruence homomorphisms to decide finiteness of matrix groups was further developed in [6], for groups over a function field of zero characteristic. In this paper we extend the ideas of [6] to positive characteristic. As in that earlier paper, our main method is the application of congruence homomorphisms to enable a comparison of dimensions of certain enveloping algebras. However, the finiteness problem in positive characteristic is more complicated: a finite subgroup of $\mathrm{GL}(n,\mathbb{F})$ need not be completely reducible, and it can be unboundedly large. The opposite holds in characteristic zero.

Despite these difficulties, we obtain a substantial improvement upon the algorithms of [3,9,10]. We avoid their most inefficient step; namely, computing a basis of the enveloping algebra of the input group over a function field (see Sections 2 and 3). As in [6], much of the computation takes place in the coefficient field – which is finite here. Although the number of (function and finite) field operations of our finiteness testing algorithm is polynomial in certain parameters of the input, our primary goal was to develop a *practical* algorithm. We have implemented it in Magma [2] and demonstrate that it performs well for a range of input.

We also give an algorithm to compute the order of a finite matrix group G over a function field of positive characteristic, relying on the same strategy used to decide finiteness. This algorithm finds an isomorphic copy of G over a finite field, which can be used to derive additional information about G. In Section 4 we present a simplified finiteness test for nilpotent groups. Finally, in Section 5 we report on the performance of our Magma implementation of the algorithms.

By elementary structure theory of finitely generated field extensions, any finitely generated matrix group G is defined over a finite extension of a function field. As explained below, we can construct an isomorphism of G onto a group defined over the function field, in larger degree. Thus the results of this paper together with [1,6] effectively allow us to decide finiteness of a finitely generated matrix group over any field (cf. also [6, Section 3.2.2]).

2. Preliminaries and background

Let $\mathbb{F}$ be a field of characteristic $p>0$, and let $G=\langle\mathcal{S}\rangle$, where $\mathcal{S}=\{S_1,\ldots,S_r\}\subseteq\mathrm{GL}(n,\mathbb{F})$. We may assume that $\mathbb{F}$ is a finite extension of a function field $\mathbb{E}=\mathbb{F}_q(X_1,\ldots,X_m)$, where the X_i are algebraically independent indeterminates, and $\mathbb{F}_q$ is the finite field of size q. Replacement of elements of $\mathbb{F}$ by matrices over $\mathbb{E}$ according to the multiplication action of $\mathbb{F}$ on an $\mathbb{E}$-basis of $\mathbb{F}$ defines an isomorphism of G into $\mathrm{GL}(nl,\mathbb{E})$, where $l=|\mathbb{F}:\mathbb{E}|$. So without loss of generality, from now on $\mathbb{F}=\mathbb{F}_q(X_1,\ldots,X_m)$, $m\geqslant 1$, and q is a power of the prime p.

In fact G is contained in $\mathrm{GL}(n,R)$ for a finitely generated integral domain $R\subseteq\mathbb{F}$. We can take $R=\frac{1}{f}\mathbb{F}_q[X_1,\ldots,X_m]$, where $f=f(X_1,\ldots,X_m)$ is a common multiple of the denominators of the non-zero entries of the S_i and S_i^{-1}, $1\leqslant i\leqslant r$. We say that $\alpha=(\alpha_1,\ldots,\alpha_m)$ is *admissible* (or *$\mathcal{S}$-admissible*) if $f(\alpha)\neq 0$. Here the α_i are in the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$; note that $\mathbb{F}_q$ need not contain α_i such that α is admissible. For an admissible α, let ν denote the positive integer such that $\mathbb{F}_q(\alpha):=\mathbb{F}_q(\alpha_1,\ldots,\alpha_m)=\mathbb{F}_{q^\nu}$. Let φ_α be the ring homomorphism $R\to\mathbb{F}_{q^\nu}$ whose kernel is generated by the monomials $X_i-\alpha_i$, $1\leqslant i\leqslant m$. If necessary, we extend φ_α to a homomorphism $\widehat{R}=\frac{1}{f}\mathbb{F}_{q^\mu}[X_1,\ldots,X_m]\to\mathbb{F}_{q^{\mu\nu}}$ for $\mu\geqslant 1$ in the obvious way. With a slight abuse of notation, the induced congruence homomorphisms on $\mathrm{GL}(n,\widehat{R})$ and on the full matrix algebra $\mathrm{Mat}(n,\widehat{R})$ will also be denoted φ_α. Evaluation of φ_α on a subset $\mathcal{M}$ of $\mathrm{Mat}(n,\widehat{R})$ is simply substitution of α_i for X_i in the entries of the elements of $\mathcal{M}$, $1\leqslant i\leqslant m$. We denote $\varphi_\alpha(\mathcal{M})$ as $\mathcal{M}(\alpha)$.

Lemma 2.1. *If G is finite then the kernel of φ_α on G is a p-group.*

Proof. This holds for $m = 1$ by [5, Proposition 3.2 and Example 3.6]. The result for $m > 1$ follows readily: the kernel of a composite of congruence homomorphisms, all of whose kernels are p-groups, is a p-group. □

Corollary 2.2. *If G is finite and completely reducible, then φ_α is an isomorphism from G onto $\varphi_\alpha(G)$ for every admissible α.*

Let $\mathbb{L}/\mathbb{K}$ be a field extension, and suppose that $\mathcal{T}$ is a finite subset of $\mathrm{GL}(n, \mathbb{L})$ such that the enveloping algebra $\langle \mathcal{T} \rangle_{\mathbb{K}}$ is finite-dimensional as a $\mathbb{K}$-vector space. We now describe a standard procedure that constructs a basis of $\langle \mathcal{T} \rangle_{\mathbb{K}}$ consisting of elements from the monoid generated by $\mathcal{T}$. (Since we use the procedure to compute an enveloping algebra basis only over a finite field, we assume that $\mathbb{L}$ is finite in the description.)

```
BasisEnvAlgebra($\mathcal{T}, \mathbb{K}$)
Input: $\mathcal{T} \subseteq \mathrm{GL}(n, \mathbb{L})$, $\mathbb{L}$ a finite field, and $\mathbb{K}$ a subfield of $\mathbb{L}$.
Output: a basis of the enveloping algebra $\langle H \rangle_{\mathbb{K}}$, where $H = \langle \mathcal{T} \rangle$.

  (I) $\mathcal{A} := \{I_n\}$.
 (II) While there exist $A \in \mathcal{A}$ and $T \in \mathcal{T}$ such that $AT \notin \mathrm{span}_{\mathbb{K}}(\mathcal{A})$ do $\mathcal{A} := \mathcal{A} \cup \{AT\}$.
(III) Return $\mathcal{A}$.
```

We now set up a convention. Suppose that $\mathcal{S}(\alpha)$ is duplicate-free. For $A(\alpha) \in \mathrm{Mat}(n, \mathbb{F}_{q^\nu})$ that is a word in the elements of $\mathcal{S}(\alpha)$, we canonically define a pre-image A of $A(\alpha)$ in $\mathrm{GL}(n, \mathbb{F})$: if $A(\alpha) = S_{i_1}(\alpha) \cdots S_{i_t}(\alpha)$ then $A = S_{i_1} \cdots S_{i_t}$.

Lemma 2.3. *Matrices $B_1, \ldots, B_l$ in $\mathrm{Mat}(n, \mathbb{F})$ are $\mathbb{F}_q$-linearly independent if and only if they are $\mathbb{F}_{q^\mu}$-linearly independent.*

Proof. The non-trivial $\mathbb{F}_{q^\mu}$-linear dependence $\sum_{i=1}^{l} a_i B_i = 0_n$ between the B_i yields a system of equations with coefficients in $\mathbb{F}$. Since $(a_1, \ldots, a_l)$ is a solution of this system, $a_i \in \mathbb{F} \cap \mathbb{F}_{q^\mu} = \mathbb{F}_q$ for all i. Thus, if the B_i are $\mathbb{F}_q$-linearly independent then they must be $\mathbb{F}_{q^\mu}$-linearly independent. The other direction is obvious. □

Corollary 2.4. *If G is finite then $\dim_{\mathbb{F}_q} \langle G \rangle_{\mathbb{F}_q} = \dim_{\mathbb{F}_{q^\mu}} \langle G \rangle_{\mathbb{F}_{q^\mu}}$.*

Proof. By Lemma 2.3, $\dim_{\mathbb{F}_q} \langle G \rangle_{\mathbb{F}_q} \leqslant \dim_{\mathbb{F}_{q^\mu}} \langle G \rangle_{\mathbb{F}_{q^\mu}}$. Conversely, $\langle G \rangle_{\mathbb{F}_{q^\mu}}$ has a basis consisting of elements of G; that basis is therefore an $\mathbb{F}_q$-linearly independent subset of $\langle G \rangle_{\mathbb{F}_q}$. Hence $\dim_{\mathbb{F}_{q^\mu}} \langle G \rangle_{\mathbb{F}_{q^\mu}} \leqslant \dim_{\mathbb{F}_q} \langle G \rangle_{\mathbb{F}_q}$. □

We write $\widehat{\mathbb{F}}$ for $\mathbb{F}_{q^\mu}(X_1, \ldots, X_m)$.

Lemma 2.5. *If G is finite then the kernel of φ_α on $\langle G \rangle_{\mathbb{F}_{q^\mu}}$ is contained in the radical of $\langle G \rangle_{\mathbb{F}_{q^\mu}}$ and the radical of $\langle G \rangle_{\widehat{\mathbb{F}}}$.*

Proof. The proofs of Proposition 3.2 and Corollary 3.3 in [3] carry over. □

Lemma 2.6. *If G is completely reducible, then G is finite if and only if $\varphi_\alpha : \langle G \rangle_{\mathbb{F}_{q^\mu}} \to \langle G(\alpha) \rangle_{\mathbb{F}_{q^\mu}}$ is an isomorphism, for any $\mathcal{S}$-admissible α and $\mu \geqslant 1$.*

Proof. If G is finite then G is completely reducible over the extension field $\widehat{\mathbb{F}}$ of $\mathbb{F}$ (see e.g. [8, 1.8, p. 12]), so the radical of $\langle G \rangle_{\widehat{\mathbb{F}}}$ is zero. Lemma 2.5 now implies that $\ker \varphi_\alpha$ on $\langle G \rangle_{\mathbb{F}_{q^\mu}}$ is trivial. □

Note that Lemma 2.6 implies Corollary 2.2.

Lemma 2.7. *The algebras $\langle G\rangle_{\mathbb{F}_{q^\mu}}$ and $\langle G(\alpha)\rangle_{\mathbb{F}_{q^\mu}}$ are isomorphic if and only if*

$$\dim_{\mathbb{F}_{q^\mu}}\langle G\rangle_{\mathbb{F}_{q^\mu}}=\dim_{\mathbb{F}_{q^\mu}}\langle G(\alpha)\rangle_{\mathbb{F}_{q^\mu}}.$$

Proof. A basis of $\langle G\rangle_{\mathbb{F}_{q^\mu}}$ maps under φ_α to a spanning set of $\langle G(\alpha)\rangle_{\mathbb{F}_{q^\mu}}$, which is a basis if and only if the $\mathbb{F}_{q^\mu}$-dimensions of these two algebras are equal. □

Corollary 2.8. *If G is completely reducible, then G is finite if and only if, for every $\mathcal{S}$-admissible α,*

$$\dim_{\mathbb{F}_{q^\mu}}\langle G\rangle_{\mathbb{F}_{q^\mu}}=\dim_{\mathbb{F}_{q^\mu}}\langle G(\alpha)\rangle_{\mathbb{F}_{q^\mu}}=\dim_{\mathbb{F}_q}\langle G\rangle_{\mathbb{F}_q}=\dim_{\mathbb{F}_q}\langle G(\alpha)\rangle_{\mathbb{F}_q}.$$

Proof. This follows from Corollary 2.4, Lemma 2.6 and Lemma 2.7. □

Lemma 2.9. *If $A_1(\alpha),\dots,A_d(\alpha)$ are $\mathbb{F}_{q^\mu}$-linearly independent, then $A_1,\dots,A_d$ are $\mathbb{F}_{q^\mu}$-linearly independent.*

Proof. Clear, since φ_α is $\mathbb{F}_{q^\mu}$-linear. □

Now we state an algorithm to decide whether an enveloping algebra $\langle G\rangle_{\mathbb{F}_{q^\mu}}$ and its congruence image $\langle G(\alpha)\rangle_{\mathbb{F}_{q^\mu}}$ are isomorphic, for admissible α and $\mu\geqslant 1$. This uses the same approach as the algorithm `IsFiniteMatGroupFuncNF` of [6].

```
IsIsomorphismEnvAlgebras($\mathcal{S},\alpha,\mu$)
Input: a finite subset $\mathcal{S}=\{S_1,\dots,S_r\}$ of GL($n,\mathbb{F}$), an $\mathcal{S}$-admissible $\alpha$, a positive integer $\mu$.
Output: 'true' if $\varphi_\alpha$ acts on $\langle G\rangle_{\mathbb{F}_{q^\mu}}$ as an isomorphism, where $G=\langle\mathcal{S}\rangle$; 'false' otherwise.

  (I) If $\mathcal{S}(\alpha)$ has duplicates then return 'false'.
 (II) Construct $\mathcal{A}(\alpha)=\{A_1(\alpha),\dots,A_d(\alpha)\}:=$ BasisEnvAlgebra($\mathcal{S}(\alpha),\mathbb{F}_{q^\mu}$).
      Let $\mathcal{A}$ be the set of canonical pre-images $\{A_1,\dots,A_d\}$.
(III) For $A_i(\alpha)\in\mathcal{A}(\alpha)$ and $S_j(\alpha)\in\mathcal{S}(\alpha)$
          find $a_k\in\mathbb{F}_{q^\mu}$ such that $A_i(\alpha)S_j(\alpha)=\sum_{k=1}^d a_kA_k(\alpha)$.
          If $A_iS_j\neq\sum_{k=1}^d a_kA_k$, then return 'false'.
 (IV) Return 'true'.
```

If `IsIsomorphismEnvAlgebras`($\mathcal{S},\alpha,\mu$) returns 'true' then G is finite, and the set $\mathcal{A}$ found in step (II) is a basis of $\langle\mathcal{S}\rangle_{\mathbb{F}_{q^\mu}}=\langle G\rangle_{\mathbb{F}_{q^\mu}}$. (For $\mathcal{A}$ is a spanning set by step (III), and it is linearly independent by Lemma 2.9.) Observe that we obtain this basis after a calculation over a finite field, rather than over the function field $\mathbb{F}$.

By Lemma 2.6, the following algorithm decides finiteness of a completely reducible subgroup of GL($n,\mathbb{F}$).

```
IsFiniteCRMatGroupFuncFF($\mathcal{S}$)
Input: a finite subset $\mathcal{S}$ of GL($n,\mathbb{F}$) such that $G=\langle\mathcal{S}\rangle$ is completely reducible.
Output: 'true' if $G$ is finite; 'false' otherwise.

 (I) Find an $\mathcal{S}$-admissible $\alpha$.
(II) Return IsIsomorphismEnvAlgebras($\mathcal{S},\alpha,\nu$).
```

Corollary 2.8 implies that we can also decide finiteness of a completely reducible group G by testing whether φ_α acts as an isomorphism on $\langle G\rangle_{\mathbb{F}_{q^\mu}}$, for any given $\mu \geqslant 1$. However $\dim_{\mathbb{F}_{q^\mu}} \langle G(\alpha)\rangle_{\mathbb{F}_{q^\mu}}$ might be larger than $\dim_{\mathbb{F}_{q^\nu}} \langle G(\alpha)\rangle_{\mathbb{F}_{q^\nu}}$, which is bounded above by n^2.

Now suppose that G is a (finitely generated, not necessarily completely reducible) subgroup of $\mathrm{GL}(n,\mathbb{F})$, and we know α such that φ_α is an isomorphism on $\langle G\rangle_{\mathbb{F}_{q^\nu}}$ if G is finite. We may now decide finiteness of G just as in `IsFiniteCRMatGroupFuncFF` – namely, by applying `IsIsomorphismEnvAlgebras`. Unfortunately, such α need not exist. On the other hand, there always exist α such that φ_α is an isomorphism on $\langle G\rangle_{\mathbb{F}_q}$ if G is finite. We consider these issues again at the end of Section 3.

3. Deciding finiteness and computing orders in positive characteristic

We now present a general algorithm to decide finiteness of a finitely generated subgroup G of $\mathrm{GL}(n,\mathbb{F})$. The approach is similar to the finiteness testing algorithm of [3], but avoids its most complicated step: computing a basis of $\langle G\rangle_{\mathbb{F}}$ over $\mathbb{F}$. We also outline a simple method to compute the order of a finite subgroup of $\mathrm{GL}(n,\mathbb{F})$.

We continue with established notation. That is, α is an $\mathcal{S}$-admissible m-tuple of elements from $\bar{\mathbb{F}}_q$ such that $\mathcal{S}(\alpha)$ is duplicate-free, and $\mathcal{A}(\alpha) = \{A_1(\alpha),\dots,A_d(\alpha)\}$ is a basis of $\langle G(\alpha)\rangle_{\mathbb{F}_q(\alpha)}$ computed via `BasisEnvAlgebra`, with canonical pre-image $\mathcal{A} = \{A_1,\dots,A_d\}$. For i and j such that $A_i(\alpha)S_j(\alpha) = \sum_{k=1}^{d} a_k A_k(\alpha)$, where $a_k \in \mathbb{F}_{q^\nu} = \mathbb{F}_q(\alpha)$, define $D = A_i S_j - \sum_{k=1}^{d} a_k A_k$. We assume that p does not divide ν. For $a \in \mathbb{F}_{q^\nu}$, denote the trace of a over $\mathbb{F}_q$ by $\mathrm{tr}(a)$:

$$\mathrm{tr}(a) = a + \sigma(a) + \cdots + \sigma^{\nu-1}(a), \qquad \mathrm{Gal}(\mathbb{F}_{q^\nu}/\mathbb{F}_q) = \langle\sigma\rangle.$$

Observe that $D' := \nu A_i S_j - \sum_{k=1}^{d} \mathrm{tr}(a_k) A_k$ is in $\langle G\rangle_{\mathbb{F}}$.

Lemma 3.1. *Let D and D' be as defined above. If G is finite and $D \neq 0_n$, then D' is a non-zero element of the radical $\mathfrak{R}$ of $\langle G\rangle_{\mathbb{F}}$.*

Proof. If $D' = 0_n$ then $A_i S_j = \sum_{k=1}^{d} b_k A_k$ where $b_k = \frac{1}{\nu}\,\mathrm{tr}(a_k) \in \mathbb{F}_q$. In fact $A_i(\alpha)S_j(\alpha) = \sum_{k=1}^{d} b_k A_k(\alpha)$ implies that $b_k = a_k$ for all k. But this contradicts $D = A_i S_j - \sum_{k=1}^{d} a_k A_k \neq 0_n$. Hence D' is non-zero. We verify that $D' \in \mathfrak{R}$ as in the proof of [3, Corollary 3.5]. □

Lemma 3.2. *The nullspace of the radical $\mathfrak{R}$ of $\langle G\rangle_{\mathbb{F}}$ is a non-zero G-module.*

Proof. For all $g \in G$ and u in the nullspace U of $\mathfrak{R}$, we have $\mathfrak{R}gu = \mathfrak{R}u = 0$, since $\mathfrak{R}$ is an ideal of $\langle G\rangle_{\mathbb{F}}$. Thus $GU \subseteq U$ as required. □

So if G is finite and $D \neq 0_n$, then the nullspace of D' contains a non-trivial G-module. We can find such a module using the following procedure.

```
ModuleViaNullspace($\mathcal{S}$, $E$)
Input: a finite subset $\mathcal{S}$ of $\mathrm{GL}(n,\mathbb{F})$, and $E \in \mathrm{Mat}(n,\mathbb{F})$.
Output: a $G$-module $U$ in the nullspace of $E$, for $G = \langle\mathcal{S}\rangle$.

  (I) $U :=$ Nullspace($E$).
 (II) While there exists $S_i \in \mathcal{S}$ such that $U \cap S_iU \neq U$ do $U := U \cap S_iU$.
(III) Return $U$.
```

Since each pass through the while loop reduces the dimension of U, `ModuleViaNullspace` terminates in at most n iterations. If E is a non-zero element of $\mathfrak{R}$ (for example, if G is finite and $E = D'$ for $D \neq 0_n$), then the output is a proper non-zero G-submodule of the underlying space V.

Now we present our main algorithm for deciding finiteness. We use the following notation. Let U be a G-submodule of V and extend a basis of U to a basis of V. Write G with respect to the latter basis in block triangular form; then ρ_U denotes the projection homomorphism from G onto the block diagonal group, whose kernel is the unitriangular subgroup that fixes U and V/U elementwise.

```
IsFiniteMatGroupFuncFF($\mathcal{S}$)
Input: a finite subset $\mathcal{S}$ of $\mathrm{GL}(n, \mathbb{F})$.
Output: 'true' if $G = \langle \mathcal{S} \rangle$ is finite; 'false' otherwise.

  (I) Find an $\mathcal{S}$-admissible $\alpha$ such that $p$ does not divide $\nu = |\mathbb{F}_q(\alpha)/\mathbb{F}_q|$.
      If $S_i(\alpha) = S_j(\alpha)$ for distinct $S_i, S_j \in \mathcal{S}$, then set $E = S_i - S_j$ and go to (IV).
 (II) $\mathcal{A}(\alpha) :=$ BasisEnvAlgebra($\mathcal{S}(\alpha), \mathbb{F}_{q^\nu}$) $= \{A_1(\alpha), \ldots, A_d(\alpha)\}$.
      Let $\mathcal{A}$ be the canonical pre-image $\{A_1, \ldots, A_d\}$ of $\mathcal{A}(\alpha)$.
(III) If there exist $A_i \in \mathcal{A}$ and $S_j \in \mathcal{S}$ such that $A_i S_j \neq \sum_{k=1}^{d} a_k A_k$, where $a_k \in \mathbb{F}_{q^\nu}$ and $A_i(\alpha)S(\alpha) =$
      $\sum_{k=1}^{d} a_k A_k(\alpha)$, then set $E = \nu A_i S_j - \sum_{k=1}^{d} \mathrm{tr}(a_k) A_k$;
      else return 'true'.
 (IV) $U_1 :=$ ModuleViaNullspace($\mathcal{S}, E$).
      If $U_1 = \{0\}$ then return 'false';
      else let $\rho = \rho_{U_1}$, $U_2 = V/U_1$,
          for $k = 1, 2$ do
              $\mathcal{A} := \{\rho(A_1)|_{U_k}, \ldots, \rho(A_d)|_{U_k}\}$, $\mathcal{S} := \{\rho(S_1)|_{U_k}, \ldots, \rho(S_r)|_{U_k}\}$, go to (III).
```

At any stage of IsFiniteMatGroupFuncFF, we test finiteness of constituents $G|_U$ of G in block triangular form. In looping back to step (III) from step (IV), the dimension of the G-module U strictly reduces. Thus, eventually the algorithm finds either that all constituents are finite, or that one of them is infinite. In the former case G has a finite homomorphic image whose kernel is a finitely generated unipotent subgroup of $\mathrm{GL}(n, \mathbb{F})$, and so is also finite; in the latter case G is infinite.

The maximum number of iterations of IsFiniteMatGroupFuncFF is $2n$, and its main component BasisEnvAlgebra has cost $O(rn^8)$ finite field operations. The principal difference between IsFiniteMatGroupFuncFF and the simpler alternative IsFiniteCRMatGroupFuncFF for completely reducible input is that the former calls ModuleViaNullspace. The operations carried out over the function field are matrix addition, matrix multiplication, and nullspace and intersection of subspaces. All use $O(n^k)$ field operations where $k \leqslant 3$. For just one indeterminate, admissible α always exist in $\mathbb{F}_{q^{d+1}}$ where d is the largest degree of denominators in entries of the matrices in $\mathcal{S}$; a similar estimate holds for $m > 1$. In practice, admissible alpha may be found by repeatedly evaluating the denominator polynomial $f(X_1, \ldots, X_m)$ for X_i chosen in finite extensions of the prime subfield, until a non-root is obtained.

We turn now to the problem of computing the order of a finite subgroup of $\mathrm{GL}(n, \mathbb{F})$. Below we give a simple procedure to solve this problem, based on the next lemma.

Lemma 3.3. *Let $\mathcal{M}$ be a finite subset of* $\mathrm{Mat}(n, \mathbb{F})$. *There are infinitely many admissible $\alpha = (\alpha_1, \ldots, \alpha_m)$, $\alpha_i \in \overline{\mathbb{F}}_q$, such that $|\mathcal{M}| = |\mathcal{M}(\alpha)|$. If $m = 1$ then $|\mathcal{M}| = |\mathcal{M}(\alpha)|$ for all but finitely many admissible α.*

Proof. Let $\mathcal{M} = \{M_1, \ldots, M_k\}$. For each pair i, j, where $i < j$, choose a position in which M_i and M_j have different entries, and let d_{ij} be the difference of the entries. Denote by h the product $\prod_{1 \leqslant i < j \leqslant k} d_{ij}$ of all these differences. If $h(\alpha) \neq 0$ then $|\mathcal{M}| = |\mathcal{M}(\alpha)|$. Since there are infinitely many admissible α such that $h(\alpha) \neq 0$, and only finitely many admissible α such that $h(\alpha) = 0$ if $m = 1$, the result follows. □

Corollary 3.4. *Let $G \leqslant \mathrm{GL}(n, \mathbb{F})$ be finite. There are infinitely many admissible α such that $|G| = |G(\alpha)|$ and $|\langle G \rangle_{\mathbb{F}_q}| = |\langle G(\alpha) \rangle_{\mathbb{F}_q}|$. If $m = 1$ then $|G| = |G(\alpha)|$ and $|\langle G \rangle_{\mathbb{F}_q}| = |\langle G(\alpha) \rangle_{\mathbb{F}_q}|$ for all but finitely many admissible α.*

Remark 3.5. It is not true that if G is finite then there are infinitely many admissible α such that $|\langle G\rangle_{\mathbb{F}_{q^\nu}}| = |\langle G(\alpha)\rangle_{\mathbb{F}_{q^\nu}}|$. Indeed $\dim_{\mathbb{F}_{q^\nu}}\langle G(\alpha)\rangle_{\mathbb{F}_{q^\nu}}$ may be less than $\dim_{\mathbb{F}_q}\langle G(\alpha)\rangle_{\mathbb{F}_q}$ for every admissible α. For example, consider the subgroup G of $\mathrm{GL}(2, \mathbb{F}_2(X))$ generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & X \\ 0 & 1 \end{pmatrix}$. For all $\alpha \in \bar{\mathbb{F}}_2$ we have $\dim_{\mathbb{F}_2(\alpha)}\langle G\rangle_{\mathbb{F}_2(\alpha)} = 3$, whereas $\dim_{\mathbb{F}_2(\alpha)}\langle G(\alpha)\rangle_{\mathbb{F}_2(\alpha)} = 2$.

By Corollary 3.4, if G is finite and $m = 1$, then there is a positive integer δ such that φ_α is an isomorphism on $\langle G\rangle_{\mathbb{F}_q}$ whenever $\alpha \in \bar{\mathbb{F}}_q \setminus \mathbb{F}_{q^\delta}$. As such δ may be impracticably large, our implementation of the following algorithm uses the intrinsic random selection function in MAGMA.

```
SizeFiniteMatGroupFuncFF($\mathcal{S}$)
Input: $\mathcal{S} \subseteq \mathrm{GL}(n, \mathbb{F})$ such that $G = \langle \mathcal{S}\rangle$ is finite.
Output: $|G|$.

 (I) Select an $\mathcal{S}$-admissible $\alpha \in \bar{\mathbb{F}}_q^{(m)}$.
(II) If IsIsomorphismEnvAlgebras($\mathcal{S}, \alpha, 1$) = 'true' then return $|G(\alpha)|$;
     else replace $\bar{\mathbb{F}}_q^{(m)}$ by $\bar{\mathbb{F}}_q^{(m)} \setminus \{\alpha\}$ and go to (I).
```

We end this section with some comments on SizeFiniteMatGroupFuncFF. Recall that $\dim_{\mathbb{F}_q}\langle G\rangle_{\mathbb{F}_q}$ may depend exponentially on n. However, sometimes we can replace $(\mathcal{S}, \alpha, 1)$ by $(\mathcal{S}, \alpha, \nu)$ in step (II) above, thereby bringing the relevant dimension back to no more than n^2. For instance, this is valid if G is cyclic or completely reducible. However, in general we cannot make this modification (cf. Remark 3.5).

Notice that SizeFiniteMatGroupFuncFF constructs an isomorphic copy of $G \leqslant \mathrm{GL}(n, \mathbb{F})$ defined over a finite field. We can use this copy and machinery for matrix groups over finite fields to answer other questions about G.

4. Deciding finiteness of nilpotent matrix groups

In this section we develop a specialized algorithm to decide finiteness of nilpotent subgroups of $\mathrm{GL}(n, \mathbb{F})$. We remove the limitation of [5, Section 4.3] that the ground field is perfect. Our algorithm represents an improvement of the positive characteristic finiteness testing algorithm in [5], including a more efficient transfer to the completely reducible case. One important application is to decide whether a single element g (equivalently, subgroup $\langle g\rangle$) of $\mathrm{GL}(n, \mathbb{F})$ has finite order.

For the rest of this section, $G \leqslant \mathrm{GL}(n, \mathbb{F})$ is nilpotent. We let g_s and g_u denote respectively the diagonalizable and unipotent parts of $g \in \mathrm{GL}(n, \mathbb{F})$. That is, g_s and g_u are the unique matrices such that $g_s \in \mathrm{GL}(n, \bar{\mathbb{F}})$ is diagonalizable, $g_u \in \mathrm{GL}(n, \bar{\mathbb{F}})$ is unipotent, and $g = g_s g_u = g_u g_s$.

Lemma 4.1. *If $g \in \mathrm{GL}(n, \mathbb{F})$ has finite order then g_s and g_u are both in $\langle g\rangle$.*

Proof. Cf. [11, Corollary 1, p. 135]. □

Define $G_s = \langle (S_1)_s, \ldots, (S_r)_s\rangle$ and $G_u = \langle (S_1)_u, \ldots, (S_r)_u\rangle$. The next result follows from part of [11, Proposition 3, pp. 136–137] (which does not require that the ground field be perfect).

Lemma 4.2.

(i) *The maps defined by $g \mapsto g_s$ and $g \mapsto g_u$ for $g \in G$ are homomorphisms; thus $G_s = \{g_s \mid g \in G\}$ and $G_u = \{g_u \mid g \in G\}$.*
(ii) *$G \leqslant G_s \times G_u$.*

Lemma 4.3. *G is finite if and only if G_s is finite.*

Proof. By Lemma 4.2(i), G_s is finite if G is finite. As a finitely generated periodic matrix group, G_u is finite. Hence if G_s is finite then G is finite by Lemma 4.2(ii). □

Let γ be the positive integer such that $p^{\gamma-1} < n \leqslant p^{\gamma}$. By [12, p. 192], p^{γ} is the maximum order of a unipotent element of $\mathrm{GL}(n, \mathbb{F})$. Define $\mathcal{S}^{p^{\gamma}} = \{S_i^{p^{\gamma}} \mid 1 \leqslant i \leqslant r\}$ and $G^{p^{\gamma}} = \langle \mathcal{S}^{p^{\gamma}} \rangle$.

Lemma 4.4.

(i) *G is finite if and only if $G^{p^{\gamma}}$ is finite.*
(ii) *If G is finite then $G^{p^{\gamma}} = G_s$ is completely reducible.*

Proof. (i) Certainly $G^{p^{\gamma}} \leqslant G$ is finite if G is finite. Suppose that $G^{p^{\gamma}}$ is finite. Then each S_i has finite order, so $(S_i)_s$ has order coprime to p. Thus $(S_i)_s \in \langle (S_i)_s^{p^{\gamma}} \rangle$. Since $(S_i)_s^{p^{\gamma}} \in \langle S_i^{p^{\gamma}} \rangle$ by Lemma 4.1, we have $G_s \leqslant G^{p^{\gamma}}$, and so G_s is finite. Lemma 4.3 now completes the proof of this item.

(ii) If G is finite then $G_s \leqslant G^{p^{\gamma}}$. Further, $G^{p^{\gamma}} \leqslant G_s$ since each generator of the nilpotent group $G^{p^{\gamma}} \leqslant G$ has trivial unipotent part (by the choice of γ). □

Lemma 4.4 establishes correctness of the following algorithm to decide finiteness of nilpotent subgroups of $\mathrm{GL}(n, \mathbb{F})$.

```
IsFiniteNilpotentMatGroupFuncFF($\mathcal{S}$)
Input: a finite subset $\mathcal{S}$ of $\mathrm{GL}(n, \mathbb{F})$ such that $G = \langle \mathcal{S} \rangle$ is nilpotent.
Output: 'true' if $G$ is finite; 'false' otherwise.

(I) $\mathcal{S}^{p^{\gamma}} := \{S_i^{p^{\gamma}} \mid 1 \leqslant i \leqslant r\}$.
(II) Return IsFiniteCRMatGroupFuncFF($\mathcal{S}^{p^{\gamma}}$).
```

For nilpotent input, `IsFiniteNilpotentMatGroupFuncFF` is superior to `IsFiniteMatGroupFuncFF`, because it immediately reduces to the completely reducible case.

`IsFiniteNilpotentMatGroupFuncFF` may be further refined. Rather than computing a basis of an enveloping algebra in step (II), it suffices to test whether φ_α has trivial kernel on $G^{p^{\gamma}}$. A practical method to do this is given at the end of [5, Section 4.2]. Likewise, computing orders can be made more efficient for nilpotent input. A specialized method to compute the order of a nilpotent subgroup of $\mathrm{GL}(n, q)$ is implemented in Nilmat [4], and may be used in step (II) of `SizeFiniteMatGroupFuncFF`.

5. Implementation and performance

Implementations of our algorithms are publicly available in Magma. In this section we report on their performance and dependence on the main input parameters: the degree n, the number of generators r, and size q of the coefficient field. We also investigated how runtimes vary with the degrees, coefficients and number of summands of polynomials appearing in matrix entries.

The experiments reported in Table 1 were undertaken on a 3.0 GHz machine with 4 GB RAM running Magma V2.15-10.

As tests, we chose groups with extremal properties, that pass through all stages of each algorithm. The column 'Runtime.1' in Table 1 lists the CPU time in seconds of `IsFiniteMatGroupFuncFF` for input G_{ij}. The column 'Runtime.2' lists the time for `IsFiniteNilpotentMatGroupFuncFF` when G_{ij} is nilpotent. Note that the G_{i1} are finite and the G_{i2} are infinite for $1 \leqslant i \leqslant 4$.

Polynomials in the matrix entries of G_{1j}, G_{2j} have degrees up to 1000, and many summands with large coefficients. The G_{1j} are absolutely irreducible: G_{11} is a conjugate of $\mathrm{GL}(40, 5^7)$ in $\mathrm{GL}(40, \mathbb{F}_{5^7}(X))$, whereas G_{12} is generated by G_{11} and infinite order matrices in $\mathrm{SL}(40, \mathbb{F}_{5^7}(X))$. Testing each group necessitates computing an algebra basis of maximal size $40^2 = 1600$ in $\mathrm{Mat}(40, 5^7)$. The

Table 1

Group	n	r	q	Runtime.1	Runtime.2
G_{11}	40	2	5^7	1646	–
G_{12}	40	10	5^7	1124	–
G_{21}	54	20	29^4	806	–
G_{22}	54	23	29^4	474	–
G_{31}	36	520	7^8	2506	113
G_{32}	36	522	7^8	252	20
G_{41}	100	1	3^{12}	423	16
G_{42}	100	1	3^{12}	8	4

Table 2

Group	n	r	q	Order	Runtime
H_1	20	3	17	$20!2^{80}$	33
H_2	40	24	3^{10}	$5^{22}7^6$	56
H_3	24	16	7^2	$3^45^47^3$	233
H_4	40	1	5^{10}	5^3	230

performance of both `IsFiniteMatGroupFuncFF` and `IsFiniteCRMatGroupFuncFF` is essentially identical for this input.

The G_{2j} have non-trivial unipotent normal subgroups, and so are not completely reducible. The group G_{21} is the Kronecker product of a conjugate of $\mathrm{GL}(6, 29^4)$ in $\mathrm{GL}(6, \mathbb{F}_{29^4}(X))$ with a 10-generator unipotent subgroup of $\mathrm{GL}(9, \mathbb{F}_{29^4}(X))$. The group G_{22} is generated by G_{21} and infinite order matrices of the form $g \otimes I_9$, where g is an upper triangular element of $\mathrm{SL}(6, \mathbb{F}_{29^4}(X))$.

The G_{3j} are nilpotent and not completely reducible. The group G_{31} is the Kronecker product of a 3-dimensional unipotent group with a 12-dimensional completely reducible nilpotent group over $\mathbb{F}_{7^8}(X)$. Specifically, the latter group is a conjugate of a 2×2 block diagonal group, whose blocks are a Sylow 3-subgroup and a Sylow 5-subgroup of $\mathrm{SL}(6, 7^8)$. The group G_{32} is generated by G_{31} and infinite order diagonal matrices of the form $g \otimes I_{18}$, where $g \in \mathrm{SL}(2, \mathbb{F}_{7^8}(X))$.

The G_{4j} are cyclic. The group G_{41} is generated by $h_1 \otimes h$, where $h, h_1 \in \mathrm{GL}(10, \mathbb{F}_{3^{12}}(X))$, h is unipotent, and h_1 is a conjugate of a randomly chosen $3'$-element of $\mathrm{GL}(10, 3^{12})$. Also $G_{42} = \langle h_2 \otimes h \rangle$ where h_2 is a lower triangular element of $\mathrm{SL}(10, \mathbb{F}_{3^{12}}(X))$. Comparison of the last two columns of Table 1 for G_{3j} and G_{4j} demonstrates the superiority of `IsFiniteNilpotentMatGroupFuncFF` for nilpotent input.

The performance of `SizeFiniteMatGroupFuncFF` depends on the algorithm used to determine the order of a matrix group defined over a finite field. MAGMA uses the (random) Schreier–Sims algorithm [7, Section 7.8]. In Table 2 we report on using `SizeFiniteMatGroupFuncFF` to compute the orders of the following groups over a univariate function field: H_1 is a conjugate of the full monomial subgroup of $\mathrm{GL}(20, 17)$, H_2 and H_3 are nilpotent groups constructed in the same manner as G_{31} (H_2 but not H_3 is completely reducible), and H_4 is cyclic unipotent.

References

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

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

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

[4] A.S. Detinko, B. Eick, D.L. Flannery, Nilmat — Computing with nilpotent matrix groups. A refereed GAP 4 package, see http://www.gap-system.org/Packages/nilmat.html, 2007.

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

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

[7] Derek F. Holt, Bettina Eick, Eamonn A. O'Brien, Handbook of Computational Group Theory, Chapman & Hall/CRC, London, 2005.

[8] B. Huppert, N. Blackburn, Finite Groups II, Springer, 1982.
[9] G. Ivanyos, Deciding finiteness for matrix semigroups over function fields over finite fields, Israel J. Math. 124 (2001) 185–188.
[10] D.N. Rockmore, K.-S. Tan, R. Beals, Deciding finiteness for matrix groups over function fields, Israel J. Math. 109 (1999) 93–116.
[11] D. Segal, Polycyclic Groups, Cambridge University Press, Cambridge, 1983.
[12] D.A. Suprunenko, Matrix Groups, Transl. Math. Monogr., vol. 45, Amer. Math. Soc., Providence, RI, 1976.