London Mathematical Society ISSN 1461–1570

ON DECIDING FINITENESS FOR MATRIX GROUPS OVER FIELDS OF POSITIVE CHARACTERISTIC

A. DETINKO

Abstract

We consider the development of algorithms for deciding whether a finitely generated matrix group over a field of positive characteristic is finite. A deterministic algorithm for deciding the finiteness is presented for the case of a field of transcendence degree one over a finite field.

1. *Introduction*

This paper deals with the development of algorithms for matrix groups. Currently, this is one of the most active areas of computational group theory (see, for example, [8]). Early algorithms for computing with matrix groups used the induced actions of suitable subgroups of these groups on carefully chosen sets of vectors and subspaces of the underlying vector space. Such an approach gives rise to algorithms with running times that depend exponentially on the input size. Moreover, in [8, p. 677] some basic ingredients have been described; these are crucial for the efficient handling of permutation groups, but are lost when dealing with matrix groups. These problems have motivated a new phase in the development of algorithms for matrix groups (historical remarks can be found in [8]). Most of the effort has been concentrated on various recognition algorithms that detect certain properties of matrix groups given by a set of generating matrices. For potentially infinite matrix groups, one of the most fundamental problems is the finiteness problem; that is, the problem of whether a finitely generated subgroup G of the general linear group $GL(n, F)$ over a field F is finite. An efficient algorithm for deciding finiteness is a necessary component of any library of algorithms to be used to determine the structure of finitely generated groups (see [1]).

In the case of number fields, polynomial-time randomized and deterministic algorithms for solving the finiteness problem have been described in [1]. One of these algorithms (Las-Vegas) has been implemented in the GAP group theory language [6]. For a function field $F = \mathcal{F}(t_1, \dots, t_l)$, the problem is considered in [7] (here, $t_1, \dots, t_l$ are independent indeterminates). A polynomial-time algorithm is presented in [7] for the case where $\mathcal{F}$ is a number field. This algorithm either recognizes the group as infinite, or constructs an isomorphic matrix group over $\mathcal{F}$ (not necessarily of the same dimension). The problem is thereby reduced to the case of groups over the number field. When $\mathcal{F}$ is the q-element field $\mathbf{F}_q$, the situation is very different, and much more complicated. In [7], two deterministic algorithms for deciding finiteness over $F = \mathbf{F}_q(t)$ are described. Both of these algorithms rely on constructing, from the $\mathbf{F}_q$-algebra generated by G, a chain of matrices that are linearly independent over $\mathbf{F}_q$. An exponential upper bound on the dimension of such an algebra, obtained in [7, Theorem 3.3], suggests that such an approach can provide only exponential-time algorithms.

Received 30 October 2000, revised 16 March 2001*; published 19 April 2001*.
2000 Mathematics Subject Classification 20C40, 20G25

https://doi.org/10.1112/S1461157000000802 Published online by Cambridge University Press

These notes represent a contribution to the study of the finiteness problem for finitely generated subgroups of $GL(n, F)$, where $\operatorname{char} F > 0$. Our main objective is to design algorithms that solve the problem by using polynomially many field operations. We assume that the reader is familiar with the elementary notions and facts used in the theory of matrix groups and algebras; readers who are new to this field are referred to [9].

2. *Preliminaries and background*

Let F be a field of characteristic $p > 0$, and let F_a be the field of elements of F which are algebraic over the p-element subfield of F. Throughout the paper, $\mathbf{F}_q$ will stand for the q-element field. We will use the notation $M(n \times m, F)$ to denote the F-module of $n \times m$ matrices with entries in F, and $M(n, F)$ for $M(n \times n, F)$.

Let $\mathcal{A}$ be an associative finite-dimensional algebra over F with an identity element. An element $x \in \mathcal{A}$ is *nilpotent* if $x^m = 0$ for some positive integer m. Similarly, $x \in \mathcal{A}$ is *strongly nilpotent*, if xy is nilpotent for every $y \in \mathcal{A}$. The *radical* $\operatorname{Rad}(\mathcal{A})$ of $\mathcal{A}$ is the set of strongly nilpotent elements of $\mathcal{A}$. Let L be a set of matrices of $M(n, F)$, and let Π be a subfield of F. The *enveloping algebra* $\operatorname{env}_{\Pi}(L)$ of L over Π is a Π-algebra generated by L.

Let $GL(n, F)$ be the group of invertible $n \times n$ matrices over F (the general linear group). Denote by F^n the vector space of column vectors of length n on which $GL(n, F)$ acts. Recall that a subgroup $G \subset GL(n, F)$ is *irreducible* if there is no non-trivial proper subspace of F^n that is invariant under G. Otherwise, G is said to be *reducible*. If F^n is a direct sum of G-invariant subspaces on which G acts irreducibly then G is called *completely reducible*.

If n is a positive integer and $n = n_1 + \cdots + n_d$, then denote $(n_1, \ldots, n_d)$ by $\overline{n}$. Let $T(\overline{n}, F)$ be the group of block upper triangular matrices $X = (X_{ij}) \in GL(n, F)$, where $X_{ij} \in M(n_i \times n_j, F)$, $i < j$, $X_{ii} \in GL(n_i, F)$ and $X_{ij} = 0$ for $i > j$. Define $T_a(\overline{n}, F)$ as the subgroup of matrices $X = (X_{ij}) \in T(\overline{n}, F)$ such that $X_{ii} \in GL(n_i, F_a)$, $1 \leqslant i \leqslant d$. Denote by φ a homomorphism $T(\overline{n}, F) \to D(\overline{n}, F)$, where $X \to \overline{X}$ is given by projection on the block-diagonal group $D(\overline{n}, F)$. Given $G \subset T(\overline{n}, F)$, write $\varphi(G)$ as $\overline{G}$. Note that $\overline{G}$ is not necessarily completely reducible.

Our approach is based on the description of periodic subgroups of $GL(n, F)$ given in [10]. *Periodic groups* (that is, groups all elements of which have finite order) are the straightforward generalization of finite groups. Note that by the well-known theorem of I. Schur (see, for example, [9, Theorem 23.5]), periodic matrix groups are locally finite.

Proposition 2.1 ([10]). *Let $G \subset GL(n, F)$ be irreducible. Then G is periodic if and only if G is conjugate to a subgroup of $GL(n, F_a)$.*

Corollary 2.2 ([10]). *Let $G \subset GL(n, F)$. Then G is periodic if and only if G is conjugate to a subgroup of $T_a(\overline{n}, F)$ for some $\overline{n}$. In particular, a finitely generated group G is finite if and only if G is conjugate to a subgroup of $T_a(\overline{n}, F)$.*

Note that [7, Theorem 3.2 and Corollary 3.6] follow directly from Corollary 2.2.

Lemma 2.3. *Let G be a subgroup of $GL(n, F)$. Then G is periodic if and only if G is conjugate to a subgroup $H \subset T(\overline{n}, F)$ such that* $\dim_{F_a}(\operatorname{env}_{F_a}(\overline{H})) \leqslant n^2$.

Proof. If G is periodic, then by Corollary 2.2, subgroup G is conjugate to a subgroup $H \subset T_a(\overline{n}, F)$. Hence $\dim_{F_a}(\operatorname{env}_{F_a}(\overline{H})) \leqslant n^2$. Conversely, let $hGh^{-1} = H \subset T(\overline{n}, F)$ for

https://doi.org/10.1112/S1461157000000802 Published online by Cambridge University Press

some $h \in GL(n, F)$, and $\dim_{F_a}(\mathrm{env}_{F_a}(\overline{H})) \leqslant n^2$. Suppose that H contains an element g of infinite order. Then the order of $\varphi(g) = \overline{g}$ is also infinite. Hence the matrices $\overline{g}, \overline{g}^2, \ldots, \overline{g}^m$ are linearly independent over F_a for any positive integer m; that is, $\dim_{F_a}(\mathrm{env}_{F_a}(\overline{H}))$ is infinite. From this contradiction it follows that G is periodic. □

Corollary 2.4. *Let G be a finitely generated subgroup of $GL(n, F)$. Then G is finite if and only if G is conjugate to a subgroup $H \subset T(\overline{n}, F)$ such that* $\dim_{F_a}(\mathrm{env}_{F_a}(\overline{H})) \leqslant n^2$.

Proof. The corollary follows directly from the abovementioned theorem of I. Schur [9, Theorem 23.5]. □

Lemma 2.5. *Let $G \subset GL(n, F)$ be completely reducible. Then G is periodic if and only if* $\dim_{F_a}(\mathrm{env}_{F_a}(G)) \leqslant n^2$.

Proof. The lemma follows immediately from Lemma 2.3. □

Direct application of the above statements provides the following approach to the problem of deciding finiteness for a finitely generated subgroup $G \subset GL(n, F)$.

(i) Construct a representation $\rho : G \to T(\overline{n}, F)$ such that the projection $\overline{\rho(G)}$ is completely reducible.

(ii) Calculate $d_a = \dim_{F_a}(\mathrm{env}_{F_a}(\overline{\rho(G)}))$.

By Lemma 2.5, if G is finite then $d_a \leqslant n^2$; therefore [2, Lemma 4.1] implies that the dimension of $\mathrm{env}_{F_a}(\overline{\rho(G)})$ can be calculated in polynomial time. If G is infinite, then by [2, Lemma 4.1] we can construct in polynomial time more than n^2 matrices of $\mathrm{env}_{F_a}(\overline{\rho(G)})$, which are linearly independent over F_a.

To construct the representation ρ we may use the correspondence between the structure of $\mathrm{env}_F(G)$ and the action of G on $V = F^n$. Let R be the radical of $\mathrm{env}_F(G)$. Then

$$V \supset RV \supset \cdots \supset R^{d-1}V \supset \{0\} \qquad (1)$$

is the chain of G-modules, where $R^{d-1} \neq 0$ and $R^d = 0$, for $d \leqslant n$ (see [9, § 13]).

Chain (1) defines the representation $\rho : G \to T(\overline{n}, F)$ where $\overline{n} = (n_1, \ldots, n_d)$ and $n_i = \dim R^{i-1}V/R^iV$, for $1 \leqslant i \leqslant d$. From [9, § 13] it follows that the group $\overline{\rho(G)}$ is completely reducible, as required.

Let $F = \mathbf{F}_q(t_1, \ldots, t_l)$. Then by [3, Corollary 3.4.6], the radical of $\mathrm{env}_F(G)$ can be found in deterministic polynomial time. This shows that finiteness for matrix groups over the function field $\mathbf{F}_q(t_1, \ldots, t_l)$ is decidable in polynomial time.

The main difficulty with this approach lies in the calculation of $\mathrm{Rad}(\mathrm{env}_F(G))$. In the next section we shall describe a more efficient approach, that relies on calculating only some nonzero elements of $\mathrm{Rad}(\mathrm{env}_F(G))$. Here we consider the case of $\mathbf{F}_q(t)$, although our results can be extended to $\mathbf{F}_q(t_1, \ldots, t_l)$.

3. *Algorithms for testing the finiteness of matrix groups over $\mathbf{F}_q(t)$*

Let $F = \mathbf{F}_q(t)$, and let $\overline{F}$ and $\overline{\mathbf{F}}_q$ be the algebraic closures of F and $\mathbf{F}_q$ respectively. If $h = h(t) = (h_{ij}(t)) \in M(n, \overline{F})$, and if α is an element of $\overline{\mathbf{F}}_q$, then define the matrix $\Psi_\alpha(h)$ as $\Psi_\alpha(h) = (h_{ij}(\alpha)) \in M(n, \overline{\mathbf{F}}_q)$; that is, $\Psi_\alpha(h)$ is obtained by evaluating all elements of h at α (assuming that they are defined). Denote by $\mathbf{F}_q(\alpha)$ the extension of $\mathbf{F}_q$ obtained by adjoining the element α, and write $|\mathbf{F}_q(\alpha)/\mathbf{F}_q|$ for the degree of $\mathbf{F}_q(\alpha)$ over $\mathbf{F}_q$.

https://doi.org/10.1112/S1461157000000802 Published online by Cambridge University Press

Throughout this section $S = \{S_1, \dots, S_r\}$, $S_k = (s_{ij}^{(k)}) \in GL(n, F)$, and $G = < S >$ is the subgroup of $GL(n, F)$ generated by S.

Lemma 3.1. *Let α be an element of $\overline{\mathbf{F}}_q$ such that matrices $\Psi_\alpha(S_i)$ are defined for all $1 \leqslant i \leqslant r$. If G is finite, then*

$$\Psi_\alpha : G \to GL(n, \overline{\mathbf{F}}_q), \qquad h(t) \to h(\alpha)$$

is a homomorphism of G into $GL(n, \overline{\mathbf{F}}_q)$.

Proof. It suffices to show that $\Psi_\alpha(h(t))$ is defined for each $h = h(t) \in G$, because in this case it is clear that $\Psi_\alpha(hg) = \Psi_\alpha(h)\Psi_\alpha(g)$ and $\Psi_\alpha(h^{-1}) = (\Psi_\alpha(h))^{-1}$, for $g \in G$.

Let $m = m(t)$ be the least common multiple of the denominators of $s_{ij}^{(k)}$, where $1 \leqslant k \leqslant r$ and $1 \leqslant i, j \leqslant n$. Since $\Psi_\alpha(S_k)$ is defined for all k, we have $m(\alpha) \neq 0$. The group G is finite, and therefore $h = S_{i_1}^{m_1} \cdot \dots \cdot S_{i_r}^{m_r}$, where m_i are nonnegative integers and $1 \leqslant i \leqslant r$. Hence $h = m^{-l}(t)h_0(t)$, where l is a positive integer and $h_0(t) \in GL(n, \mathbf{F}_q[t])$. Thus $\Psi_\alpha(h)$ is defined, as required. □

Let $\alpha \in \overline{\mathbf{F}}_q$ be defined as in Lemma 3.1. Note that such an α exists. For example, if the degree of the extension $\mathbf{F}_q(\alpha)/\mathbf{F}_q$ is greater than the degrees of the denominators of $s_{ij}^{(k)}$, where $1 \leqslant k \leqslant r$ and $1 \leqslant i, j \leqslant n$, then α satisfies conditions of Lemma 3.1.

Let $P = \mathbf{F}_q(\alpha)$. If G is finite, then Lemma 3.1 implies that $\Psi_\alpha : \mathrm{env}_P(G) \to M(n, P)$, $h \to \Psi_\alpha(h)$ is a homomorphism of algebra $\mathrm{env}_P(G)$ into $M(n, P)$.

Proposition 3.2. *If G is finite, then* $\ker \Psi_\alpha \subset \mathrm{Rad}(\mathrm{env}_P(G))$.

Proof. To prove the proposition, it suffices to show that each element $h \in \ker \Psi_\alpha$ is nilpotent. By Corollary 2.2, $\mathrm{env}_P(G)$ is conjugate to a subalgebra of $\mathrm{env}_P(T_a(\overline{n}, F))$. Hence h is conjugate to a matrix of $\mathrm{env}_P(T_a(\overline{n}, F))$. Consequently, all the coefficients of the characteristic polynomial $f(x)$ of h are contained in P. Hence $f(x)$ is the characteristic polynomial of the matrix $\Psi_\alpha(h)$. From $h \in \ker \Psi_\alpha$, it follows that $\Psi_\alpha(h) = 0$; therefore $f(x) = x^n$. Thus $h^n = 0$; that is, h is nilpotent. □

Corollary 3.3. *If G is finite, then* $\ker \Psi_\alpha \subset \mathrm{Rad}(\mathrm{env}_{P(t)}(G))$.

Proof. By Proposition 3.2, the kernel $\ker \Psi_\alpha$ is a nilpotent ring; therefore [**4**, Chapter 8, § 5, Theorem 1] implies that the linear span of $\ker \Psi_\alpha$ over $P(t)$ is a nilpotent ideal of $\mathrm{env}_{P(t)}(G)$. Thus $\ker \Psi_\alpha \subset \mathrm{Rad}(\mathrm{env}_{P(t)}(G))$, as desired. □

Now let us choose an element $\alpha \in \overline{\mathbf{F}}_q$ in the following manner. Let c be the largest of the degrees of the denominators of $s_{ij}^{(k)}$, where $1 \leqslant k \leqslant r$ and $1 \leqslant i, j \leqslant n$. If $c = 0$ (that is, if $S_i \in GL(n, \mathbf{F}_q[t])$ for $1 \leqslant i \leqslant r$), then let $\alpha \in \mathbf{F}_q$ (for example, $\alpha = 0$). If $c > 0$ and $p \nmid c + 1$, then let α be an element of $\overline{\mathbf{F}}_q$ such that $\mathbf{F}_q(\alpha) = \mathbf{F}_{q^{c+1}}$. If $c > 0$ and $p \mid c + 1$, then let α be an element of $\overline{\mathbf{F}}_q$ such that $\mathbf{F}_q(\alpha) = \mathbf{F}_{q^{c+2}}$. Denote $\mathbf{F}_q(\alpha)$ as above by P, and define η as the degree of the extension $P/\mathbf{F}_q$. Note that if $S_i \in GL(n, \mathbf{F}_q[t])$, where $1 \leqslant i \leqslant r$, then $P = \mathbf{F}_q$ and $\eta = 1$.

Define the matrices $J = J(A_k)$ and $J' = J'(A_k)$ as follows. Let

$$A_1, \dots, A_k \tag{2}$$

be matrices of $\mathrm{env}_P(G)$ that are linearly independent over P, such that

$$\Psi_\alpha(A_1), \dots, \Psi_\alpha(A_k) \in M(n, P) \tag{3}$$

are linearly dependent over P; that is

$$\Psi_\alpha(A_k) = \sum_{i=1}^{k-1} \alpha_i \Psi_\alpha(A_i) \tag{4}$$

for some $\alpha_i \in P$.

Denote by $J(A_k)$ the matrix $J(A_k) = A_k - \sum_{i=1}^{k-1} \alpha_i A_i \in \operatorname{env}_P(G)$, and define $J'(A_k) = \eta A_k - \sum_{i=1}^{k-1} \operatorname{tr}(\alpha_i) A_i \in \operatorname{env}_{\mathbf{F}_q}(G)$, where $\operatorname{tr}(\alpha_i)$ is the trace of $\alpha_i \in P$ over $\mathbf{F}_q$. Note that if $P = \mathbf{F}_q$, then $J = J'$.

Lemma 3.4. *If G is finite, then J is a nonzero element of* $\ker \Psi_\alpha$.

Proof. Since $\Psi_\alpha(J(A_k)) = \Psi_\alpha(A_k - \sum_{i=1}^{k-1} \alpha_i A_i) = \Psi_\alpha(A_k) - \sum_{i=1}^{k-1} \alpha_i \Psi_\alpha(A_i)$, equation (4) implies that $\Psi_\alpha(J(A_k)) = 0$; that is, $J(A_k) \in \ker \Psi_\alpha$. Matrices (2) are linearly independent over P, and therefore $J(A_k) \neq 0$. □

Corollary 3.5. *If G is finite and $A_i \in \operatorname{env}_{\mathbf{F}_q}(G)$, then $J'(A_k)$ is a nonzero element of* $\operatorname{Rad}(\operatorname{env}_F(G))$.

Proof. Let σ be an automorphism of P over $\mathbf{F}_q$ which generates the Galois group $\operatorname{Gal}(P/\mathbf{F}_q)$. We shall also denote by σ the extension of σ to $P(t)$ such that $\sigma(t) = t$. Since $A_i \in M(n, F)$, we have $\sigma^j(A_i) = A_i$, for $1 \leqslant j \leqslant \eta$, and hence $\Psi_{\sigma^j(\alpha)}(A_i) = \sigma^j(\Psi_\alpha(A_i))$. Thus

$$\Psi_{\sigma^j(\alpha)}(A_k) = \sigma^j\big(\Psi_\alpha(A_k)\big) = \sigma^j\left(\sum_{i=1}^{k-1} \alpha_i \Psi_\alpha(A_i)\right) = \sum_{i=1}^{k-1} \sigma^j(\alpha_i) \Psi_{\sigma^j(\alpha)}(A_i).$$

Lemma 3.4 implies that the matrix

$$B_{\sigma^j} = A_k - \sum_{i=1}^{k-1} \sigma^j(\alpha_i) A_i \tag{5}$$

is contained in $\ker \Psi_{\sigma^j(\alpha)}$, for $1 \leqslant j \leqslant \eta$; that is, by Corollary 3.3, $B_{\sigma^j} \in \operatorname{Rad}(\operatorname{env}_{P(t)}(G))$. Hence, by equation (5) it follows that

$$\sum_{j=1}^{\eta} B_{\sigma^j} = \eta A_k - \sum_{i=1}^{k-1} \operatorname{tr}(\alpha_i) A_i = J'(A_k) \in \operatorname{Rad}(\operatorname{env}_{P(t)}(G)).$$

Since $J'(A_k) \in M(n, F)$, we have $J'(A_k) \in \operatorname{Rad}(\operatorname{env}_F(G))$. Finally, note that $J'(A_k) \neq 0$ because matrices (2) are linearly independent over $\mathbf{F}_q$ and $p \nmid \eta$. □

Lemma 3.6. *Let $A_1, \ldots, A_k \in \operatorname{env}_P(G)$ be linearly dependent over $P(t)$. Then $\Psi_\alpha(A_1), \ldots, \Psi_\alpha(A_k)$ are linearly dependent over P.*

Proof. Let

$$A_k = \sum_{i=1}^{k-1} \alpha_i(t) A_i, \qquad \alpha_i(t) \in P(t). \tag{6}$$

Let β be an element of $\overline{\mathbf{F}}_q$ such that $\alpha_i(\beta)$ are defined for each $\alpha_i(t)$, where $1 \leqslant i \leqslant k-1$, and p does not divide the degree τ of the extension $P(\beta)/P$. By [5, Theorem 2.23], we can choose β in such a way that $\mathrm{tr}(\beta) = \alpha$, where $\mathrm{tr}(\beta)$ is the trace of β over P. Let $< \delta > = \mathrm{Gal}(P(\beta)/P)$. Then equation (6) implies that

$$\Psi_{\delta^j(\beta)}(A_k) = \sum_{i=1}^{k-1} \delta^j(\beta_i)\Psi_{\delta^j(\beta)}(A_i), \tag{7}$$

where $1 \leqslant j \leqslant \tau$ and $\beta_i = \alpha_i(\beta)$. Since $\mathrm{tr}(\beta) = \alpha$, we have $\sum_{j=1}^{\tau} \Psi_{\delta^j(\beta)}(A_i) = \Psi_\alpha(A_i)$.

Hence the sum of both sides of equation (7) over j will give

$$\Psi_\alpha(A_k) = \sum_{i=1}^{k-1} \mathrm{tr}(\beta_i)\Psi_\alpha(A_i),$$

where $\mathrm{tr}(\beta_i) \in P$. Thus, $\Psi_\alpha(A_1), \ldots, \Psi_\alpha(A_k)$ are linearly dependent over P. □

In particular, Lemma 3.6 implies that in order to construct the matrices $J(A_k)$, it is actually not necessary to calculate $\Psi_\alpha(A_i)$, and to test whether the matrices (3) are linearly dependent over P. Indeed, suppose that matrices (3) are linearly dependent over $P(t)$; that is, that

$$A_k = \sum_{i=1}^{k-1} \alpha_i(t)A_i, \qquad \alpha_i(t) = \frac{\alpha_{1i}(t)}{\alpha_{2i}(t)},$$

where $\alpha_{1i}(t), \alpha_{2i}(t) \in P[t]$ and $1 \leqslant i \leqslant k-1$. If $\alpha_{2i}(\alpha) \neq 0$ for each i, $1 \leqslant i \leqslant k-1$, then it is easy to see that $J(A_k) = A_k - \sum_{i=1}^{k-1} \alpha_i A_i$, where $\alpha_i = \alpha_i(\alpha)$. If $\alpha_{2i}(\alpha) = 0$ for some i, then we can always replace α by another element β from $\overline{\mathbf{F}}_q$ satisfying the conditions of Lemma 3.1 and such that $\alpha_{2i}(\beta) \neq 0$, for $1 \leqslant i \leqslant k-1$ and $p \nmid |\mathbf{F}_q(\beta)/\mathbf{F}_q|$. Since $J'(A_k)$ is always contained in $M(n, F)$, such a replacement causes no extension of the ground field in further calculations.

Thus, if G is finite, then we have constructed a nonzero element of $\mathrm{Rad}(\mathrm{env}_F(G))$.

Now we proceed to construct a nonzero G-module by means of J'. Given a set X of matrices of $M(n, F)$, denote by $\mathrm{kr}X$ the set $\{v \in F^n : g(v) = 0, g \in X\}$. If $B \in \mathrm{env}_F(G)$, denote by $\mathcal{B}$ the right ideal of $\mathrm{env}_F(G)$ generated by B.

Lemma 3.7. *Let $A_1, \ldots, A_m$ be a basis of $\mathrm{env}_F(G)$ such that $\det A_i \neq 0$, for $1 \leqslant i \leqslant m$. If $B \in \mathrm{env}_F(G)$ and $W = \mathrm{kr}B$, then $U = A_1^{-1}(W) \cap \cdots \cap A_m^{-1}(W)$ is a G-invariant subspace of F^n.*

Proof. First prove that $U = \mathrm{kr}\mathcal{B}$. Let $u \in U$; that is, $u = A_i^{-1}(v_i)$ where $v_i \in W$ and $1 \leqslant i \leqslant m$. If h is an element of $\mathcal{B}$, then $h = Bg$ for some $g \in \mathrm{env}_F(G)$. Since $g = \sum_{i=1}^m \alpha_i A_i$, for $\alpha_i \in F$, we have

$$\begin{aligned} h(u) &= Bg(u) &&= \Big(B \sum_{i=1}^m \alpha_i A_i\Big)(u) \\ &= \sum_{i=1}^m \alpha_i BA_i(u) &&= \sum_{i=1}^m \alpha_i BA_iA_i^{-1}(v_i) \\ &= \sum_{i=1}^m \alpha_i B(v_i) &&= 0, \end{aligned}$$

because $v_i \in W$. Thus $u \in \mathrm{kr}\mathcal{B}$; that is, $U \subset \mathrm{kr}\mathcal{B}$.

Conversely, let $v \in \mathrm{kr}\mathcal{B}$; that is, $Bg(v) = 0$ for each $g \in \mathrm{env}_F(G)$. Setting $g = A_i$, we see that $BA_i(v) = 0$; that is, $A_i(v) = u_i \in W$, for $1 \leqslant i \leqslant m$. Consequently, $v = A_i^{-1}(u_i)$ and $v \in \cap_{i=1}^m A_i^{-1}(W)$. Thus $\mathrm{kr}\mathcal{B} \subset U$, and hence $\mathrm{kr}\mathcal{B} = U$.

https://doi.org/10.1112/S1461157000000802 Published online by Cambridge University Press

Finally, we show that U is a G-module. Let $u \in \mathrm{kr}\mathcal{B}$, and let $g \in \mathrm{env}_F(G)$. Since $\mathcal{B}$ is a right ideal of $\mathrm{env}_F(G)$, we have $hg \in \mathcal{B}$ for each $h \in \mathcal{B}$. Hence $hg(u) = h(g(u)) = 0$, and therefore $g(u) \in \mathrm{kr}\mathcal{B}$. Thus, $g(u) \in \mathrm{kr}\mathcal{B}$ for each $u \in \mathrm{kr}\mathcal{B}$ and $g \in \mathrm{env}_F(G)$; that is, $\mathrm{kr}\mathcal{B} = U$ is a G-module. □

Corollary 3.8. *Let $B \in \mathrm{Rad}(\mathrm{env}_F(G))$, and let U be defined as in Lemma 3.7. Then U is a nontrivial G-module.*

Proof. By Lemma 3.7, it suffices to show that $U \neq 0$. Let $R = \mathrm{Rad}(\mathrm{env}_F(G))$. Since $B \in R$, we have $\mathcal{B} \subset R$. Hence $\mathrm{kr}\mathcal{B} \supset \mathrm{kr}R \neq 0$. □

Corollary 3.9. *Let G be irreducible, and let U be defined as in Lemma 3.7. If $U \neq F^n$, then $U = 0$.*

Proof. By Lemma 3.7, subspace U is a G-invariant subspace of F^n. Since G is irreducible, $U = 0$, as required. □

Define the set S^k as follows: $S^1 = S$ and for $k > 1$ let $S^k = \cup_{A \in S} S^{k-1}A$; that is, S^k is a set of products of length k over S. In [1] the following procedure for constructing a basis of $\mathrm{env}_\Pi(S)$, for $\Pi \subset \overline{F}$, is described. Let $A_1 = E_n$ (here E_n is the identity matrix). Suppose that matrices $A_1, \ldots, A_e$, which are linearly independent over Π and satisfy the condition $A_j \in S^k$, where $k \leqslant e-1$ and $1 < j \leqslant e$, have been constructed. If there are $S_i \in S$ and A_j (for $1 \leqslant j \leqslant e$), such that $A_1, \ldots, A_e, A_jS_i$ are linearly independent over Π, then let $A_{e+1} = A_jS_i$. We repeat this process until we reach $e = m$, such that all of the products A_jS_i, for $1 \leqslant j \leqslant m$ and $1 \leqslant i \leqslant r$, are contained in $\mathrm{Span}_\Pi(A_1, \ldots, A_m)$. Then $A_1, \ldots, A_m$ is a basis of $\mathrm{env}_\Pi(S)$. In what follows we denote by $A_1, \ldots, A_m$ the basis of $\mathrm{env}_F(S)$ constructed by this procedure. Let $B \in \mathrm{env}_F(S)$ and let $W = \mathrm{kr}B$. Denote the subspace $A_1^{-1}(W) \cap \cdots \cap A_m^{-1}(W)$ by $\mathrm{Kr}B$.

Based on the results of this section, we develop the following algorithm for testing the finiteness of $G = < S >$.

```
**Input:** $S = \{S_1, \ldots, S_r\}$
**Step 1:** calculate $A_1, \ldots, A_m$, a basis of $\mathrm{env}_F(S)$;
  **if** there are $S_i$ and $A_j$ such that $A_jS_i \notin \mathrm{Span}_{\mathbf{F}_q}(A_1, \ldots, A_m)$
    **then** set $A_{m+1} := A_jS_i$ and proceed to Step 2
    **else** return ‘$G$ is finite’;
**Step 2:** calculate $J' = J'(A_{m+1})$ and the chain $\mathrm{Kr}(J') \subset \cdots \subset \mathrm{Kr}((J')^n)$;
  **if** $\mathrm{Kr}(J') = 0$ or $\mathrm{Kr}((J')^n) \neq F^n$
    **then** return ‘$G$ is infinite’
    **else** calculate $\overline{\rho(S_1)}, \ldots, \overline{\rho(S_r)}$;
Go to Step 1, setting $S := \{\overline{\rho(S_1)}|_{U_i}, \ldots, \overline{\rho(S_r)}|_{U_i}\}$, where $U_i = \mathrm{Kr}((J')^i)/\mathrm{Kr}((J')^{i-1})$, for $1 \leqslant i \leqslant n$.
```

Remark 1. (i) To construct the representation $\rho : G \to T(\overline{n}, F)$, the algorithm calculates the matrix $h \in GL(n, F)$ such that $\rho(G) = hGh^{-1} \in T(\overline{n}, F)$. To avoid an extension of the field P, the algorithm turns $\overline{\rho(S_i)}$ into the form $h^{-1}(\overline{hS_ih^{-1}})h$.

(ii) The algorithm decides the finiteness for each of the groups $\overline{\rho(G)}|_{U_i}$. If, for at least one U_i, the algorithm recognizes $\overline{\rho(G)}|_{U_i}$ as infinite, then it returns ‘G is infinite’. Otherwise, the algorithm recognizes the group as finite.

Note that all the assumptions which are necessary for the feasible calculation by the algorithm of the matrix J' are fulfilled. Indeed, since $A_1, \dots, A_{m+1}$ are linearly independent over $\mathbf{F}_q$ and $A_i \in GL(n, F)$, for $1 \leqslant i \leqslant m+1$, we find that $A_1, \dots, A_{m+1}$ are linearly independent over P. By Lemma 3.6, the matrices $\Psi_\alpha(A_1), \dots, \Psi_\alpha(A_{m+1})$ are linearly dependent over P. Hence J' can be calculated in Step 2. Also note that, since $A_1, \dots, A_{m+1}$ are linearly independent over $\mathbf{F}_q$, the definition of J' implies that $J' \neq 0$.

The algorithm terminates as follows.

Suppose that G is finite. Then Corollary 3.5 implies that J' is an element of $\mathrm{Rad}(\mathrm{env}_F(G))$. By Corollary 3.8, the subspace $\mathrm{Kr}(J')$ is a nontrivial G-module. Since each round reduces the dimension of at least one of the $\overline{\rho(G)}$-modules U_i, Corollary 2.4 implies that in at most n rounds the algorithm constructs matrices $\overline{\rho(S_1)}, \dots, \overline{\rho(S_r)}$ generating the group $\overline{\rho(G)}$ which is conjugate to a subgroup of $GL(n, \mathbf{F}_q)$. Hence, in the next round the algorithm calculates a basis of $\mathrm{env}_{\mathbf{F}_q}(\overline{\rho(G)})$, and terminates after having recognized the group as finite.

Let G be infinite. In contrast to the case of a finite group, it follows from Corollary 2.4 that a matrix $A_{m+1} = A_j S_i \notin \mathrm{Span}_{\mathbf{F}_q}(A_1, \dots, A_m)$ always exists. Hence, in each round the algorithm will be able to calculate J'. If J' is not nilpotent, then $(J')^n \neq 0$, and the algorithm recognizes G as infinite. Suppose that J' is nilpotent. By Lemma 3.7, $\mathrm{Kr}(J')$ is a proper G-invariant subspace (recall that $J' \neq 0$). If $\mathrm{Kr}(J') \neq 0$, then we proceed to the next round. If $\mathrm{Kr}(J') = 0$, then the algorithm terminates with the result that the group is infinite. Note that by Corollary 3.5 and Corollary 3.8 the situation $\mathrm{Kr}(J') = 0$ is possible only for the case of an infinite group. Each round reduces the dimension of at least one of the $\overline{\rho(G)}$-modules U_i; therefore in at most n rounds the algorithm constructs a $\overline{\rho(G)}$-module U_i such that the group $\overline{\rho(G)}|_{U_i}$ is irreducible and infinite. Hence, by Corollary 3.9, the algorithm terminates at the next round after having recognized the group as infinite.

The calculation of the basis $A_1, \dots, A_m$ of $\mathrm{env}_F(G)$ is the key component of this algorithm. Since $m \leqslant n^2$, by [7, p. 110] in order to construct $A_1, \dots, A_m$ we need at most $O(rn^8)$ field operations, in contrast to the algorithms presented in [7].

Note that the construction of the chain of G-modules $\mathrm{Kr}(J') \subset \cdots \subset \mathrm{Kr}((J')^n)$ relies on solving systems of linear algebraic equations, and can be performed by means of Gaussian elimination.

References

1. L. Babai, R. Beals and D. Rockmore, ‘Deciding finiteness of matrix groups in deterministic polynomial time’, *Proc. ISSAC ’93* (ACM Press, 1993) 117–126. 64, 64, 70

2. R. Beals, ‘Algorithms for matrix groups and the Tits alternative’, *Proc. 36th IEEE FOCS* (IEEE, 1995) 593–602. 66, 66

3. G. Ivanyos, ‘Algorithms for algebras over global fields’, Ph.D. Thesis, Hungarian Academy of Science, 1996. 66

4. M. Jakobson, *Structure of rings* (Amer. Math. Soc., Providence, RI, 1956). 67

5. R. Lidl and H. Niederreiter, *Finite fields* (Addison-Wesley, Reading, MA, 1983). 68

6. M. Schönert *et al.*, GAP—*Groups, algorithms and programming*, 5th edn (Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, 1995). 64

7. D. Rockmore, K.-S. Tan and R. Beals, 'Deciding finiteness for matrix groups over function fields', *Israel J. Math.* 109 (1999) 93–116. 64, 64, 64, 64, 65, 71, 71

8. A. Seress, 'An introduction to computational group theory', *Notices Amer. Math. Soc.* 44 (1997) 671–679. 64, 64, 64

9. D. Suprunenko, *Matrix groups*, Trans. Math. Monographs 45 (Amer. Math. Soc., Providence, RI, 1976). 65, 65, 66, 66, 66

10. A. E. Zalesskii, 'Maximal periodic subgroups of the general linear group over a field of positive characteristic', *Vestsı̄ Akad. Navuk BSSR Ser. Fı̄z.-Mat. Navuk*2 (1966) 121–123. 65, 65, 65

A. Detinko das@psu.unibel.by

Department of Applied Mathematics
Polotsk State University
Novopolotsk
Belarus
211440

https://doi.org/10.1112/S1461157000000802 Published online by Cambridge University Press