Deciding finiteness for matrix semigroups over function fields over finite fields

A note on a paper by Rockmore, Tan, and Beals

Gábor Ivanyos *

Abstract

We present a deterministic polynomial time algorithm for testing finiteness of a semigroup S generated by matrices with entries from function fields of constant transcendence degree over finite fields. A special case of the problem was shown to be algorithmically soluble in [RTB] by giving a sharp exponential upper bound on the dimension of the matrix algebra generated by S over the field of constants. One of the exponential time algorithms proposed in [RTB] was expected to be improvable. The polynomial time method presented in this note combines the ideas of that algorithm with a procedure from [IRSz] for calculating the radical.

We assume that the reader is familiar with the elementary notions and facts from the theory of associative algebras.

The following simple observation from [RTB] reduces our task to deciding finiteness of certain matrix rings.

Observation. *Let F be a finite field, K be an arbitrary extension field of F, and S be a multiplicative subsemigroup of $M_n(K)$ generated by the finite set $\{a_1, \ldots, a_s\}$ of n by n matrices. Then S is finite if and only if the F-subalgebra A of $M_n(K)$ generated by $a_1, \ldots, a_s$ is finite.*

It is pointed out in [RTB], Theorem 3.16 that $\dim_F A$ can be exponential in n. The next statement enables us to avoid computing a basis of the whole algebra.

Lemma. *Let A be a finitely generated algebra over an arbitrary field F and assume that I is a nilpotent ideal of A such that A/I is finite dimensional. Then A is finite dimensional as well.*

Proof. Assume that $a_1, \ldots, a_s$ generate A as an F-algebra. Choose elements $b_1, \ldots, b_r$ from A such that $b_1 + I, \ldots, b_r + I$ form a basis of A/I. Write $a_l =$

*Computer and Automation Institute, Hungarian Academy of Sciences, Lágymányosi u. 11., H-1111 Budapest, Hungary E-mail: `Gabor.Ivanyos@sztaki.hu`. Research supported by NWO-OTKA Grant N26673, FKFP Grant 0612/1997, OTKA Grants 016503, 022925, and EC Grant ALTEC-KIT.

$\sum_{k=1}^{r} \alpha_{lk} b_k + c_l$ and $b_i b_j = \sum_{k=1}^{r} \beta_{ijk} b_k + d_{ij}$ with $\alpha_{lk}, \beta_{ijk} \in F$ and $c_l, d_{ij} \in I$. We claim that the elements c_l $(l = 1, \ldots, s)$ and d_{ij} $(i, j = 1, \ldots, r)$ generate I as an ideal of A. Indeed, let J be the ideal generated by these elements. Obviously $J \leq I$. On the other hand, $b_1 + J, \ldots, b_r + J$ span a subalgebra of A/J complementary to I/J. Also, it contains all the generators $a_i + J$ for A/J. Hence $I/J = (0)$, which means that $I = J$. From the claim we infer that I/I^2 is a finitely generated A/I-module and hence it is finite dimensional over F. Thus A/I^2 is finite dimensional as well and the proof can be completed by induction on the nilpotency class of I. □

The next result can be considered as a generalization of [RTB], Theorem 3.2. It turns out that modulo the radical of KA, the dimension of A is small.

Theorem. *Let F be an arbitrary field. Assume that K is an extension field of F such that for every finite extension E of F the algebra $K \otimes_F E$ is a field (e.g., K is purely transcendental over F). Let A be a finitely generated F-subalgebra of the finite dimensional K-algebra B. Let J stand for the Jacobson radical of KA and let ϕ stand for the natural projection $B \to B/J$. Then the following assertions are equivalent.*

(1) $\dim_F A$ *is finite.*

(2) $\dim_F \phi(A)$ *is finite.*

(3) $\phi(KA)$ *and* $K \otimes_F \phi(A)$ *are isomorphic K-algebras.*

(4) $\dim_F \phi(A) \leq \dim_K(B)$.

Proof. The implications (1)⇒(2), (3)⇒(4), and (4) ⇒ (2) are obvious. Since J is a finite dimensional nilpotent K-algebra we have $J^{\dim_K J} = (0)$. This also implies that $ker\phi_{|A} = A \cap J$ is a nilpotent ideal of A. The implication (2)⇒(1) follows from this observation and the lemma.

To see that (2) implies (3) assume that $\dim_F \phi(A)$ is finite. Without loss of generality we may assume that $B = KA$. By going over the factors $A/(A \cap J)$ and $B/K(A \cap J)$, we may further assume that $A \cap J = (0)$. Then, since the K-linear span of every nilpotent ideal of A is a nilpotent ideal of B, A is either semisimple or zero. If A is zero then (3) trivially holds. Otherwise let $A_1, \ldots, A_r$ be the minimal nonzero ideals of A. Then $A = A_1 + \ldots + A_r$ and the sum is direct. Also, $K \otimes_F A$ is the direct sum of the ideals $K \otimes_F A_i$. We claim that for every index i the K-algebra $K \otimes_F A_i$ is simple. Indeed, let C_i be the center of A_i. Then C_i is a finite extension field of F. By the assumption on K, $K \otimes_F C_i$ is again a field. On the other hand, it is easy to see that the center of $K \otimes_F A_i$ is $K \otimes_F C_i$. Thus $K \otimes_F A_i$ is a simple K-algebra, as claimed. Next observe the natural map $K \otimes A \to B$ induced by the multiplication of elements of A by scalars from K is a K-algebra epimorphism. But this map is a monomorphism as well because it is nonzero on any simple component $K \otimes_K A_i$ of $K \otimes_K A$. This concludes the proof of the theorem. □

In [IRSz] a deterministic algorithm is presented, which computes the radical of a matrix algebra $A \leq M_n(F_q(x_1, \ldots, x_m))$. The running time is $(n+s+d+\log q)^{O(m)}$, where s is the number of generators and d is the maximum degree among all the numerators and denominators of the entries appearing in the generators for A. (For a more general – and more transparent – approach to computing the radical of algebras of positive characteristic the reader is referred to [CIW].) Using the algorithm of [IRSz], we can find generators for the algebra $\phi(A)$ defined in the theorem in time $(n+s+d+\log q)^{O(m)}$. Then we proceed with collecting F_q-linearly independent elements of $\phi(A)$ as products of generators. We either find a basis of $\phi(A)$ in $O(n^2)$ rounds, or stop with the conclusion that our semigroup is infinite. Note that the method can be considered as an improved and generalized version of the algorithm proposed in [RTB], Subsection 3.4.1. We obtained the following.

Corollary. *There is a deterministic algorithm, which, in time $(n+s+d+\log q)^{O(m)}$ decides whether a semigroup generated by a finite set of matrices from the ring $M_n[F_q(x_1, \ldots, x_m)]$ is finite. Here, s is the number of generators and d stands for the maximum among the degrees of all the numerators and denominators of the entries in the generators. In particular, the algorithm runs in polynomial time for bounded m.*

References

[CIW] A. M. Cohen, G. Ivanyos, D. B. Wales, Finding the radical of an algebra of linear transformations, *Journal of Pure and Applied Algebra 117-118 (1997),177-193.*

[IRSz] G. Ivanyos, L. Rónyai, Á. Szántó, Decomposition of algebras over $F_q(X_1, \ldots, X_m)$, *Applicable Algebra in Engineering, Communication and Computing 5 (1994),71-90.*

[RTB] D. N. Rockmore, K.-S. Tan, R. Beals, Deciding Finiteness for Matrix Groups over Function Fields, *Israel J. Math 109 (1999), 93-116.*