Theoretical Computer Science 5 (1977) 101–111.

ON FINITE SEMIGROUPS OF MATRICES*

Arnaldo MANDEL[1] and Imre SIMON[2]

Instituto de Matemática e Estatística, Universidade de São Paulo, 05508 São Paulo, SP, Brasil

Communicated by M. Nivat
Received February 1977

Abstract. Finite semigroups of n by n matrices over the naturals are characterized both by algebraic and combinatorial methods. Next we show that the cardinality of a finite semigroup S of n by n matrices over a field is bounded by a function depending only on n, the number of generators of S and the maximum cardinality of its subgroups. As a consequence, given n and k, there exist, up to isomorphism, only a finite number of finite semigroups of n by n matrices over the rationals, generated by at most k elements. Among other applications to Automaton Theory, we show that it is decidable whether the behavior of a given $\mathbf{N}-\Sigma$ automaton is bounded.

1. Introduction

The results in this paper originated from the investigation of the following question in Automaton Theory: Is it decidable whether the behavior of a given $\mathbf{N}-\Sigma$ automaton is bounded? This is answered affirmatively and it leads to the study of finite semigroups of matrices over the naturals. After obtaining effective characterizations of these semigroups, we investigate finite semigroups of matrices over a field. This enables us to generalize, to matrices over the rationals, one of the results obtained earlier.

If K is a semiring [2, p. 122] we denote by $M_n(K)$ the multiplicative monoid of n by n matrices over K, matrix multiplication being defined as usual. We will refer to the semiring $\mathbf{N}$ of natural numbers and the semiring $\mathbf{N}_2 = \{0, 1, 2\} \subseteq \mathbf{N}$, with operations $a \oplus b = \min\{a + b, 2\}$ and $a \odot b = \min\{ab, 2\}$. Let $\Psi : M_n(\mathbf{N}) \to M_n(\mathbf{N}_2)$ be the monoid morphism given by $(A\Psi)_{ij} = \min\{A_{ij}, 2\}$ and let ι denote the set inclusion $\iota : M_n(\mathbf{N}_2) \to M_n(\mathbf{N})$. An element a of a semigroup is *torsion* if $a^p = a^q$ for some naturals $p < q$. A *torsion semigroup* is one in which every element is torsion. We denote by $\mathbf{Q}$ and $\mathbf{C}$ the fields of rational and complex numbers respectively.

Our main results can be stated as follows.

Theorem 1.1. *A finitely generated subsemigroup S of $M_n(\mathbf{N})$ is finite iff for all $A \in S\Psi$, if A is idempotent then $A\iota$ is torsion.*

* Part of the results of this paper were presented at the IV Escola de Algebra, São Paulo, July 1976.

[1] Present address: Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ont. N2L 3G1, Canada.

[2] Supported by CNPq, under 1111.1952/76.

An algebraic proof of Theorem 1.1 is given in Section 2. We also present a combinatorial proof of a much stronger version of Theorem 1.1, which gives an upper bound on the cardinality of S, depending only on n and the number of generators of S (Theorem 2.8). The existence of this upper bound raises the question whether it also exists for other semirings. In this direction we prove the following two results, in Sections 3 and 4 respectively.

Theorem 1.2. *There exists a function $f : \mathbf{N}^3 \to \mathbf{N}$, such that, for a field F, if S is a finite subsemigroup of $M_n(F)$, generated by k of its elements, and the subgroups of S have cardinality at most g, then S has cardinality at most $f(n, k, g)$.*

Theorem 1.2 implies the existence of a function f', such that any finite subsemigroup S of $M_n(F)$, generated by k of its elements, contains a subgroup of cardinality at least $f'(|S|, n, k)$. Note the similarity between this and Jordan's theorem [1, Theorem 36.13, p. 258] establishing the existence of a function $t(n)$, such that every finite subgroup of $\mathrm{GL}(n, \mathbf{C})$ contains an abelian normal subgroup of index at most $t(n)$. For the field $\mathbf{Q}$, we have an even stronger result:

Theorem 1.3. *Given naturals n and k, there exist, up to semigroup isomorphism, only a finite number of finite subsemigroups of $M_n(\mathbf{Q})$, generated by at most k elements.*

Finally, in Section 5 we give applications of these results to Automaton Theory.

2. On semigroups of matrices over the naturals

First, we give an algebraic proof of Theorem 1.1, based on a generalization [6] of the classical result of Schur on torsion groups of matrices over the complex numbers:

Theorem 2.1 (McNaughton and Zalcstein). *Every torsion semigroup of n by n matrices over a field is locally finite.*

Let $\mathbf{N}[x]$ denote the semiring of polynomials over x, with coefficients in $\mathbf{N}$.

Lemma 2.2. *Let A and B be matrices in $M_n(\mathbf{N})$, such that $A\Psi = B\Psi$. Then A is torsion iff B is torsion.*

Proof. Assume that A is torsion. It is sufficient to prove that if B is such that $A\Psi = B\Psi$ and $A_{ij} \neq B_{ij}$ for exactly one pair (i, j) of indices, then B is torsion. Indeed, since $A\Psi = B\Psi$, it follows that $A_{ij}, B_{ij} \geq 2$. Consider an indeterminate x and the matrix $A' \in M_n(\mathbf{N}[x])$, given by $A'_{rs} = A_{rs}$ if $(r, s) \neq (i, j)$ and $A'_{ij} = x$. Now,

for all $m \geq 0$, $A'^m \in M_n(\mathbf{N}[x])$ and $A'^m_{rs}(A_{ij}) = A^m_{rs}$. Since A is torsion, there exists a k, such that $A^m_{rs} \leq k$ for all m, r and s. We claim that the family $\{A'^m_{rs}\}$ of polynomials is finite. Indeed, if this is not the case, then, since $A_{ij} \geq 2$ and the polynomials have coefficients in $\mathbf{N}$, the family $\{A'^m_{rs}(A_{ij})\}$ is unbounded, which is a contradiction. It follows that A' is torsion, hence so is $B = A'(B_{ij})$. □

Lemma 2.3. *Let P be a torsion semigroup and let $\gamma : S \to P$ be a morphism, such that for all $s \in S$, $s\gamma$ idempotent implies that s is torsion. Then S is torsion.*

Proof. Let $x \in S$. Since P is torsion, $(x\gamma)^m$ is idempotent for some m, hence x^m is torsion by hypothesis and thus, so is x. □

Proof of Theorem 1.1. Let S be finite, then it is torsion. Let $A \in S\Psi$ be idempotent, and let $B \in S$ be such that $B\Psi = A$. Now, $B\Psi = A\iota\Psi$, since $A = A\iota\Psi$. Hence $A\iota$ is torsion by Lemma 2.2. Conversely, assume that S satisfies the conditions. We claim that for all A in S, $A\Psi$ idempotent implies that A is torsion. Indeed, by the hypothesis, $A\Psi\iota$ is torsion, and since $A\Psi = A\Psi\iota\Psi$, the claim follows from Lemma 2.2. Thus, since $M_n(\mathbf{N}_2)$ is finite, it is torsion, and from Lemma 2.3, S is also torsion. The result now follows from Theorem 2.1, considering our matrices over the naturals as being over the rationals. □

Now we give a combinatorial proof of a stronger version of Theorem 1.1. This will use a classical result of Ramsey [7].

Theorem 2.4 (Ramsey). *Given naturals $m \geq 2$, and $n \geq k \geq 1$, there exists a natural $R(m, n, k)$ such that for every set X of cardinality at least $R(m, n, k)$ and every partition of the cardinality k subsets of X in m blocks, there exists a subset Y of X, with cardinality n, such that all cardinality k subsets of Y belong to the same block.*

We begin by characterizing torsion elements of $M_n(\mathbf{N})$. Given A in $M_n(\mathbf{N})$, the graph GA has vertex set $\mathbf{n} = \{1, 2, \ldots, n\}$ and it has a directed edge, labeled A_{ij}, from i to j, whenever $A_{ij} \neq 0$. For an edge e, we denote its label by $e\rho$, and for a walk $T = (i_0, e_1, i_1, \ldots, e_r, i_r)$, we define its label $T\rho$ as being $\Pi e_j\rho$. The following is well known:

Lemma 2.5. *For all r in $\mathbf{N}$, A^r_{ij} is the sum of the labels of the length r walks from i to j.*

Before proceeding we note that $A \in M_n(\mathbf{N})$ is torsion iff there exists a natural m, such that $A^r_{ij} \leq m$ for all r, i and j.

Lemma 2.6. *Let A be a matrix in $M_n(\mathbf{N})$. The following statements are equivalent:*

(a) *A is torsion.*

(b) *GA contains neither a directed circuit with label at least 2, nor two distinct directed circuits joined by a path.*

(c) *There exists a permutation matrix P, such that* $P^{-1}AP$ *has the block form (some blocks might be empty)*

$$\begin{bmatrix} B_{11} & B_{12} & B_{13} \\ 0 & B_{22} & B_{23} \\ 0 & 0 & B_{33} \end{bmatrix}, \tag{1}$$

where B_{11} *and* B_{33} *are upper triangular with null diagonal, and* B_{22} *is a permutation matrix.*

Proof. (a) implies (b). Assume that GA contains a circuit T, such that $T\rho \geq 2$. Let $l > 0$ be the length of T and let i be one of its vertices. Then, by Lemma 2.5, $A_{ii}^{l} \geq (T\rho)^r \geq 2^r$ for all r, hence A is not torsion. Assume now that GA contains two distinct circuits T_1 and T_2 through vertices i and j respectively, and a path T_3 from i to j. Let l_k be the length of T_k. It follows that for all m, there are at least m pairwise distinct walks, of the form $T_1^{ml_2}T_3T_2^{ml_1}$, of length $ml_1l_2 + l_3$, from i to j. Thus, by Lemma 2.5, $A_{ij}^{ml_1l_2+l_3} \geq m$; hence A is not torsion.

(b) implies (c). We say that a strong component of GA is trivial if it contains no edges. Consider the following partition of the vertex set of GA:

$$V_2 = \{i \in \mathbf{n} : i \text{ belongs to a nontrivial strong component of } GA\}$$

$$V_1 = \{i \in \mathbf{n} \setminus V_2 : \text{there exists a path from } i \text{ to some vertex in } V_2\}$$

$$V_3 = \mathbf{n} \setminus (V_1 \cup V_2).$$

Let G_k denote the subgraph of GA, induced by V_k ($k = 1, 2, 3$). It follows that G_1 and G_3 are acyclic, hence there exist total orders $\leqslant_1$ and $\leqslant_3$, on V_1 and V_3 respectively, such that for every edge (i, j) in G_k, $i \leqslant_k j$ ($k = 1, 3$). Thus, there exists a permutation π of $\mathbf{n}$, such that

$$\text{for all } i, j \in V_k, \quad i\pi < j\pi \quad \text{iff} \quad i <_k j \quad (k = 1, 3), \tag{2}$$

$$\text{for all } i \in V_k, \quad j \in V_l, \quad \text{if } k < l \quad \text{then } i\pi < j\pi. \tag{3}$$

Let P be the permutation matrix defined by $P_{ij} = \delta_{i,j\pi}$, then $(P^{-1}AP)_{ij} = A_{i\pi,j\pi}$. Let B_{ij} denote the restriction of $P^{-1}AP$ to $V_i\pi \times V_j\pi$. It follows from the definitions of V_1, V_2 and V_3, and from (3), that B_{31} and B_{32} are null. Further, since no vertex in $V_1 \cup V_3$ belongs to some nontrivial strong component of GA, it follows that B_{11} and B_{33} have null diagonal; from (2), it follows that they are upper triangular. Conditions (b) imply that the strong components of GA are circuits with label 1, and that for every edge (i, j) of GA, if i and j belong to different strong components and $i \in V_2$, then $j \in V_3$. Hence B_{22} is a permutation matrix and B_{21} is null.

(c) implies (a). Let r be such that B_{22}^r is an identity matrix, and $r \geq n$. A simple computation shows that $A^{2r} = A^{3r}$. □

Note that another proof of Lemma 2.2 can be obtained by using Lemma 2.6. Indeed, if $A, B \in M_n(\mathbb{N})$ are such that $A\Psi = B\Psi$, then GA satisfies condition (b) iff GB does, hence A is torsion iff B is. Another consequence is:

Corollary 2.7. *If $A \in M_n(\mathbb{N})$ is torsion and $A\Psi$ is idempotent, then $A^2 = A^3$, and there exists a permutation matrix P, such that $P^{-1}AP$ has the block form (some blocks might be empty):*

$$\begin{bmatrix} 0 & C & D \\ 0 & I & E \\ 0 & 0 & 0 \end{bmatrix}, \tag{4}$$

where I is an identity matrix.

Proof. Let P be a permutation matrix, such that $P^{-1}AP$ has the form (1). Since $A\Psi$ is idempotent, $(P^{-1}AP)\Psi = (P^{-1}AP)^2\Psi$, and this implies that B_{11} and B_{33} are null, and that B_{22} is an identity matrix. Hence $P^{-1}AP$ has the form (4). Clearly $A^2 = A^3$. □

Theorem 2.8. *Let S be a subsemigroup of $M_n(\mathbb{N})$, generated by k of its elements. The following statements are equivalent:*

(a) *S is finite.*

(b) *For all $A \in S\Psi$, if A is idempotent then $(A\iota)^2 = (A\iota)^3$.*

(c) *$|S| \leq g(n,k)$ where g is a function depending only on n and k.*

Proof. (a) implies (b). Since S is finite, it is torsion. Let $A \in S\Psi$ be idempotent, and let $B \in S$ be such that $B\Psi = A$. Since $A = A\iota\Psi$, it follows that $B\Psi = A\iota\Psi$. Since B is torsion, by Lemma 2.2 so is $A\iota$. By Corollary 2.7, $(A\iota)^2 = (A\iota)^3$.

(b) implies (c). Let $m = 3^{n^2} = |M_n(\mathbb{N}_2)|$, $p = R(m,4,2)$ and $g(n,k) = \sum_{i=0}^{p-1} k^i$. Without loss of generality, we may assume that S is a monoid. Since S is generated by k of its elements, there is an epimorphism $\gamma : X^* \to S$, where X^* is the free monoid generated by a set X of cardinality k. Now we claim that if $x \in X^*$ is a word of length $|x| \geq p$, then there exists another word y, with $|y| < |x|$, such that $x\gamma = y\gamma$. It follows that $x\gamma = z\gamma$ for some word z, such that $|z| < p$; hence $|S| \leq g(n,k)$. To see the claim, let $r = |x|$ and let $x = x_1x_2 \cdots x_r$, with $x_i \in X$. Let us partition the 2-subsets of $\{1,2,\ldots,r\}$ into m blocks $\{Q_A : A \in M_n(\mathbb{N}_2)\}$, defining

$$Q_A = \{\{i,j\} : i < j \text{ and } (x_ix_{i+1} \cdots x_{j-1})\gamma\Psi = A\}.$$

Since $r \geq p$, there exist, by Theorem 2.4, $1 \leq i_1 < i_2 < i_3 < i_4 \leq r$, such that all the 2-subsets of $\{i_1, i_2, i_3, i_4\}$ belong to the same block, say Q_A. Let $y_k = x_{i_k} \cdots x_{i_{k+1}-1}$ $(k = 1,2,3)$, and let $u, v \in X^*$ be such that $x = uy_1y_2y_3v$. Denote the composition $\gamma\Psi$ by ξ. Since $\{i_1, i_2\}, \{i_2, i_3\}, \{i_1, i_3\}, \{i_2, i_3\} \in Q_A$, we have,

$$A = y_1\xi = y_2\xi = (y_1y_2)\xi = y_3\xi. \tag{5}$$

Thus, $A = (y_1y_2)\xi = y_1\xi y_2\xi = A^2$, i.e. A is an idempotent in $S\Psi$. By the hypothesis, $(A\iota)^2 = (A\iota)^3$, and by Corollary 2.7, there exists a permutation matrix P, such that $P^{-1}(A\iota)P$ has the block form (4). Since P and P^{-1} are permutation matrices, it follows from (5) that $P^{-1}A\iota P = (P^{-1}y_k\gamma P)\Psi\iota$ $(k = 1,2,3)$, hence from the definition of Ψ and ι, $P^{-1}y_k\gamma P$ has the block form

$$\begin{bmatrix} 0 & C_k & D_k \\ 0 & I & E_k \\ 0 & 0 & 0 \end{bmatrix}.$$

This implies that $(P^{-1}y_1\gamma P)(P^{-1}y_2\gamma P)(P^{-1}y_3\gamma P) = (P^{-1}y_1\gamma P)(P^{-1}y_3\gamma P)$. Hence $P^{-1}(y_1y_2y_3\gamma)P = P^{-1}(y_1y_3\gamma)P$, i.e. $y_1y_2y_3\gamma = y_1y_3\gamma$. Thus, $x\gamma = uy_1y_3v\gamma$ and this completes the proof, since $|y_2| > 0$.

(c) implies (a). This is clear. □

Note that Theorem 1.3 generalizes, for subsemigroups of $M_n(\mathbf{Q})$, the result: (a) implies (c). However, Theorem 2.8 gives a better upper bound for the cardinality of $S \subseteq M_n(\mathbf{N})$. We also remark that this upper bound can be further improved. Indeed, by using a result in [10], p can be replaced in the above proof by 2^{3m}, which is smaller than $R(m,4,2)$, given by Theorem 2.4.

3. On semigroups of matrices over a field

In this section we prove Theorem 1.2. We need:

Lemma 3.1. *Let F be a field and S a finite semigroup of linear transformations on the vector space $V = F^n$, such that the subgroups of S have cardinality at most g. Let W be a subspace of V, and let $A, B_1, B_2, \ldots, B_g$ be elements of S, such that $VA = WB_k = W$ for $k = 1, 2, \ldots, g$. Then there exist $1 \leq i < j \leq g$, such that $AB_1B_2 \cdots B_g = AB_1 \cdots B_iB_{j+1} \cdots B_g$.*

Proof. Let $T = \{B \in S : WB = W\}$. Clearly T is a subsemigroup of S. Now $WB = W$ implies that $B \mid W$ is invertible, thus $\gamma : T \to \mathrm{GL}(W)$, given by $B\gamma = B \mid W$ is a morphism. Since T is finite, $T\gamma$ is a finite subgroup of $\mathrm{GL}(W)$, hence there exists a subgroup G of T, such that $G\gamma = T\gamma$ (see [3, Proposition 4.5, p. 68]). Thus, $|G\gamma| \leq |G| \leq g$ and there exist $1 \leq i < j \leq g$, such that $(B_1 \cdots B_i)\gamma = (B_1 \cdots B_j)\gamma$, hence $(B_i \cdots B_g)\gamma = (B_1 \cdots B_iB_{j+1} \cdots B_g)\gamma$. The result follows from the observation that for each B in T, $AB = A(B\gamma)$. □

Proof of Theorem 1.2. Given k and g, let α_h and β_h be defined recursively by $\alpha_0 = \beta_0 = g$, $\alpha_h = \alpha_{h-1} + gk\beta_{h-1} + 1$, and $\beta_h = \sum_{i=0}^{\alpha_h} k^i$. Let $f(n,k,g) = \beta_n$.

Without loss of generality we may assume that S is a monoid, whose identity is

the identity matrix. We fix a basis of $V = F^n$, and consider the elements of S as linear transformations on V. Let $\gamma : X^* \to S$ be an epimorphism, where X^* is the free monoid generated by a set X of cardinality k. We will prove by induction on h, that for every A in S, if A has rank $n-h$, then $A\gamma^{-1}$ contains a word of length at most α_h. Consequently S has at most β_h elements of rank at least $n-h$. This establishes the theorem.

For $h = 0$, the subset of invertible (rank n) elements of S form a subgroup G of S, hence $|G| \leq g = \beta_0$. Since G is generated by the invertible elements of $X\gamma$, it is easy to see that for A in G, $A\gamma^{-1}$ contains a word of length at most $g = \alpha_0$. To see the induction step, let $h > 0$, let $A \in S$ have rank $n-h$ and let w be a shortest word in $A\gamma^{-1}$. Assume that $|w| > \alpha_h$. Let $Y = \{VB : B \text{ in } S \text{ has rank } n-h\}$. We first show that $|Y| \leq k\beta_{h-1}$. Indeed, let B be a rank $n-h$ element of S and let $v \in B\gamma^{-1}$. Let $v = v_1 x v_2$ be a factorization of v, such that $x \in X$, and xv_2 is the shortest nonempty terminal segment of v, for which $xv_2\gamma$ has rank $n-h$. Then $V(v\gamma) \subseteq V(xv_2\gamma)$, and since $v\gamma$ and $xv_2\gamma$ have the same rank, equality holds, i.e. $v\gamma$ and $xv_2\gamma$ have the same image. Now, by the choice of xv_2, $v_2\gamma$ has rank at least $n-h+1$. It follows that $|Y| \leq k\beta_{h-1}$. Let now u be the shortest initial segment of w, such that $u\gamma$ has rank $n-h$. From the choice of w and the induction hypothesis, $|u| \leq 1 + \alpha_{h-1}$. Since $u\gamma$ and $w\gamma$ have the same rank, for every initial segment u' of w, at least as long as u, $u'\gamma$ has rank $n-h$. Now, $|w| > \alpha_h$ implies that w has at least $\alpha_h - \alpha_{h-1} = gk\beta_{h-1} + 1$ initial segments of rank $n-h$. Since there are at most $k\beta_{h-1}$ images of rank $n-h$ elements of S, there exists a dimension $n-h$ subspace W of V and a factorization $w = v_0 v_1 \cdots v_g v_{g+1}$, such that, for $i = 0, 1, \ldots, g$, $|v_i| > 0$ and $V(v_0 \cdots v_i\gamma) = W$. Thus, $W(v_i\gamma) = W$, for $i > 0$. By Lemma 3.1, there exist $1 \leq i < j \leq g$, such that $(v_0 v_1 \cdots v_g)\gamma = (v_0 v_1 \cdots v_i v_{j+1} \cdots v_g)\gamma$, hence, there exists a word w' in $A\gamma^{-1}$, such that $|w'| < |w|$. This contradiction establishes the theorem. □

Note that Theorem 1.2 is best possible, in the sense that fixing any two of the parameters $n = 2$, $k = 1$ and $g = 1$ there exist finite semigroups of matrices over $\mathbf{C}$, with unbounded cardinality, satisfying those two parameters. However, it is likely that our upper bound $f(n, k, g)$ can be significantly improved.

4. On semigroups of matrices over the rationals

The next two lemmas appear to be known, however, we could not find a reference to them. The proof of Lemma 4.2 has been suggested by Professor Irving Reiner.

Lemma 4.1. *There exists a function* $r : \mathbf{N} \to \mathbf{N}$, *such that for every matrix* A *in* $M_n(\mathbf{Q})$, *if* A *is torsion, then* $A^n = A^{n+r(n)}$.

Proof. We denote by Φ_d the cyclotomic polynomial of order d, and ϕ is the Euler function. Let $r(n)$ be the least common multiple of $\{d \in \mathbf{N} : \phi(d) \leq n\}$. Since A is torsion, $A^p = A^q$ for some naturals $p < q$. If m_A is the minimal polynomial of A, then $m_A \mid x^p(x^{q-p} - 1)$. Since $x^{q-p} - 1$ is a product of distinct cyclotomic polynomials, and these are irreducible over $\mathbf{Q}$, it follows that $m_A = x^s \Phi_{d_1} \cdots \Phi_{d_k}$, where $d_1, \ldots, d_k$ are distinct. Since m_A has degree at most n, and that of Φ_d is $\phi(d)$, we have that $m_A \mid x^n(x^{r(n)} - 1)$. Hence $A^n = A^{n+r(n)}$. □

Lemma 4.2. *There exists a function $s : \mathbf{N} \to \mathbf{N}$, such that any finite subgroup G of $\mathrm{GL}(n, \mathbf{Q})$ has cardinality at most $s(n)$.*

Proof. Consider the elements of G as matrices over the field $\mathbf{C}$ of complex numbers. First we show that if G is abelian, then $|G| \leq r(n)^n$. Indeed, it is well-known that a finite abelian subgroup of $\mathrm{GL}(n, \mathbf{C})$ is similar to a subgroup of diagonal matrices in $\mathrm{GL}(n, \mathbf{C})$. From Lemma 4.1, the nonnull entries in this diagonal form are m th roots of 1, with $m \mid r(n)$. The claim follows. Now, let G be a finite subgroup of $\mathrm{GL}(n, \mathbf{Q})$. By Jordan's theorem [1, Theorem 36.13, p. 258], there exists a function $t(n)$, such that G contains an abelian normal subgroup of index at most $t(n)$. Thus, letting $s(n) = r(n)^n t(n)$, $|G| \leq s(n)$. □

Proof of Theorem 1.3. Clearly, for a field F, any subgroup of $M_n(F)$ is isomorphic to a subgroup of $\mathrm{GL}(n, F)$. Thus, combining Theorem 1.2 and Lemma 4.2, if S is a finite subsemigroup of $M_n(\mathbf{Q})$, generated by k of its elements, then $|S| \leq f(n, k, s(n))$. □

Note that Theorem 1.3 can not be extended to the field $\mathbf{R}$ of real numbers, since any cyclic group has a faithful representation of degree 2 over $\mathbf{R}$.

5. Applications to Automaton Theory

In this section we follow the notation of Eilenberg [2]. In particular, given a finite alphabet Σ and a semiring K, a *K-subset* A of Σ^* is a function $A : \Sigma^* \to K$, and a *K-Σ automaton* $\mathcal{A} = (Q, I, T, E)$ consists of a finite set Q, a row vector $I \in K^{\{1\} \times Q}$, a column vector $T \in K^{Q \times \{1\}}$ and a function $E : \Sigma \to K^{Q \times Q}$, where $K^{Q \times Q}$ is regarded as the multiplicative monoid of $Q \times Q$ matrices over K. The unique extension of E to a morphism is denoted by E^*. The *behavior* $|\mathcal{A}|$ of $\mathcal{A}$ is a K-subset of Σ^*, given by $s|\mathcal{A}| = I(sE^*)T$. A K-subset of Σ^* is *recognizable* if it is the behavior of some K-Σ automaton. Whenever convenient, we identify Q with $\{1, 2, \ldots, n\}$ for some n, and in this case we identify $K^{Q \times Q}$ with $M_n(K)$. Given $\mathcal{A}$, its *monoid* $M_{\mathcal{A}}$ is the submonoid of $M_n(K)$, generated by $\{\sigma E : \sigma \in \Sigma\}$, i.e. $M_{\mathcal{A}} = \{sE^* : s \in \Sigma^*\}$. A K-Σ automaton $\mathcal{A}$ is *trim* if for every q in Q, there exists a path

$$C: p_0 \xrightarrow{k_1\sigma_1} p_1 \xrightarrow{k_2\sigma_2} p_2 \longrightarrow \cdots \longrightarrow p_{m-1} \xrightarrow{k_m\sigma_m} p_m$$

such that $I_{p_0} \neq 0 \neq T_{p_m}$, $q = p_j$ for some j and $k_i \neq 0$ for $i = 1, \ldots, m$.

An **N**-subset A of Σ^* is *bounded* if there exists a natural p, such that $sA \leq p$ for every s in Σ^*. Recognizable bounded **N**-subsets of Σ^* are introduced by Eilenberg [2], and they have interesting properties, see for instance [2, Section VI, 11, p. 153]. Here we show that it is decidable whether the behavior of a given **N**-Σ automaton is bounded. Note that given recognizable **N**-subsets B and C of Σ^*, it is undecidable whether $B \leq C$ [2, Theorem VI, 12.2, p. 157].

Lemma 5.1. *The behavior of a trim* **N**-Σ *automaton is bounded iff its monoid is finite.*

Proof. The if part is trivial. To see the only if part, let $\mathcal{A} = (Q, I, T, E)$ be a trim **N**-Σ automaton, such that $|\mathcal{A}|$ is bounded; i.e. $s|\mathcal{A}| \leq p$ for some p and all $s \in \Sigma^*$. It is sufficient to show that $(sE^*)_{qr} \leq p$ for all $s \in \Sigma^*$ and $q, r \in Q$. Indeed, assume that $(sE^*)_{qr} > p$ for some s, q and r. Since $\mathcal{A}$ is trim, there exist paths $C_1: q' \to q$ and $C_2: r \to r'$, such that $I_{q'}, T_{r'} > 0$ and $|C_j| = k_j s_j$ with $k_j > 0$, for $j = 1, 2$. Then

$$\begin{aligned} s_1 s s_2 |\mathcal{A}| &= \sum_{t,t' \in Q} (Is_1E^*)_t (sE^*)_{tt'} (s_2E^*T)_{t'} \\ &\geq (Is_1E^*)_q (sE^*)_{qr} (s_2E^*T)_r \\ &\geq (I_{q'}k_1)(xE^*)_{qr}(k_2T_{r'}) > p, \end{aligned}$$

which is impossible. □

Corollary 5.2. *It is decidable whether the behavior of a given* **N**-Σ *automaton* $\mathcal{A}$ *is bounded.*

Proof. First one constructs a trim **N**-Σ automaton $\mathcal{A}'$ such that $|\mathcal{A}| = |\mathcal{A}'|$. This can be done by standard methods, see for instance [2, Section II, 4, p. 22]. Now, by Lemma 5.1, it is sufficient to decide whether $M_{\mathcal{A}'}$ is finite, which can be done, using Theorem 2.8. □

Now we indicate how this result can be extended to arbitrary subsemirings of **Q**, though the decision procedure in this case is much less elaborate, for lack of a convenient extension of Theorem 1.1, and also of Lemma 5.1. By using methods of Fliess and those of the Equality Theorem of Eilenberg and Schützenberger [2, Theorem VI, 8.1, p. 143] one can prove the following version of Theorem 2.1.1 in [4] (details can be found in [5]).

Theorem 5.3 (Fliess). *Let K be a (commutative) field, $\mathcal{A}$ a K-Σ automaton with m states and $A = |\mathcal{A}|$. The Hankel matrix of A is $\mathcal{H}_A: \Sigma^* \times \Sigma^* \to K$, given by $(\mathcal{H}_A)_{v,w} = vwA$ for $v, w \in \Sigma^*$. Then*

(a) *$\mathcal{H}_A$ has finite rank $n \leq m$.*

(b) *There exist words* $g_1, \ldots, g_n$, $d_1, \ldots, d_n$ *of length at most* m, *such that the* n *by* n *matrix* B, *given by* $B_{ij} = g_i d_j A$, *is invertible.*

(c) *There exists a* K-Σ *automaton* $\mathcal{B}$ *with* n *states and behavior* A, *whose morphism* E^* *is given by* $sE^* = \mathcal{B}^{-1}(s\mathcal{H})$, *where* $s\mathcal{H}$ *is the* n *by* n *matrix, given by* $(s\mathcal{H})_{ij} = g_i s d_j A$.

The K-Σ automaton referred to in (c) is called *reduced*, and has interesting properties. Its existence has been established by Schützenberger [8]. Note that the only improvement over the original version of Fliess, is that the matrix B is obtained from words of length at most m. This is essential in our case, since we need to construct the reduced automaton.

Corollary 5.4. *Let* K *be a subsemiring of* $\mathbf{Q}$. *It is decidable whether the behavior of a given* K-Σ *automaton* $\mathcal{A}$ *has finite image.*

Proof. By Theorem 5.3, we can effectively construct a reduced automaton $\mathcal{B}$, such that $|\mathcal{A}| = |\mathcal{B}|$. Now, it is easy to see from (c), that $|\mathcal{A}|$ has finite image iff the monoid $M_{\mathcal{B}}$ of $\mathcal{B}$ is finite. But this can be decided, since by Theorem 1.2 and Lemma 4.2, $M_{\mathcal{B}}$ is finite iff $|M_{\mathcal{B}}| \leq f(n, |\Sigma|, s(n))$, and functions f and s can be computed. □

Finally, we mention a related problem. Let $\mathbf{M}$ be the semiring with support $\mathbf{N} \cup \{\infty\}$, where $a \oplus b = \min\{a, b\}$ and $a \odot b = a + b$. In [9], a characterization of torsion elements of $M_n(\mathbf{M})$ is given, which is similar to Lemma 2.6(b), and it is conjectured that every finitely generated torsion subsemigroup of $M_n(\mathbf{M})$ is finite. This would answer positively a problem of Brzozowski: "Is it decidable whether, for a given recognizable subset A of Σ^*, $(A \cup \{1\})^n = A^*$ for some natural n?" It is not clear whether the methods of Theorem 2.8 can be used in this case.

Note added in proof

The authors learned that Gerard Jacob has independently obtained some of the results presented in this paper. His work can be found [11, 12].

References

[1] C.W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras* (Wiley-Interscience, New York, 1962).

[2] S. Eilenberg, *Automata, Languages and Machines*, Vol. A (Academic Press, New York, 1974).

[3] S. Eilenberg, *Automata, Languages and Machines*, Vol. B (Academic Press, New York, 1976).

[4] M. Fliess, Matrices de Hankel, *J. Math. Pures Appl.* **53** (1974) 197–224.

[5] A. Mandel, K-subconjuntos limitados de um monoide livre, Master's Thesis, IME-USP (1976).
[6] R. McNaughton and Y. Zalcstein, The Burnside problem for semigroups, *J. Algebra* **34** (1975) 292–299.
[7] F.P. Ramsey, On a problem of formal logic, *Proc. London Math. Soc.* 2nd Ser. **30** (1930) 264–286.
[8] M.P. Schützenberger, On the definition of a family of automata, *Information and Control* **4** (1961) 245–270.
[9] I. Simon, On limited events IME-USP (1974).
[10] I. Simon, An extremal problem for finite semigroups, in preparation.
[11] G. Jacob, La finitude des representations lineaires des semi-groupes est decidable, *J. Algebra* (submitted).
[12] G. Jacob, Un algorithme calculant le cardinal, fini ou infini, des demi groups de matrices, *Theoret. Comput. Sci.* **5** (1977).