# GROWTH OF LINEAR SEMIGROUPS

JAN OKNIŃSKI

Communicated by P. G. Trotter

## Abstract

We show that the growth function of a finitely generated linear semigroup $S \subseteq M_n(K)$ is controlled by its behaviour on finitely many cancellative subsemigroups of $S$. If the growth of $S$ is polynomially bounded, then every cancellative subsemigroup $T$ of $S$ has a group of fractions $G \subseteq M_n(K)$ which is nilpotent-by-finite and of finite rank. We prove that the latter condition, strengthened by the hypothesis that every such $G$ has a finite unipotent radical, is sufficient for $S$ to have a polynomial growth. Moreover, the degree of growth of $S$ is then bounded by a polynomial $f(n, r)$ in $n$ and the maximal degree $r$ of growth of finitely generated cancellative $T \subseteq S$.

## 1. Introduction

It is known that certain classes of finitely generated semigroups have polynomial growth. In particular, this holds for semigroups with the so called permutation property [10]. (Linear semigroups of this type even yield semigroup algebras satisfying a polynomial identity [15].) If $S$ is linear and the semigroup algebra $K[S]$ is semiprime right Goldie, then the growth of $S$ is equal to that of a cancellative subsemigroup of $S$ [13], so it can be determined by Bass's formula via the recent result of Grigorchuk [2] (cf. [10]). The latter states that a finitely generated cancellative semigroup $T$ has polynomial growth if and only if it has a group of fractions $G$ which is nilpotent-by-finite. Moreover, the degrees of growth of $S$ and $G$ are then equal.

The aim of the present paper is to study the growth of arbitrary finitely generated linear semigroups $S \subseteq M_n(K)$ over a field $K$. The local structure of linear semigroups of polynomial growth has been studied in [14]. In particular, every maximal cancellat-

18

ive subsemigroup $T$ of such a semigroup $S \subseteq M_n(K)$ has a nilpotent-by-finite group of fractions isomorphic to a subgroup $G$ of $M_n(K)$. In fact, $G$ is the group generated by the intersection of $T$ with a maximal subgroup of $M_n(K)$. Therefore, speaking of groups generated by subsemigroups of $S$, we can assume that they lie in $M_n(K)$.

The structure theorem for linear semigroups contained in [11] implies there are at most $2^n$ linear groups and as many sandwich matrices over these groups associated to each $S \subseteq M_n(K)$. The result of Grigorchuk, together with the philosophy of studying $S$ via its cancellative subsemigroups (and the associated groups) and their interactions (via the group action and the action on the sandwich matrices) makes it possible to attack the growth problem for $S$.

We show that the growth function of a finitely generated linear semigroup $S \subseteq M_n(K)$ is controlled by its behaviour on the cancellative subsemigroups of $S$. If the associated groups of fractions are nilpotent-by-finite, have finite rank and finite unipotent radicals (they are abelian-by-finite in this case), then $S$ has polynomial growth of degree bounded by a polynomial $f(n, r)$ in $n$ and the maximal degree $r$ of growth of cancellative $T \subseteq S$. We note that, if the unipotent radicals of the associated linear groups are not finite, this is no longer true. Namely, there exist semigroups $S \subseteq M_n(K)$ all of whose cancellative subsemigroups are almost nilpotent (even commutative), but the growth of $S$ is not polynomial [14].

Let $S = \langle s_1, \ldots, s_r \rangle$ be a semigroup. For any subset $A$ of $S$ let $f_A(m)$ denote the cardinality of the set $\{s_{i_1} \cdots s_{i_t} \in A \mid t \leq m, i_j \in \{1, \ldots, r\}\}$. Then $d_S(m) = f_S(m)$ is called the *growth function* of $S$ with respect to the generating set $\{s_1, \ldots, s_r\}$. We say that $S$ has *polynomial growth* if $d_S(m)$ is bounded by a polynomial in $m$. We refer to [6] for basic results on the growth and the Gelfand-Kirillov dimension. By $|s|$ we mean the minimal length of $s \in S$ in the generators $s_1, \ldots, s_r$. For $a \in M_n(K)$ we denote its rank by $\text{rk}(a)$.

## 2. $f_T(m)$ **controls** $d_S(m)$

A semigroup $U$ of a completely 0-simple semigroup $Z$ will be called *uniform* if it intersects all non-zero $\mathcal{H}$-classes of $Z$.

Let $M_j = \{a \in M_n(K) \mid \text{rk}(a) \leq j\}$, $j = 0, 1, \ldots, n$. Every semigroup $S \subseteq M_n(K)$ has a chain $S = I_n \supseteq I_{n-1} \supseteq \cdots \supseteq I_0$ where $I_j = S \cap M_j$ are ideals of $S$, if non-empty. Let $N_j = \{a \in I_j \mid \text{rk}(a) < j$ or $S^1 a S^1$ does not intersect the maximal subgroups of $M_j \setminus M_{j-1}\}$. Then $I_{j-1} \subseteq N_j \subseteq I_j$ and $N_j$ are ideals of $S$, if non-empty. It was shown in [11] that $N_j/I_{j-1}$ is nilpotent of index $\leq \binom{n}{j}$ and $I_j/N_j$ is a 0-disjoint union of at most $\binom{n}{j}$ ideals, each being a uniform subsemigroup of a completely 0-simple subsemigroup of $M_j/M_{j-1}$. Therefore, $S$ has an ideal chain $S = S_0 \supseteq S_1 \supseteq \cdots \supseteq S_t$ with all factors being nilpotent or uniform. Such a chain

will be called a structural chain of $S$.

It is well-known that the $j$th exterior power, $j = 1, \ldots, n$, can be treated as a semigroup homomorphism $\Lambda^j : M_n(K) \to M_{\binom{n}{j}}(K)$. Moreover, $rk(\Lambda^j(a)) = \binom{rk(a)}{j}$ if $rk(a) \geq j$ and 0 otherwise. We claim that for $a, b \in M_n(K)$ of rank $\geq j$ one has

$$a \mathcal{H} b \quad \text{if and only if} \quad \Lambda^j(a) \mathcal{H} \Lambda^j(b)$$

where $\mathcal{H}$ is the Green relation on $M_n(K)$, $M_{\binom{n}{j}}(K)$ respectively. We know that $\Lambda^j(a) \mathcal{H} \Lambda^j(b)$ implies that $rk(a) = rk(b)$, so that $a \mathcal{J} b$. Suppose that $a, b$ are not $\mathcal{L}$-related. Then there exists $c \in M_n(K)$ such that $rk(ac) = rk(a)$ and $rk(bc) < rk(a)$ (since $a, b$ have different kernels, when treated as endomorphisms of $K^n$). Then $0 = \Lambda^j(bc) = \Lambda^j(b) \Lambda^j(c)$, but $\Lambda^j(a) \Lambda^j(c) \neq 0$. This contradicts the fact that $\Lambda^j(a)$, $\Lambda^j(b)$ are $\mathcal{L}$-related. Hence $a \mathcal{L} b$, and similarly $a \mathcal{R} b$, so that $a \mathcal{H} b$. The converse is clear.

LEMMA 1. *Let $S \subseteq M_n(K)$ and let $S = S_0 \supseteq S_1 \supseteq \cdots \supseteq S_t$ be a structural chain for $S$. Assume that $S_i/S_{i+1}$ is a uniform factor and let $s$ be the common rank of matrices in $S_i \setminus S_{i+1}$. Then $S_i \setminus S_{i+1}$ contains elements $x_1, \ldots, x_r$, $r \leq \binom{n}{s}$, such that for every $y \in S_i \setminus S_{i+1}$ there exists $j$ with $x_j y \notin S_{i+1}$.*

PROOF. From the above remarks and from [11] it follows that $U = \Lambda^s(S_i \setminus S_{i+1}) \cup \{0\}$ is a subsemigroup in the matrices of dimension $t = \binom{n}{s}$ over $K$. Moreover, every non-zero matrix of $U$ has rank 1 and $U$ is uniform in a completely 0-simple subsemigroup of $M_t(K)$.

Let $W = \bigcap W_u \subseteq K^t$ where $W_u = \ker(u)$ and the intersection runs over all $u \in U$, $u \neq 0$. There exists $w_1, \ldots, w_r \in U$, $r \leq t$, such that $W = W_{w_1} \cap \cdots \cap W_{w_r}$. Suppose that $w_i v = 0$, $i = 1, \ldots, r$, for some $v \in U$, $v \neq 0$. Then $\text{Im}(v) \subseteq \ker(w_i)$, so that $\text{Im}(v) \subseteq W_{w_1} \cap \cdots \cap W_{w_r} = W$. Thus, $\text{Im}(v) \subseteq W_u$ for every $0 \neq u \in U$. This means that $Uv = 0$, contradicting the fact that $U$ is uniform. Hence, for each $0 \neq v \in U$ there exists $j$ such that $w_j v \in U \setminus \{0\}$. The inverse images of $w_1, \ldots, w_r$ in $S$ then satisfy the assertion for $S_i \setminus S_{i+1}$.

REMARK. A dual argument allows us to find elements $z_1, \ldots, z_q$, $q \leq \binom{n}{s}$, such that for every $y \in S_i \setminus S_{i+1}$ there exists $k$ such that $y z_k \notin S_{i+1}$. Therefore, for each $y \in S_i \setminus S_{i+1}$, we have $x_j y z_k \notin S_{i+1}$ for some $j, k$. Let $T = H \cap (S_i \setminus S_{i+1}) \neq \emptyset$ for a maximal subgroup $H$ in $M_n(K)$. It is easy to see that there exists a uniform subsemigroup $A$ of $S_i/S_{i+1}$ whose inverse image $B$ in $S$ intersects finitely many $\mathcal{H}$-classes of $M_n(K)$ and contains $T$ and all $z_1, \ldots, z_q, x_1, \ldots, x_r$. Since $A$ is uniform, there exists a finite collection $V$ of elements of $B$ such that for every $0 \neq b \in B$ there exist $v_1, v_2 \in V$ with $v_1 b v_2 \in T$. Hence, we have shown that:

there exists a finite subset $Z \subseteq S_i \setminus S_{i+1}$ such that for every $x \in S_i \setminus S_{i+1}$,

$z_1 x z_2 \in T$ for some $z_1, z_2 \in Z$.

Let $J$ be an ideal of a finitely generated semigroup $S = \langle s_1, \ldots, s_r \rangle$ and $J \subseteq I$ for a completely 0-simple semigroup $I$. Let $h(m)$ denote the number of $\mathscr{H}$-classes of $I$ that contain elements of $S$ that are words of length $\leq m$ in $s_1, \ldots, s_r$. We call $h(m)$ the *growth function* for the number of $\mathscr{H}$-classes of $I$ with respect to $J$ and the generators $s_1, \ldots, s_r$.

LEMMA 2. *Let $I$ be a completely 0-simple ideal of a semigroup $U$ and $S = \langle s_1, \ldots, s_r \rangle$ a subsemigroup of $U$. Let $J = S \cap I$ and suppose that $S/J$ has polynomial growth of degree $\leq d$. Then the growth function of the number of $\mathscr{H}$-classes of $I$ with respect to $J$ and the generators $s_1, \ldots, s_r$ is polynomial of degree not exceeding $4d$.*

PROOF. Let $D_n = \{w = s_{i_1} \cdots s_{i_k} \in J \mid k \leq n$, the proper subwords of $w$ are not in $J\}$. Then $|D_n| \leq r(d_{S/J}(n))$ since every $w \in D_n$ is of the form $w = s_i z$ where $i \in \{1, \ldots, r\}$ and $z \notin J$.

Let $0 \neq w = s_{i_1} \cdots s_{i_k} \in J$. Then $w = w_1 v$, where $w_1 = s_{i_1} \cdots s_{i_t}$, $v = s_{i_{t+1}} \cdots s_{i_k}$ and $w_1$ is the shortest initial segment of $w$ that lies in $J$. Write $w = x_1 y_1$ where $y_1$ is the shortest terminal segment of $w_1$ (treated as the word $s_{i_1} \cdots s_{i_t}$) that lies in $J$. Note that $v, x_1$ can be empty words. Then $w = x_1 y_1 v$, so that $w \mathscr{R} x_1 y_1$ in $I$. Moreover, $x_1 \notin J$ and $y_1 \in D_n$. Hence such an element $w$ can lie in at most $d_{S/J}(n)|D_n|$ $\mathscr{R}$-classes of $I$. A symmetric argument shows that $w$ can lie in at most $d_{S/J}(n)|D_n|$ $\mathscr{L}$-classes of $I$. Hence $h(n) \leq d_{S/J}(n)^2|D_n|^2 \leq r^2 d_{S/J}(n)^4$. The assertion follows.

COROLLARY. *Let $I$ be a completely 0-simple ideal of a semigroup $U$ and $S = \langle s_1, \ldots, s_r \rangle \subseteq U$, $J = S \cap I$. If $S/J$ has polynomial growth and for every $\mathscr{H}$-class $H$ in $I$ we have $f_{S \cap H}(m) \leq cm^d$ for some $c, d \geq 0$, independent of $m$ and $H$, then $S$ has polynomial growth.*

PROOF. $f_J(m) \leq cm^d h(m)$ has polynomial growth by Lemma 2. Hence, the assertion follows from the fact that $d(m) \leq f_J(m) + d_{S/J}(m)$.

Our first aim is to show that the growth of a linear semigroup $S$ is in some sense determined by the cancellative subsemigroups of $S$.

THEOREM 1. *Let $S = \langle s_1, \ldots, s_r \rangle \subseteq M_n(K)$ be a semigroup. For each uniform factor $S_i/S_{i+1}$ of a structural chain $S = S_0 \supseteq S_1 \supseteq \cdots \supseteq S_t$ of $S$ choose a cancellative subsemigroup $T_i$ which is of the form $S \cap H$ for a maximal subgroup $H$ of $M_n(K)$. Then the following conditions are equivalent:*

(1) *$S$ has polynomial growth;*
(2) *$f_T(M)$ has polynomial growth for every cancellative subsemigroup $T$ of $S$ which is of the form $T = S \cap H$ for a maximal subgroup $H$ of $M_n(K)$;*

(3)   $f_{T_i}(m)$ *has polynomial growth for every* $T_i$.

*Moreover, in this case, $GK(S) \leq g(n, d)$, where $g$ is a function of $n$ and the maximal degree $d$ of polynomials bounding the growth of the functions $f_{T_i}$.*

PROOF. The implications (1) implies (2) and (2) implies (3) are obvious. Thus assume that (3) holds. We will inductively show that $GK(S/S_i) < \infty$.

(i) If $S/S_1$ is nilpotent, then it is finite and $GK(S/S_1) = 0$. If $S/S_1$ is uniform, then from [13] it follows that $GK(S/S_1) = GK(T_1)$.

(ii) Suppose we know that $GK(S/S_i) < \infty$. Again consider two cases. If $S_i/S_{i+1}$ is nilpotent, then $(S_i/S_{i+1})^k = 0$ where $k \leq \binom{n}{j}$, $j$ denoting the rank of matrices in $S_i \setminus S_{i+1}$ [11]. Hence $GK(S_i/S_{i+1}) \leq kGK(S/S_i) < \infty$ by [6, Corollary 5.10].

Assume now that $S_i/S_{i+1}$ is uniform. From the remark following Lemma 1 we know that for every $\mathcal{H}$-class $H$ in $M_n(K)$ such that $T = H \cap (S_i \setminus S_{i+1}) \neq \emptyset$ there exist $x, y \in S_i \setminus S_{i+1}$ (chosen from a finite set $Z$) such that $0 \neq xTy \subseteq T_i$. Since $z \mapsto xzy$, $z \in T$, is a one-to-one mapping, it follows that $f_T(m) \leq f_{T_i}(m + N)$ where $N = 2\{\max |w|; w \in Z\}$. Hence $f_T(m)$ is bounded by a polynomial independent of the choice of $H$. The corollary implies that $GK(S/S_{i+1}) < \infty$. This establishes (1).

Existence of the function $g$ follows from the above proof and the fact that the structural chain must satisfy $t \leq 2^{n+1}$ (cf. [11]).

We note that there exist finitely generated semigroups $S \subseteq M_n(K)$, all of whose maximal cancellative subsemigroups have finite $GK$-dimension, but where the growth of $S$ is not polynomially bounded. Such an example is $S = \langle e, g \rangle \subseteq M_3(\mathbb{Z})$, where

$$e = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 1 & 1 \\ 0 & b & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ for } b \geq 2 \text{ (cf. [14]). (In fact, } S = \langle g \rangle \cup J,$$

for a uniform ideal $J$ consisting of matrices of rank 2, and the maximal cancellative subsemigroups of $S$ embed into the infinite cyclic group.) Thus, the growth of $S$ cannot be in general determined locally – just by looking at the cancellative pieces of $S$. This is in contrast with various results connected to the Burnside theorem for linear semigroups (that is, the case of Gelfand-Kirillov dimension 0) and some of their generalizations. Namely, it is known that certain finiteness conditions for an arbitrary $S \subseteq M_n(K)$ can be decided by studying the corresponding properties of the intersections $S \cap H$ with the maximal subgroups of $M_n(K)$ (cf. [4, 7]).

## 3.  Main result

From [14] we know that whenever a finitely generated $S \subseteq M_n(K)$ has polynomial growth, then every maximal cancellative subsemigroup $T$ of $S$ has a nilpotent-by-finite group of fractions $G \subseteq M_n(K)$. Moreover, this local condition on $S$ is equivalent to

the existence of an identity that is satisfied in $S$. If $GK(S) < \infty$, we also know that each such $G$ is finitely generated modulo its unipotent radical.

Our main goal is to show that the problem (as occurs in the above example) can only come from the unipotent radical of the groups of fractions $H$ of the maximal cancellative subsemigroups of $S$. We will prove that for a class of $S \subseteq M_n(K)$, the polynomiality of the growth of $S$ can be decided by measuring the $GK$-dimension of all (in fact, of finitely many) such $H$. We will need preparatory lemmas.

LEMMA 3. *Let* $s_1, \ldots, s_r \in M_n(K)$, $e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_n(K)$ *be the idempotent of rank one, and let* $0 \neq es_{i_1} \cdots s_{i_m} e = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$ *for some* $i_j \in \{1, \ldots, r\}$, $m \geq 1$, $x \in K$. *Then*

(i) *If* $A$ *is the set of entries of the matrices* $s_1, \ldots, s_r$, *then* $x$ *is a sum of* $n^{m-1}$ *elements of the form* $a_1 \cdots a_m$, $a_i \in A$.

(ii) *Let* $E$ *be a subfield of* $K$ *with* $[K : E] = k < \infty$, *and* $\phi : M_n(K) \to M_{nk}(E)$ *the embedding coming from the regular representation* $K \mapsto M_k(E)$. *If* $B$ *is the set of entries of* $\phi(s_1), \ldots, \phi(s_r)$ *and if* $x \in E$, *then* $x$ *is a sum of* $(nk)^{m-1}$ *elements of the form* $b_1 \cdots b_m$, $b_i \in B$.

(iii) *Assume that* $E \subseteq K$ *is Galois and* $N_{K/E}(x) = 1$. *Let* $\bar{\sigma}$ *be the natural extension of* $\sigma \in G(K/E)$ *to an automorphism of* $M_n(K)$. *Let* $C$ *be the set of entries of the matrices* $\bar{\sigma}(s_j)$, $\sigma \in G(K/E)$, $j = 1, \ldots, r$. *Then* $x^{-1}$ *is a sum of* $n^{(m-1)l}$ *elements of the form* $c_1 \cdots c_{ml}$ *where* $c_i \in C$ *and* $|G(K/E)| = l + 1$.

(iv) *Let* $v$ *be a discrete valuation of rank one on* $K$. *Then* $v(x) \geq mv(a)$ *for* $a \in A$ *with minimal valuation and, if* (iii) *holds, then* $|v(x)| \leq mN$ *for some* $N$ *dependent on* $A, C$ *and* $l$ *only.*

PROOF. (i) is clear. (ii) follows from (i) and the fact that $x$ can be viewed as a scalar $k \times k$ submatrix of $M_{nk}(E)$.

(iii) The hypothesis implies that $x^{-1} = \sigma_1(x) \cdots \sigma_l(x)$, where $\sigma_i \in G(K/E)$. Thus, $x^{-1}$ is the non-zero entry of the product of $e\bar{\sigma}_j(s_{i_1}) \cdots \bar{\sigma}_j(s_{i_m})e$, $j = 1, \ldots, l$. The assertion then follows as in (i).

(iv) By (i) we have $v(x) \geq \min\{v(a_1 \cdots a_m)\} \geq mv(a)$. But (iii) implies that $v(x^{-1}) \geq mlv(c)$ for some $c \in C$. Hence (iv) follows.

LEMMA 4. *Let* $X = (x_{ij})$, $i = 1, \ldots, n$, $j = 1, \ldots, t$, *be a matrix with real coefficients such that*

$$|a_1 x_{11} + \cdots + a_t x_{1t}| \leq M,$$

$$\cdots$$

$$|a_1 x_{n1} + \cdots + a_t x_{n1}| \leq M$$

for some $a_1, \ldots, a_t$, $M \in \mathbb{R}$. If $X$ has rank $t$, then there exists $a \in \mathbb{R}$ such that $|a_j| \leq aM$ for $j = 1, \ldots, t$.

PROOF. If $t = 1$, then $|a_1 x_{k1}| \leq M$ for every $k$ and $x_{i1} \neq 0$ for some $i$ because $X$ has rank 1. Hence we can put $a = |x_{i1}|^{-1} M$.

Let $t > 1$. Let for example $x_{11}$ be a non-zero element of the first column of $X$. For $j = 2, \ldots, n$ we have

$$
\begin{aligned}
&\left| a_2 \left( x_{j2} - x_{12} x_{j1} x_{11}^{-1} \right) + \cdots + a_t \left( x_{jt} - x_{1t} x_{j1} x_{11}^{-1} \right) \right| \\
&\leq \left| a_1 x_{j1} + a_2 x_{j2} + \cdots + a_t x_{jt} \right| + \left| a_1 x_{11} x_{j1} x_{11}^{-1} + a_2 x_{12} x_{j1} x_{11}^{-1} + \cdots + a_t x_{1t} x_{j1} x_{11}^{-1} \right| \\
&\leq M + M \left| x_{j1} x_{11}^{-1} \right|.
\end{aligned}
$$

This yields a system of inequalities with an $(n-1) \times (t-1)$ matrix $Y$ that has rank $t-1$. (We performed elementary row operations on $X$ eliminating the non-zero entries below $x_{11}$.) This allows us to complete the proof by induction on $t$.

LEMMA 5. Let $L \supseteq D = F(t_1, \ldots, t_u) \supseteq F$ be field extensions such that $[L : D] = p < \infty$ and $t_1, \ldots, t_u$ is a transcendence basis of $D$ over $F$. Let $S = \langle s_1, \ldots, s_r \rangle \subseteq M_n(L)$, $\sigma \in \mathrm{Aut}(F)$. Assume that $e \in M_n(L)$ is a diagonal idempotent of rank 1 and $e s_{i_1} \cdots s_{i_m} e$ has the only non-zero entry $x \in F$. There exists a field isomorphism $\tau : L \to L'$ such that the only non-zero entry of $e \bar{\tau}(s_{i_1}) \cdots \bar{\tau}(s_{i_m}) e \in M_n(L')$ is equal to $\sigma(x)$, where $\bar{\tau} : M_n(L) \to M_n(L')$ is the natural extension of $\tau$.

PROOF. Extend $\sigma$ to $D$, sending each $t_i$ to $t_i$, and then to $\sigma' : M_p(D) \to M_p(D)$. Let $L$ be embedded into $M_p(D)$ via the regular representation. Put $L' = \sigma'(L)$ and extend $\tau = \sigma'|_L$ to $\bar{\tau} : M_n(L) \to M_n(L')$. All these mappings agree with $\sigma$ when restricted to $F$. Hence

$$
e \bar{\tau}(s_{i_1}) \cdots \bar{\tau}(s_{i_m}) e = \bar{\tau}(e s_{i_1} \cdots s_{i_m} e)
$$

has the non-zero entry equal to $\sigma(x)$.

PROPOSITION 1. Let $S = \langle s_1, \ldots, s_r \rangle \subseteq M_n(K)$ be a finitely generated semigroup. Let $e \in M_n(K)$ be a diagonal idempotent of rank one and $z_1, \ldots, z_t$ free generators of a subgroup $H$ of $K^*$. Suppose that $A$ is a subset of $S$ such that for each $a = s_{j_1} \cdots s_{j_m} \in A$ with $0 \neq s = eae$, $j_k \in \{1, \ldots, r\}$, $m \geq 1$, the non-zero entry of the matrix $s$ is of the form $x = z_1^{i_1} \cdots z_t^{i_t}$ for some $i_j \in \mathbb{Z}$. Then there exists a constant $M$ (independent of $a$, $m$ and $j_1, \ldots, j_m$) such that $|i_j| \leq Mm$ for $j = 1, \ldots, t$.

PROOF. We shall proceed by induction on $t$. However, the case $t = 1$ will be dealt with later. Firstly, we show how to proceed with the induction step.

Let $L$ be a finitely generated subfield of $K$ such that $S \subseteq M_n(L)$ and let $K_o \subseteq K_o(t_1, \ldots, t_s) \subseteq L$ for the prime subfield $K_o$ of $K$ and a transcendence basis $t_1, \ldots, t_s$ of $L$ over $K_o$. It is known that this can be chosen so that $E = K_o(t_1, \ldots, t_s) \subseteq L$ is a separable field extension (cf. [19, Theorems II.13.30 and II.13.31]), so that extending $L$ we can assume that $E \subseteq L$ is a finite Galois extension. Let $N = N_{L/E}$ be the corresponding norm. Then for $G = G(L/E)$ we have

$$\prod_{\sigma \in G} \sigma(x) = N(x) = N(z_1)^{i_1} \cdots N(z_t)^{i_t}$$

and $N(x)$, $N(z_i) \in E$. Moreover, the non-zero entry of the matrix $e\bar{\sigma}(s_{j_1}) \cdots \bar{\sigma}(s_{j_m})e$ is equal to $\sigma(x)$, where $\bar{\sigma}$ is the natural extension of $\sigma$ to an automorphism of $M_n(L)$. We consider two cases:

Case 1. $N_{L/E}(x)$ is not a root of unity.
Then let for example $N(z_1), \ldots, N(z_p)$, $1 \le p \le t$, be a maximal subset of $\{N(z_i)|i = 1, \ldots, t\}$ that freely generates a subgroup of $L^*$. If $p < t$ then there exists $k \in \mathbb{N}$ such that $N(z_j)^k = N(z_1)^{a_{1j}} \cdots N(z_p)^{a_{pj}}$ for $j = p + 1, \ldots, t$ and some $a_{ij} \in \mathbb{Z}$. Hence $N(x)^k = N(z_1)^{b_1} \cdots N(z_p)^{b_p}$ where $b_q = ki_q + i_{p+1}a_{q,p+1} + \cdots + i_t a_{q,t}$ for $q = 1, \ldots, p$. Moreover, the matrix in $eM_n(L)e$ with the only non-zero entry equal to $N(x)^k$ is a word of length $(m + 2)k|G|$ in the generators of the semigroup $S' = \langle e, \bar{\sigma}(s_i)|\sigma \in G, i = 1, \ldots, r\rangle \subseteq M_n(L)$. If $G = \{\sigma_1, \ldots, \sigma_{|G|}\}$, let $A' = \{(e\bar{\sigma}_1(a)e\bar{\sigma}_2(a)e \cdots e\bar{\sigma}_{|G|}(a)e)^k \,|\, a \in A\}$. Then $A' \subseteq S'$ satisfy the hypotheses of the proposition with respect to the free generators $N(z_1), \ldots, N(z_p)$ of a subgroup of $L^*$.

Since $p < t$, we have performed an induction step, so the induction hypothesis shows that $|b_q| \le M(m + 2)k|G|$, $q = 1, \ldots, p$, for a constant $M$. Note that $M$ is independent of $(m + 2)k|G|$, and so of $m$, because $k$ depends on $z_1, \ldots, z_t$ only, and $M$ is independent of the choice of $a \in A$ and $j_1, \ldots, j_m$. Thus $|b_q| \le M'm$ where $M' = 3Mk|G|$. Now $x^k z_1^{-b_1} = y_2^{i_2} \cdots y_t^{i_t}$ where $y_j = z_j^k$ for $j = 2, \ldots, p$, and $y_j = z_j^k z_1^{-a_{1j}}$ for $j = p + 1, \ldots, t$. But $y_2, \ldots, y_t$ are free generators of a subgroup of $L^*$. Hence the above equality fulfills the hypotheses of the proposition with respect to $S'' = \langle S, u, v\rangle$ where $u, v \in M_n(L)$ are such that the non-zero entries of $u = eue$, $v = eve$ are $z_1, z_1^{-1}$ respectively, and the subset $A'' = \{(eae)^k u^{b_1}|a \in A, b_1 < 0\} \cup \{(eae)^k v^{b_1}|a \in A, b_1 \ge 0\}$. (Note that $b_1$ depends on $s$.) Consequently the induction hypothesis implies that

$$|i_j| \le M''((m + 2)k + |b_1|) \le (3k + M')M''m \quad \text{for} \quad j = 2, \ldots, t$$

for some $M''$ (independent of $a \in A$, $m$, $j_1, \ldots, j_m$) because $x^k z_1^{-b_1}$ is the non-zero entry of $ewe$ for a word $w$ of length $(m+2)k+|b_1|$ in $S''$. In view of the definition of $b_1$ and, again, the bound $|b_1| \le M'm$, this completes the inductive argument, establishing a linear bound also for $|i_1|$.

Assume now that $p = t$. Then we replace $x, z_1, \ldots, z_t$ by $N(x), N(z_1), \ldots, N(z_t) \in E$. Thus, passing to the semigroup $S'$ and its subset $\{e\bar{\sigma}_1(a)e\bar{\sigma}_2(a)e \cdots e\bar{\sigma}_{|G|}(a)e | a \in A\}$ we can assume that $x, z_1, \ldots, z_t \in E$. If $K_o = E$, and $\mathrm{ch}(K) = p > 0$, all $z_i \in \mathbb{F}_p$ have finite order, a contradiction. Otherwise we treat $E$ as the field of fractions of the polynomial ring $R = \mathbb{F}_p[t_1, \ldots, t_s]$ or of $R = \mathbb{Z}[t_1, \ldots, t_s]$. Let $q$ be a prime element of $R$. From Lemma 3(ii) it follows easily that $|i_1 c_1 + \cdots + i_t c_t| \leq Nm$ for some $N$ (dependent on $s_1, \ldots, s_r$ only), where $c_i = \delta(z_i)$ is the $q$-adic valuation of $z_i$. Suppose $c_1 = \cdots = c_t = 0$ for every such $q$. Then $z_1, \ldots, z_t$ lie in the group of units of $R$ (cf. [19, Corollary VI.10.3]). Since the latter is finite, this is a contradiction. Thus, for some such $\delta$ one of the $c_i$, say $c_1$, is non-zero. Let $i_1 = c_1 f_1 + d$, $0 \leq d < c_1$. Then $xz_1^{-d} = (z_1^{c_1})^{f_1} z_2^{i_2} \cdots z_t^{i_t}$ and $z_1^{c_1}, z_2, \ldots, z_t$ still are free generators of a subgroup of $L^*$. If we show that the absolute values of $f_1, i_2, \ldots, i_t$ are linearly bounded with respect to $m$, the same is true for $i_1$ and we are finished. But the elements $xz_1^{-d}$ inherit the hypotheses of the proposition with respect to the semigroup $\langle S, v \rangle$, where $v = eve$ has the non-zero entry $z_1^{-1}$, and the set $A \cup Av \cup \cdots \cup Av^{c_1-1}$. As above, this allows us to assume that $c_1 = 1$ and $f_1 = i_1$. Now $x = z_1^{k_1}(z_2 z_1^{-c_2})^{i_2} \cdots (z_t z_1^{-c_t})^{i_t}$ where $k_1 = i_1 + c_2 t_2 + \cdots + c_t i_t$ and $y_i = z_i z_1^{-c_i}$, $i = 2, \ldots, t$, are free generators of a subgroup of $L^*$. Then $xz_1^{-k_1} = y_2^{i_2} \cdots y_t^{i_t}$ and the left side is the non-zero entry of $ewe$ for a word $w$ of length $\leq m + Nm$ in $s_1, \ldots, s_r, eue, eve$, the latter two defined as above. Induction shows that $|i_j| \leq M(N+1)m$ for $j = 2, \ldots, t$, for some $M$ (independent of $m$), so that we also get a desired bound on $|i_1|$. This completes the inductive argument in Case 1.

Case 2. $N_{L/E}(x)$ is a root of unity.
As above, passing to $x^k = (z_1^k)^{i_1} \cdots (z_t^k)^{i_t}$ for some $k \geq 1$, we can assume that $N_{L/E}(x) = 1$. Then Lemma 3(iv) shows that $|v(x)| \leq Nm$ for some $N$ (independent of $m$) and every valuation with value group $\mathbb{Z}$ of $L$. If for some such $v$ one of $v(z_1), \ldots, v(z_t)$ is non-zero, we can decrease $t$ as in Case 1, performing the inductive step. Therefore we need to consider only the case where $v(z_1) = \cdots = v(z_t) = 0$ for every such $v$. It is well-known that this implies that each $z_i, z_i^{-1}$ is integral over $C = \mathbb{Z}$ or $C = \mathbb{F}_p$, depending on the characteristic of $K$. (In fact, if $a \in L$ is not integral, then $v(a) \neq 0$ for the $a^{-1}C[a^{-1}]$-adic valuation $v$ on $C[a^{-1}]$. Then $v$ can be extended to a valuation on $L$ that is again discrete of rank one – cf. [19, Lemma VI.11.1 and p. 85].) If $C = \mathbb{F}_p$, we have $\langle z_i \rangle \subseteq \mathbb{F}_p[z_i]$ is finite, contradicting the assumption on $z_i$. Thus, assume that $\mathrm{ch}(K) = 0$. Let $F$ be a finite Galois extension of $\mathbb{Q}$ containing $z_1, \ldots, z_t$. Extending $L$ we can assume that $F \subseteq L$. We know that the integral closure $B$ of $\mathbb{Z}$ in $F$ contains the group $H$ generated by $z_1, \ldots, z_t$. Let $u = u_1 + u_2$, where $\sigma_i \in G(F/Q)$, $i = 1, \ldots, u_1$, are such that $\sigma_i(F) \subseteq \mathbb{R}$ and $\sigma_i, \sigma_i' \in G(F/Q)$, $i = u_1 + 1, \ldots, u$, are the conjugate pairs of the remaining automorphisms of $F$. It is known that there exists $k \geq 1$ such that the $u \times t$ matrix

$(\ln |\sigma_i(z_j^k)|)_{i,j}$ has rank $t$ (cf. [9, §47.2]). As before, using the presentation

$$x^k = (z_1^k)^{i_1} \cdots (z_t^k)^{i_t}$$

and the fact that $z_1^k, \ldots, z_t^k$ freely generate a subgroup of $L^*$, we can reduce our problem to the case where $k = 1$. Now for every $\sigma = \sigma_i \in G(F/Q)$

$$|\sigma(x)| = |\sigma(z_1)^{i_1} \cdots \sigma(z_t)^{i_t}| = e^{\ln |\sigma(z_1)^{i_1} \cdots \sigma(z_t)^{i_t}|}$$

and $a^m \geq |\sigma(x)| \geq b^m$ for some positive $a, b \in \mathbb{R}$, by Lemma 3(i),(iii) and Lemma 5. Therefore

$$\left| i_1 \ln |\sigma(z_1)| + \cdots + i_t \ln |\sigma(z_t)| \right| \leq Mm$$

for some $M$ (not dependent on $m$). Lemma 4 yields $|i_j| \leq Nm$ for $j = 1, \ldots, t$, and some $N$ independent of $m$. This completes the inductive argument in Case 2.

It remains to check the validity of the assertion in case $t = 1$, that is, $x = z_1^{i_1}$. However, it is clear that the above reasoning takes care of this case, too. This completes the proof of the proposition.

We are now in a position to prove the first main result of this section. Recall that the unipotent radical of a linear group $G$ is the largest normal subgroup of $G$ consisting of unipotent elements.

THEOREM 2. *Let $S = \langle s_1, \ldots, s_r \rangle \subseteq M_n(K)$ be a finitely generated semigroup such that every non-empty intersection $T = S \cap F$ with a maximal subgroup $F$ of $M_n(K)$ has a group of fractions $G \subseteq F$ that is nilpotent-by-finite and finitely generated modulo its unipotent radical $U$. Then the number of cosets in $G/U$ that contain elements of $T$ that are words of length $\leq m$ in $s_1, \ldots, s_r$ is bounded by a polynomial in $m$, depending on the torsion-free rank of $G/U$ and on the rank of matrices in $T$.*

PROOF. From [14, Proposition 1], we know that the group $G$ of fractions of $T$ has a nilpotent normal subgroup $D$ of finite index that is triangularizable in $f M_n(K) f \cong M_{\text{rk}(f)}(K)$, where $f = f^2 \in D$. We can assume that $f$ is diagonal and $D$ is triangular in $M_n(K)$. Note that $U$ contains the unipotent radical of $D$, that is, the kernel of the projection $D \to \text{diag}(D)$. Then $\text{diag}(D)$ has a subgroup $B$ of finite index with all rank one diagonal projections being torsion-free subgroups of $K^*$ ($D/(D \cap U) \cong \text{diag}(D) \subseteq (K^*)^{\text{rk}(f)}$ is finitely generated since it has finite index in the finitely generated group $G/U$). Thus, there is a finite set $Z \subseteq G$ such that for every $g \in G$ there exists $z \in Z$ with $zg \in D$ and $\text{diag}(zg) \in B$. Let $e \leq f$ be a diagonal idempotent of rank one. From Proposition 1 it follows that for each non-zero $a = e z s_{i_1} \cdots s_{i_k} e$, $k \leq m$, $z \in Z$, such that $\text{diag}(z s_{i_1} \cdots s_{i_k}) \in B$, the power of each generator of the projection $e B e$ of $B$ appearing in the presentation of $a$ has absolute

value $\leq N(m+1)$ where $N$ is independent of $m$ and $i_1, \ldots, i_k$. Hence, the set $\{ezse|z \in Z, \text{diag}(zs) \in B, \text{length of } s \leq m\}$ has at most $(2N(m+1)+1)^t$ elements, where $t$ is the rank of $eBe$. Since this argument works for every diagonal of rank one $e \leq f$, we get a polynomial bound on $q_m = |\{\text{diag}(zs_{i_1} \cdots s_{i_k}) \in B|z \in Z, k \leq m\}|$. Now, the number of cosets in $G/U$ that contain elements of $T$ that are words of length $\leq m$ in $s_1, \ldots, s_r$ does not exceed $q_m|Z|$. This proves the theorem.

For any semigroup $S$ we define the rank of $S$ by $\text{RK}(S) = \sup\{t|S \text{ has a free com-}$mutative subsemigroup on $t$ generators $\}$. It is known that, for $S \subseteq M_n(K)$, $\text{RK}(S) = \text{RK}(T)$ for a cancellative subsemigroup $T$ of $S$ contained in a maximal subgroup of $M_n(K)$. If $T$ has a group of fractions that is finite-by-abelian-finite, then $\text{RK}(T) = \text{RK}(G)$ and it is equal to the Gelfand-Kirillov dimension of $G$ [10]. In particular, this applies to the case described in Theorem 3 below. (Note that such groups are in fact finitely generated and abelian-by-finite; cf. [14].)

The above result leads naturally to a condition under which we are able to prove the finiteness of $GK(S)$. Namely, assume that there exists $q \in \mathbb{N}$ such that $|\phi_T^{-1}\phi_T(t)| \leq q$ for every $t \in T$, where $\phi_T : T \to G/U$ is the natural homomorphism. Then Theorem 2 yields a polynomial bound on $f_T(m)$. Suppose that $a_1, \ldots, a_r \in G$ are in the same coset of $U$. Since $G$ is the group of fractions of $T$, $a_i = w_iv^{-1}$ for some $w_i, v \in T$. Then $w_i = a_iv \in T$ are in the same coset of $U$, so that $r \leq q$. It follows that the above condition is equivalent to saying that $U$ is a finite group.

THEOREM 3. *Let $S \subseteq M_n(K)$ be a finitely generated semigroup of finite rank $r$ such that every non-empty intersection $T = S \cap F$ with a maximal subgroup $F$ of $M_n(K)$ has a group of fractions $G \subseteq F$ that is nilpotent-by-finite; equivalently, $S$ has finite rank and satisfies an identity. If each $G$ has finite unipotent radical, then $S$ has polynomial growth of degree bounded by $f(n, r)$, where $f$ is a function of $n$ and $r$.*

PROOF. In view of Theorem 1 we need to show that $f_T(m)$ is polynomially bounded for every cancellative subsemigroup of $S$ of the form $T = S \cap F$. This is a direct consequence of Theorem 2.

The existence of the function $f(n, r)$ follows from the proof.

REMARK. (1) From the remark preceding Theorem 3 and the proof it follows that $S \subseteq M_n(K)$ has polynomial growth if and only if the associated groups $G = TT^{-1}$ are nilpotent-by-finite and for each $t \in T$ which is a word of length $\leq m$ in the generators of $S$ we have $|\phi_T^{-1}\phi_T(t)| \leq q(m)$ for a fixed polynomial $q$. In fact, in this case $f_T(m)$ also is polynomially bounded.

(2) The hypotheses of the theorem are satisfied if each $G$ is a diagonalizable-by-finite group of finite rank.

(3) Assume that ch$(K) = 0$. Then, by [18, Lemma 7.1], an abelian subgroup $D$ of finite index in a linear group $G$ is diagonalizable if and only if each $g \in G$ is a diagonalizable element. However, if each $t \in T$ is diagonalizable, then $T \cap D$ is a diagonalizable semigroup, so that $D = (D \cap T)(D \cap T)^{-1}$ is diagonalizable. Therefore, the hypotheses of the theorem are met if each $G$ is abelian-by-finite, has finite rank and a power of each $s \in S$ is a diagonalizable element.

Clearly, $S \cap Gl_n(K)$ is finitely generated (if non-empty) whenever $S$ is. Note also that a nilpotent subgroup of $Gl_2(K)$ is abelian-by-finite (cf. [18, Chapter 7]). Thus, the following is an immediate consequence of Remark (1) and the results of [14].

COROLLARY. *Let $S \subseteq M_2(K)$ be a finitely generated semigroup. Then the following conditions are equivalent:*
(i) *$S$ has polynomial growth;*
(ii) *$S$ satisfies an identity and has finite rank;*
(iii) *each cancellative subsemigroup of $S$ embeds into a finitely generated linear group of polynomial growth;*
(iv) *$S \cap Gl_2(K)$ is an almost-nilpotent semigroup, if non-empty, and every non-empty intersection $S \cap H$ with a maximal subgroup $H \neq Gl_2(K)$ of $M_2(K)$ lies in a finitely generated subgroup of $H$.*

We conclude with a comment on the growth rate of two other classes of linear semigroups, admitting in general big unipotent components, but having finite $GK$-dimension. Assume that $S = \langle s_1, \ldots, s_r \rangle$ is a Malcev nilpotent semigroup of class $t$ (cf. [8, 10]). A linear semigroup $S$ of this type has a very special structure. Namely, $S$ intersects only finitely many maximal subgroups of $M_n(K)$ ([5]). Therefore, the sandwich matrices corresponding to the uniform pieces of $S$ have finitely many rows and columns. As in [13] one then shows that $GK(S) \leq 2^p ks$, where $p = |\{j : S$ has a uniform factor consisting of matrices of rank $j\}|$, $k =$ the product of the nilpotency indices of the nilpotent factors of the structural chain of $S$, and $s =$ the maximal $GK$-dimension of the cancellative subsemigroups of $S$, (we know that $k \leq \prod_{j=1}^n \binom{n}{j}$, $p \leq n$). The connection between the nilpotency classes of $S$ and of the maximal cancellative subsemigroups of $S$ is not straightforward since the class of Malcev nilpotent semigroups is not closed under ideal extensions.

Another special class is that consisting of finitely generated semigroups with the following permutation property: there exists $m > 1$ such that for every $a_1, \ldots, a_m \in S$ one has $a_1 \cdots a_m = a_{\sigma(1)} \cdots a_{\sigma(m)}$ for a non-trivial permutation $\sigma$. Here, the finiteness of $GK(S)$, and a bound in terms of $r$ and $m$, come from the Shirshov height theorem (cf. [17],[10, Theorem 19.4]). Linear semigroups of this type have been described in [15]. The maximal cancellative subsemigroups have abelian-by-finite groups of fractions, and the associated sandwich matrices can be infinite; but they have a very

strong 'finiteness of rank' property.

# References

[1]  M. Boffa and R. M. Bryant, 'Les groupes linéaires vérifiant une identité monoidale', *C. R. Acad. Sci. Paris Ser I Math.* **308** (1989), 127–128.

[2]  R. I. Grigorchuk, 'Cancellative semigroups of power growth', *Mat. Zametki* **43** (1988), 305–319.

[3]  M. Gromov, 'Groups of polynomial growth and expanding maps', *Inst. Hautes Études Sci. Publ. Math.* **53** (1981), 53–73.

[4]  G. Jacob, 'La finitude de representations linéaires des semigroupes est décidable', *J. Algebra* **52** (1978), 437–459.

[5]  E. Jespers and J. Okniński, 'Nilpotent semigroups and semigroup algebras', *J. Algebra* **169** (1994), 984–1011.

[6]  G. R. Krause and T. H. Lenagan, *Growth of algebras and Gelfand-Kirillov dimension* (Pitman, London, 1985).

[7]  A. de Luca and S. Varricchio, 'A finiteness condition for semigroups generalizing a theorem of Coudrain and Schutzenberger', preprint.

[8]  A. I. Malcev, 'Nilpotent semigroups', *Uč. Zap. Ivanovsk. Ped. Inst.* **4** (1953), 107–111.

[9]  Ju. I. Merzljakov, *Rational groups* (Nauka, Moscow, 1987) (in Russian).

[10]  J. Okniński, *Semigroup algebras* (Marcel Dekker, New York, 1991).

[11]  ———, 'Linear representations of semigroups', in: *Monoids and semigroups with applications* (World Sci. Publ., Singapore, 1991) pp. 257–277.

[12]  ———, 'Strongly $\pi$-regular closure of linear semigroups', in: *Semigroups with applications, Oberwolfach 1991* (World Sci. Publ., Singapore, 1992) pp. 90–100.

[13]  ———, 'Gelfand-Kirillov dimension of noetherian semigroup algebras', *J. Algebra* **162** (1993), 302–316.

[14]  ———, 'Linear semigroups with identities', in: *Semigroups - Algebraic theory and applications to formal languages and codes* (World Sci. Publ., Singapore, 1993), 201–211.

[15]  J. Okniński and M. S. Putcha, 'PI semigroup algebras of linear semigroups', *Proc. Amer. Math. Soc.* **109** (1990), 39–46.

[16]  M. S. Putcha, *Linear algebraic monoids*, London Math. Soc. Lecture Note Ser. 133 (Cambridge Univ. Press, London, 1988).

[17]  L. H. Rowen, *Polynomial identities in ring theory* (Academic Press, New York, 1980).

[18]  B. A. F. Wehrfritz, *Infinite linear groups* (Springer, Berlin, 1973).

[19]  O. Zariski and P. Samuel, *Commutative algebra*, vols. I, II (Van Nostrand, Princeton, 1958, 1960).

Institute of Mathematics
Warsaw University
Banacha 2
02-097 Warsaw
Poland
e-mail: okninski@mimuw.edu.pl