On the Size of Finite Rational Matrix Semigroups

Georgina Bumpus
University of Oxford, UK

Christoph Haase [ORCID]
University College London, UK

Stefan Kiefer
University of Oxford, UK

Paul-Ioan Stoienescu
University of Oxford, UK

Jonathan Tanner
University of Oxford, UK

──── **Abstract** ────

Let n be a positive integer and $\mathcal{M}$ a set of rational $n \times n$-matrices such that $\mathcal{M}$ generates a finite multiplicative semigroup. We show that any matrix in the semigroup is a product of matrices in $\mathcal{M}$ whose length is at most $2^{n(2n+3)} g(n)^{n+1} \in 2^{O(n^2 \log n)}$, where $g(n)$ is the maximum order of finite groups over rational $n \times n$-matrices. This result implies algorithms with an elementary running time for deciding finiteness of weighted automata over the rationals and for deciding reachability in affine integer vector addition systems with states with the finite monoid property.

1 Introduction

The Burnside Problem

An element g of a semigroup G is called *torsion* if $g^i = g^j$ holds for some naturals $i < j$, and G *torsion* if all its elements are torsion. Burnside [6] asked in 1902 a question which became known as the *Burnside problem* for groups: is every finitely generated torsion group finite? Schur [28] showed in 1911 that this holds true for groups of invertible complex matrices, i.e., any finitely generated torsion subgroup of $GL(n, \mathbb{C})$ is finite. This was generalised by

47th International Colloquium on Automata, Languages, and Programming (ICALP 2020).
Editors: Artur Czumaj, Anuj Dawar, and Emanuela Merelli; Article No. 115; pp. 115:1–115:13
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Kaplansky [21, p. 105] to matrices over arbitrary fields. The Burnside problem for groups has a negative answer in general: in 1964 Golod and Shafarevich exhibited a finitely generated infinite torsion group [13, 14].

The Maximal Order of Finite Matrix Groups

Schur's result [28] assures that finitely generated torsion matrix groups are finite, but does not bound the group order. Indeed, it is easy to see that any finite cyclic group is isomorphic to a group generated by a matrix in $GL(2, \mathbb{R})$. The same is not true for $GL(n, \mathbb{Q})$: An elementary proof, see e.g. [23], shows that any finite subgroup of $GL(n, \mathbb{Q})$ is conjugate to a finite subgroup of $GL(n, \mathbb{Z})$. Another elementary proof shows that the order of any finite subgroup of $GL(n, \mathbb{Z})$ divides $(2n)!$; see, e.g., [27, Chapter IX]. Thus, denoting the order of the largest finite subgroup of $GL(n, \mathbb{Q})$ by $g(n)$, we have $g(n) \leq (2n)!$. It is shown in a paper by Friedland [12] that $g(n) = 2^n n!$ holds for all sufficiently large n. This bound is attained by the group of signed permutation matrices. Friedland's proof rests on an article by Weisfeiler [34] which in turn is based on the classification of finite simple groups. Feit showed in an unpublished manuscript [9] that $g(n) = 2^n n!$ holds if and only if $n \in \mathbb{N} \setminus \{2, 4, 6, 7, 8, 9, 10\}$.[1] Feit's proof relies on an unpublished manuscript [33], also based on the classification of finite simple groups, which Weisfeiler left behind before his tragic disappearance.

Deciding Finiteness of Matrix Groups

Bounds on group orders give a straightforward, albeit inefficient, way of deciding whether a given set of matrices generates a finite group: starting from the set of generators, enlarge it with products of matrices in the set, until either it is closed under product or the bound on the order has been exceeded. One can do substantially better: it is shown in [2] that, using computations on quadratic forms, one can decide in polynomial time if a given finite set of rational matrices generates a finite group.

Deciding Finiteness of Matrix Semigroups

The Burnside problem has a natural analogue for semigroups. In 1975, McNaughton and Zalcstein [26] positively solved the Burnside problem for matrix semigroups, i.e., they showed, for any field $\mathbb{F}$, that any finitely generated torsion subsemigroup of $\mathbb{F}^{n \times n}$ is finite, using the result for groups by Schur and Kaplansky as a building block. From a computational point of view, McNaughton and Zalcstein's result suggests an approach for deciding finiteness of the semigroup generated by a given set of rational matrices: finiteness is recursively enumerable, by closing the set of generators under product, as described above for groups. On the other hand, infiniteness is recursively enumerable by enumerating elements in the generated semigroup and checking each element whether it is torsion. By the contrapositive of McNaughton and Zalcstein's result, if the generated matrix semigroup is infinite, it has a non-torsion element, witnessing infiniteness. However, deciding whether a given matrix has finite order is nontrivial. Only in 1980 did Kannan and Lipton [19, 20] show that the so-called *orbit problem* is decidable (in polynomial time), implying an algorithm for checking whether a matrix has finite order.

---

[1] A list of the maximal-order finite subgroups of $GL(n, \mathbb{Q})$ for $n \in \{2, 4, 6, 7, 8, 9, 10\}$ can be found in [3, Table 1].

Avoiding this problem, Mandel and Simon [25] showed in 1977 that there exists a function $f : \mathbb{N}^3 \to \mathbb{N}$ such that if S is a finite subsemigroup of $\mathbb{F}^{n \times n}$, generated by m of its elements, and the subgroups of S have order at most g, then S has size (cardinality) at most $f(n, m, g)$. For rational matrices, one may use the function $g(n)$ from above for g. By making, in a sense, McNaughton and Zalcstein's proof quantitative, Mandel and Simon explicitly construct such a function f, which implies an algorithm, with bounded runtime, for deciding finiteness of a finitely generated rational matrix semigroup. A similar result about the decidability of this problem was obtained independently and concurrently by Jacob [18].

Size Bounds

Unlike the function g for rational matrix groups, Mandel and Simon's function $f(n, m, g)$ depends on m, the number of generators. This is unavoidable: the semigroup generated by the set $\mathcal{M}_m := \left\{ \begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix} : i \in \{0, \dots, m-1\} \right\}$ is the set $\mathcal{M}_m$ itself, with $|\mathcal{M}_m| = m$ for any $m \in \mathbb{N}$. Further, the growth in n of Mandel and Simon's f is, roughly, a tower of exponentials of height n. They write in [25, Section 3]: "However, it is likely that our upper bound $[f(n, m, g)]$ can be significantly improved."

In [4, Chapter VI], Berstel and Reutenauer also show, for the rational case, the existence of a function in n and m that bounds the semigroup size. They write: "As we shall see, the function [...] grows extremely rapidly." An analysis of their proof shows that the growth of their function is comparable with the growth of Mandel and Simon's function. A related approach is taken in [31]. Further proofs of McNaughton and Zalcstein's result can be found, e.g., in [24, 11, 8, 30], but they do not lead to better size bounds.

Length Bounds

In 1991, Weber and Seidl [32] considered semigroups over *nonnegative* integer matrices. Using combinatorial and automata-theoretic techniques, they showed that if a finite set $\mathcal{M} \subseteq \mathbb{N}^{n \times n}$ generates a finite monoid, then for any matrix M of that monoid there are $M_1, \dots, M_\ell \in \mathcal{M}$ with $\ell \leq \lceil e^2 n! \rceil - 2$ such that $M = M_1 \cdots M_\ell$; i.e., any matrix in the monoid is a product of matrices in $\mathcal{M}$ whose *length* is at most $\lceil e^2 n! \rceil - 2$. Note that this bound does not depend on the number of generators. Weber and Seidl also give an example that shows that such a length bound cannot be smaller than 2^{n-2}.

Almeida and Steinberg [1] proved in 2009 a length bound for rational matrices and expressing the zero matrix: if a finite set $\mathcal{M} \subseteq \mathbb{Q}^{n \times n}$ (with $n > 1$) generates a *finite* semigroup that includes the zero matrix 0, then there are $M_1, \dots, M_\ell \in \mathcal{M}$ with $\ell \leq (2n - 1)^{n^2} - 1$ such that $0 = M_1 \cdots M_\ell$. A length bound of n^5 for expressing the zero matrix was recently given in the nonnegative integer case [22]. It is open whether there is a polynomial length bound for expressing the zero matrix in the rational case.

Our Contribution

We prove a $2^{O(n^2 \log n)}$ length bound for the rational case:

▶ **Theorem 1.** *Let $\mathcal{M} \subseteq \mathbb{Q}^{n \times n}$ be a finite set of rational matrices such that $\mathcal{M}$ generates a finite semigroup $\overline{\mathcal{M}}$. Then for any $M \in \overline{\mathcal{M}}$ there are $M_1, \dots, M_\ell \in \mathcal{M}$ with $\ell \leq 2^{n(2n+3)} g(n)^{n+1} \in 2^{O(n^2 \log n)}$ such that $M = M_1 \cdots M_\ell$. (Here $g(n) \leq (2n)!$ denotes the order of the largest finite subgroup of $GL(n, \mathbb{Q})$.)*

The example by Weber and Seidl mentioned above shows that any such length bound must be at least 2^{n-2}. A length bound trivially implies a size bound, and Theorem 1 allows us to obtain the first significant improvement over the fast-growing function of Mandel and Simon.

▶ **Corollary 2.** *Let $\mathcal{M} \subseteq \mathbb{Q}^{n \times n}$ be a finite set of m rational matrices that generate a finite semigroup $\overline{\mathcal{M}}$. Then $|\overline{\mathcal{M}}| \leq m^{2^{O(n^2 \log n)}}$.*

The proof of Theorem 1 is largely based on linear-algebra arguments, specifically on the structure of a certain graph of vector spaces obtained from $\mathcal{M}$. This graph was introduced and analysed by Hrushovski et al. [17] for the computation of the *Zariski closure* of the generated matrix semigroup.

After the preliminaries (section 2) and the proof of Theorem 1 (section 3), we discuss applications in automata theory (section 4). In particular we show that our result implies the first elementary-time algorithm for deciding finiteness of weighted automata over the rationals.

2   Preliminaries

We write $\mathbb{N} = \{0, 1, 2, \ldots\}$. For a finite alphabet Σ, we write $\Sigma^* = \{a_1 \cdots a_k : k \geq 0, \ a_i \in \Sigma\}$ and $\Sigma^+ = \{a_1 \cdots a_k : k \geq 1, \ a_i \in \Sigma\}$ for the free monoid and the free semigroup generated by Σ. The elements of Σ^* are called *words*. For a word $w = a_1 \cdots a_k$, its *length* $|w|$ is k. We denote by ε the empty word, i.e., the word of length 0. For $L \subseteq \Sigma^*$, we also write $L^* = \{w_1 \cdots w_k : k \geq 0, \ w_i \in L\} \subseteq \Sigma^*$ and $L^+ = \{w_1 \cdots w_k : k \geq 1, \ w_i \in L\} \subseteq \Sigma^*$.

We denote by I_n the $n \times n$-identity matrix, and by $\vec{0}$ the zero vector. For vectors $v_1, \ldots, v_k$ from a vector space, we denote their span by $\langle v_1, \ldots, v_k \rangle$. In this article, we view elements of $\mathbb{Q}^n$ as *row* vectors.

For some $n \in \mathbb{N} \setminus \{0\}$, let $\mathcal{M} \subseteq \mathbb{Q}^{n \times n}$ be a finite set of rational matrices, generating a finite semigroup $\overline{\mathcal{M}}$. For notational convenience, throughout the paper, we associate to $\mathcal{M}$ an alphabet Σ with $|\mathcal{M}| = |\Sigma|$, and a bijection $M : \Sigma \to \mathcal{M}$ which we extend to the monoid morphism $M : \Sigma^* \to \overline{\mathcal{M}} \cup \{I_n\}$. Thus we may write $M(\Sigma)$ and $M(\Sigma^*)$ for $\mathcal{M}$ and $\overline{\mathcal{M}} \cup \{I_n\}$, respectively.

We often identify a matrix $A \in \mathbb{Q}^{n \times n}$ with its linear transformation $A : \mathbb{Q}^n \to \mathbb{Q}^n$ such that $x \mapsto xA$ for row vectors $x \in \mathbb{Q}^n$. To avoid clutter, we extend linear-algebra notions from matrices to words, i.e., we may write $\operatorname{im} w$, $\ker w$, $\operatorname{rk} w$ for the image $\operatorname{im}(M(w)) = \mathbb{Q}^n M(w)$, the kernel $\ker(M(w)) = \{x \in \mathbb{Q}^n : xM(w) = \vec{0}\}$, and the rank of $M(w)$.

If all matrices in $M(\Sigma)$ are invertible and $M(\Sigma^*)$ is finite, then $M(\Sigma^*)$ is a finite subgroup of $GL(n, \mathbb{Q})$. For $n \in \mathbb{N}$, let us write $g(n)$ for the size of the largest finite subgroup of $GL(n, \mathbb{Q})$. As discussed in the introduction, a non-trivial but elementary proof shows $g(n) \leq (2n)!$, and it is known that $g(n) = 2^n n!$ holds for sufficiently large n.

Exterior Algebra

This brief introduction is borrowed and slightly extended from [17, Section 3]. Let V be an n-dimensional vector space over a field $\mathbb{F}$. (We will only consider $V = \mathbb{Q}^n$.) For any $r \in \mathbb{N}$, let $\mathcal{A}_r$ denote the set of maps $B : V^r \to \mathbb{F}$ so that B is linear in each argument and further $B(v_1, \ldots, v_r) = 0$ holds whenever $v_i = v_{i+1}$ holds for some $i \in \{1, \ldots, r-1\}$. These conditions imply that swapping two adjacent arguments changes the sign, i.e.,

$$B(v_1, \ldots, v_{i-2}, v_{i-1}, v_{i+1}, v_i, v_{i+2}, v_{i+3}, \ldots, v_r) \ = \ -B(v_1, \ldots, v_r).$$

These properties of $\mathcal{A}_r$ imply that, given an arbitrary basis $\{e_1, \ldots, e_n\}$ of V, any $B \in \mathcal{A}_r$ is uniquely determined by all $B(e_{i_1}, \ldots, e_{i_r})$ where $1 \leq i_1 < i_2 < \ldots < i_r \leq n$. For any $v_1, \ldots, v_r \in V$, define the *wedge product*

$$v_1 \wedge \cdots \wedge v_r : \mathcal{A}_r \to \mathbb{F} \quad \text{by} \quad (v_1 \wedge \cdots \wedge v_r)(B) = B(v_1, \ldots, v_r).$$

It follows from the properties of $\mathcal{A}_r$ above that the wedge product is linear in each argument: if $v_i = \lambda u + \lambda' u'$ then

$$\Big(\bigwedge_{1 \leq i \leq k} v_i \Big)(B) = \lambda \Big(\bigwedge_{1 \leq j < i} v_j \wedge u \wedge \bigwedge_{i < j \leq k} v_j \Big)(B) + \lambda' \Big(\bigwedge_{1 \leq j < i} v_j \wedge u' \wedge \bigwedge_{i < j \leq k} v_j \Big)(B)$$

Moreover, $(v_1 \wedge \cdots \wedge v_r)(B) = 0$ if $v_i = v_j$ holds for some i, j with $i \neq j$.

For $r \in \mathbb{N}$ define $\Lambda^r V$ as the vector space generated by the length-r wedge products $v_1 \wedge \cdots \wedge v_r$ with $v_1, \ldots, v_r \in V$. For any basis $\{e_1, \ldots, e_n\}$ of V, the set $\{e_{i_1} \wedge \cdots \wedge e_{i_r} : 1 \leq i_1 < \ldots < i_r \leq n\}$ is a basis of $\Lambda^r V$; hence $\dim \Lambda^r V = \binom{n}{r}$. Note that $\Lambda^1 V = V$ and $\binom{n}{r} = 0$ for $r > n$. One can view the wedge product as an associative operation $\wedge : \Lambda^r V \times \Lambda^\ell V \to \Lambda^{r+\ell} V$. Define the *exterior algebra of V* as the direct sum $\Lambda V = \Lambda^0 V \oplus \Lambda^1 V \oplus \cdots$. Then also $\wedge : \Lambda V \times \Lambda V \to \Lambda V$.

It follows that for $u_1, \ldots, u_r \in V$, we have $u_1 \wedge \cdots \wedge u_r \neq \vec{0}$ if and only if $\{u_1, \ldots, u_r\}$ is linearly independent. Furthermore, for $u_1, \ldots, u_r, v_1, \ldots, v_r \in V$ and $u = u_1 \wedge \cdots \wedge u_r \neq \vec{0}$ and $v = v_1 \wedge \cdots \wedge v_r \neq \vec{0}$, we have that u, v are scalar multiples if and only if $\langle u_1, \ldots, u_r \rangle = \langle v_1, \ldots, v_r \rangle$.

The Grassmannian $\mathrm{Gr}(n)$ is the set of subspaces of $\mathbb{Q}^n$. By the above-stated properties of the wedge product there is an injective function

$$\iota : \mathrm{Gr}(n) \to \Lambda \, \mathbb{Q}^n$$

such that, for all $W \in \mathrm{Gr}(n)$, we have $\iota(W) = v_1 \wedge \cdots \wedge v_r$ where $\{v_1, \ldots, v_r\}$ is an arbitrarily chosen basis of W. Note that the particular choice of a basis for W only changes the value of $\iota(W)$ up to a constant. Given subspaces $W_1, W_2 \in \mathrm{Gr}(n)$, we moreover have $W_1 \cap W_2 = \{\vec{0}\}$ if and only if $\iota(W_1) \wedge \iota(W_2) \neq \vec{0}$.

3   Proof of Theorem 1

It is convenient to state and prove our main result in terms of monoids rather than semigroups:

▶ **Theorem 3.** *Let $M : \Sigma^* \to \mathbb{Q}^{n \times n}$ be a monoid morphism whose image $M(\Sigma^*)$ is finite. Then for any $w \in \Sigma^*$ there is $u \in \Sigma^*$ with $M(w) = M(u)$ and*

$$|u| \; \leq \; 2^{n(2n+3)} g(n)^{n+1} \in 2^{O(n^2 \log n)}.$$

With this theorem at hand, Theorem 1 follows immediately:

Proof of Theorem 1. Let $M \in \overline{\mathcal{M}}$ be an element of the semigroup generated by $\mathcal{M}$. If $M \neq I_n$, by Theorem 3, M can be written as a short product. Otherwise, $M = I_n \in G$, where $G = \overline{\mathcal{M} \cap GL(n, \mathbb{Q})}$ is a finite group of order at most $g(n)$. For any product $M_1 \cdots M_\ell$ with $\ell > g(n)$, there are $1 \leq i < j \leq \ell$ such that $M_1 \cdots M_i = M_1 \cdots M_j$, and so $M_1 \cdots M_\ell = M_1 \cdots M_i M_{j+1} \cdots M_\ell$. Hence, there are $\ell \in \{1, \ldots, g(n)\}$ and $M_1, \ldots, M_\ell \in \mathcal{M}$ such that $M = I_n = M_1 \cdots M_\ell$. ◀

▶ **Remark 4.** *The same argument as in the proof above shows that in a finite monoid $(H, \cdot)$, generated by $G \subseteq H$, for any $h \in H$ there are $\ell \in \{0, \ldots, |H| - 1\}$ and $g_1, \ldots, g_\ell \in G$ with $h = g_1 \cdots g_\ell$.*

In the remainder of this section, we prove Theorem 3. We assume that $M : \Sigma^* \to \mathbb{Q}^{n \times n}$ is a monoid morphism with finite image $M(\Sigma^*)$.

3.1 The Maximum-Rank Case

In this subsection we prove:

▶ **Proposition 5.** *Suppose that there is $r \le n$ with $\operatorname{rk} a = r$ for all $a \in \Sigma$. Let $w \in \Sigma^*$ with $\operatorname{rk} w = r$. Then there is $u \in \Sigma^*$ with $M(w) = M(u)$ and*

$$|u| \;\le\; 2^{2n+3} g(n) - 1 \;\in\; 2^{O(n \log n)}.$$

In this subsection we assume that $\operatorname{rk} a = r$ holds for all $a \in \Sigma$. For the proof of Proposition 5, we define a directed labelled graph G whose vertices are the vector spaces $\operatorname{im} w$ for $w \in \Sigma^*$ such that $\operatorname{rk} w = r$, and whose edges are triples (V_1, a, V_2) such that $a \in \Sigma$ and $V_1 M(a) = V_2$. Let (V_1, a, V_2) be an edge; then $V_2 \subseteq \operatorname{im} a$, but $\dim V_2 = r = \operatorname{rk} a = \dim \operatorname{im} a$, hence $V_2 = \operatorname{im} a$, i.e., the edge label determines the edge target. We will implicitly use the fact that any path in G is determined by its start vertex and the sequence of its edge labels. Note that if V_1 is a vertex and $a \in \Sigma$, the edge $(V_1, a, \operatorname{im} a)$ is present in G if and only if $\operatorname{rk} V_1 M(a) = r$ if and only if $V_1 \cap \ker a = \{\vec{0}\}$.

The following two lemmas, which are variants of lemmas in [17, Section 6], are statements about the structure of G in terms of its strongly connected components (SCCs).

▶ **Lemma 6.** *Let $w = w_1 \cdots w_k$ for $w_1, \ldots, w_k \in \Sigma^+$ with $\operatorname{rk} w = r$ such that the k vertices $\operatorname{im} w_1, \ldots, \operatorname{im} w_k$ are all in different SCCs of G. Then $k \le 2\binom{n}{r}$.*

Proof. Let $i \in \{2, \ldots, k-1\}$. Since $\operatorname{rk} w_i = r = \operatorname{rk}(w_i w_{i+1})$, we have $\operatorname{im} w_i \cap \ker w_{i+1} = \{\vec{0}\}$, thus $\iota(\operatorname{im} w_i) \wedge \iota(\ker w_{i+1}) \ne \vec{0}$. On the other hand, for any $j < i$, since $\operatorname{im} w_i, \operatorname{im} w_j$ are in different SCCs and $\operatorname{im} w_i$ is reachable from $\operatorname{im} w_j$, the vertex $\operatorname{im} w_j$ is not reachable from $\operatorname{im} w_i$; therefore we have $\operatorname{im} w_i \cap \ker w_j \ne \{\vec{0}\}$, thus $\iota(\operatorname{im} w_i) \wedge \iota(\ker w_j) = \vec{0}$. It follows that $\iota(\ker w_{i+1}) \notin \langle \iota(\ker w_j) : j < i \rangle$. Indeed, if $\iota(\ker w_{i+1}) = \sum_{j<i} \lambda_j \iota(\ker w_j)$ for some $\lambda_1, \ldots, \lambda_{i-1}$ then, by linearity of the wedge product, $\iota(\operatorname{im} w_i) \wedge \iota(\ker w_{i+1}) = \sum_{j<i} \lambda_j (\iota(\operatorname{im} w_i) \wedge \iota(\ker w_j)) = \vec{0}$, a contradiction.

We show by induction on i that $\dim \langle \iota(\ker w_j) : j \in \{1, \ldots, i\} \rangle \ge i/2$ for all $i \in \{1, \ldots, k\}$. This is clear for $i = 1, 2$. For the induction step, we have $\dim \langle \iota(\ker w_j) : j \in \{1, \ldots, i+1\} \rangle \ge \dim \langle \iota(\ker w_{i+1}), \iota(\ker w_j) : j \in \{1, \ldots, i-1\} \rangle \ge 1 + (i-1)/2 = (i+1)/2$. Hence $k/2 \le \dim \langle \iota(\ker w_j) : j \in \{1, \ldots, k\} \rangle \le \dim \Lambda^{n-r} \mathbb{Q}^n = \binom{n}{r}$. ◀

▶ **Lemma 7.** *Let $a_1 \cdots a_k \in \Sigma^*$ be (the edge labels of) a shortest path in G from a vertex $\operatorname{im} a_0$ to $\operatorname{im} a_k$. Then $k \le \binom{n}{r}$.*

Proof. Let $i \in \{0, \ldots, k-2\}$. We have $\operatorname{im} a_i \cap \ker a_{i+1} = \{\vec{0}\}$, thus $\iota(\operatorname{im} a_i) \wedge \iota(\ker a_{i+1}) \ne \vec{0}$. On the other hand, for any $j > i+1$, since $a_{i+1} \cdots a_j$ is a shortest path from $\operatorname{im} a_i$ to $\operatorname{im} a_j$, there is no edge from $\operatorname{im} a_i$ to $\operatorname{im} a_j$; therefore we have $\operatorname{im} a_i \cap \ker a_j \ne \{\vec{0}\}$, thus $\iota(\operatorname{im} a_i) \wedge \iota(\ker a_j) = \vec{0}$. It follows that $\iota(\ker a_{i+1}) \notin \langle \iota(\ker a_j) : j > i+1 \rangle$.

By induction it follows that $\dim \langle \iota(\ker a_j) : j \in \{i+1, \ldots, k\} \rangle \ge k - i$ holds for all $i \in \{0, \ldots, k-1\}$. Hence $k \le \dim \langle \iota(\ker a_j) : j \in \{1, \ldots, k\} \rangle \le \dim \Lambda^{n-r} \mathbb{Q}^n = \binom{n}{r}$. ◀

The next lemmas discuss *cycles* $w \in \Sigma^+$ in G, i.e., (the edge labels of) paths in G such that $\operatorname{im} w \cap \ker w = \{\vec{0}\}$. A cycle w is said to be *around* $\operatorname{im} w_0$ if $\operatorname{im} w = \operatorname{im} w_0$. The following lemma says, loosely speaking, that cycles around a single vertex "generate a group".

▶ **Lemma 8.** *Let $w_0 \in \Sigma^+$ with $\operatorname{rk} w_0 = r$, and let $P \in \mathbb{Q}^{r \times n}$ be a matrix with $\operatorname{im} P = \operatorname{im} w_0$. Then for every cycle $w \in \Sigma^+$ around $\operatorname{im} w_0$ there exists a unique invertible matrix $M'(w) \in GL(r, \mathbb{Q})$ such that $PM(w) = M'(w)P$. Moreover, for any nonempty set $C \subseteq \Sigma^+$ of cycles around $\operatorname{im} w_0$, $M'(C^+)$ is a finite subgroup of $GL(r, \mathbb{Q})$.*

Proof. Let $w \in \Sigma^+$ be a cycle around $\operatorname{im} w_0$. Since $\operatorname{im} P \cap \ker(M(w)) = \{\vec{0}\}$, it follows that $\operatorname{im}(PM(w)) = \operatorname{im} w = \operatorname{im} P$. So the rows of $PM(w)$ are linear combinations of rows of P, and vice versa, hence there is a unique $M'(w) \in GL(r, \mathbb{Q})$ with $PM(w) = M'(w)P$.

Let $C \subseteq \Sigma^+$ be a nonempty set of cycles around $\operatorname{im} w_0$. For any $w_1, w_2 \in C$ we have $M'(w_1 w_2)P = PM(w_1 w_2) = PM(w_1)M(w_2) = M'(w_1)PM(w_2) = M'(w_1)M'(w_2)P$, and since the rows of P are linearly independent, it follows that $M'(w_1 w_2) = M'(w_1)M'(w_2)$. Thus, $M'(C^+)$ is a semigroup.

Towards a contradiction, suppose $M'(C^+)$ were infinite. Since the rows of P are linearly independent, it follows that $M'(C^+)P$ is infinite, thus $PM(C^+)$ is infinite. Since $\operatorname{im} w_0 = \operatorname{im} P$, there is a matrix $B \in \mathbb{Q}^{n \times r}$ with $M(w_0) = BP$. Since the columns of B are linearly independent, the set $BPM(C^+)$ is infinite. But this set equals $M(w_0 C^+)$, contradicting the finiteness of $M(\Sigma^*)$. Thus the semigroup $M'(C^+)$ is finite. As $M'(C^+) \subseteq GL(r, \mathbb{Q})$, it follows that $M'(C^+)$ is a finite group.   ◀

The following lemma allows us, loosely speaking, to limit the number of cycles in a word.

▶ **Lemma 9.** *Let $w_0, w_1, \ldots, w_k \in \Sigma^+$ such that $w_1, \ldots, w_k$ are cycles around $\operatorname{im} w_0$. Then there exist $\ell \leq g(n) - 1$ and $\{u_1, \ldots, u_\ell\} \subseteq \{w_1, \ldots, w_k\}$ such that $M(w_0 w_1 \cdots w_k) = M(w_0 u_1 \cdots u_\ell)$.*

Proof. We can assume $k \geq 1$. Let $C = \{w_1, \ldots, w_k\}$. Let P and $M'(w)$ for $w \in C$ as in Lemma 8. By Lemma 8, the set $M'(C^+)$ is a finite subgroup of $GL(r, \mathbb{Q})$, so we have $|M'(C^+)| \leq g(r) \leq g(n)$. By Remark 4, there are $\ell \leq g(n) - 1$ and $u_1, \ldots, u_\ell \in C$ such that $M'(w_1) \cdots M'(w_k) = M'(u_1) \cdots M'(u_\ell)$. Since $\operatorname{im} w_0 = \operatorname{im} P$, there is a matrix $B \in \mathbb{Q}^{n \times r}$ with $M(w_0) = BP$. Hence we have $M(w_0 w_1 \cdots w_k) = BPM(w_1) \cdots M(w_k) = BM'(w_1) \cdots M'(w_k)P = BM'(u_1) \cdots M'(u_\ell)P = BPM(u_1) \cdots M(u_\ell) = M(w_0 u_1 \cdots u_\ell)$.
                                                                        ◀

The following lemma allows us to add cycles to a word.

▶ **Lemma 10.** *Let $w \in \Sigma^+$ be a cycle in G. Then there exists $\rho(w) \in \mathbb{N} \setminus \{0\}$ such that $M(w_0) = M(w_0 w^{\rho(w)})$ holds for all $w_0 \in \Sigma^+$ with $\operatorname{im} w_0 = \operatorname{im} w$.*

Proof. Let $P \in \mathbb{Q}^{r \times n}$ be a matrix with $\operatorname{im} P = \operatorname{im} w$. By Lemma 8, there exists $M'(w) \in GL(r, \mathbb{Q})$ such that $PM(w) = M'(w)P$ and $\{M'(w)^i : i \in \mathbb{N}\}$ is a finite group. Define $\rho(w)$ to be the order of this group, i.e., $M'(w)^{\rho(w)} = I_r$. Let $w_0 \in \Sigma^+$ with $\operatorname{im} w_0 = \operatorname{im} w$. Since $\operatorname{im} w_0 = \operatorname{im} P$, there is a matrix $B \in \mathbb{Q}^{n \times r}$ with $M(w_0) = BP$. Hence $M(w_0) = BP = BI_r P = BM'(w)^{\rho(w)}P = BPM(w)^{\rho(w)} = M(w_0)M(w)^{\rho(w)} = M(w_0 w^{\rho(w)})$.   ◀

The following lemma allows us to limit the length of paths within an SCC.

▶ **Lemma 11.** *Let $a \in \Sigma$, and let $w \in \Sigma^*$ be a path in G from $\operatorname{im} a$ such that $\operatorname{im} a$ and $\operatorname{im} w$ are in the same SCC. Then there exists $u \in \Sigma^*$ with $M(aw) = M(au)$ and*

$$|u| \leq 2^{n+2}g(n) - 2 \in 2^{O(n \log n)}.$$
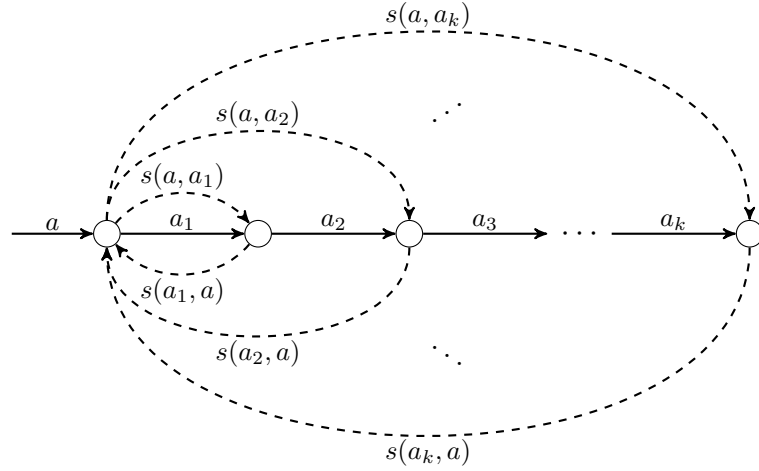
Figure 1 Illustration of the paths w and w' in Lemma 11. Edges are depicted as solid arrows, paths as dashed arrows.

Proof. For any $b_1, b_2 \in \Sigma$ such that $\operatorname{im} b_1, \operatorname{im} b_2$ are in the SCC of $\operatorname{im} a$, let $s(b_1, b_2) \in \Sigma^*$ be a shortest path from $\operatorname{im} b_1$ to $\operatorname{im} b_2$. By Lemma 7, we have $|s(b_1, b_2)| \leq \binom{n}{r}$.

Suppose $w = a_1 \cdots a_k$ for $a_i \in \Sigma$. For $i \in \{1, \ldots, k\}$ define the cycle $w_i := s(a_i, a)s(a, a_i)$ around $\operatorname{im} a_i$. By Lemma 10, we have $M(aw) = M(aw')$ for

$$w' := a_1 w_1^{\rho(w_1)} a_2 w_2^{\rho(w_2)} \cdots a_k w_k^{\rho(w_k)}.$$

For $i \in \{1, \ldots, k\}$ also define the cycle $v_i := s(a, a_i)s(a_i, a)$ around $\operatorname{im} a$. Then we have:

$$w' = a_1 s(a_1, a) v_1^{\rho(w_1)-1} s(a, a_1) a_2 s(a_2, a) v_2^{\rho(w_2)-1} s(a, a_2) \cdots a_k s(a_k, a) v_k^{\rho(w_k)-1} s(a, a_k)$$

Figure 1 illustrates the paths w and w'. Define a set of cycles $C \subseteq \Sigma^*$ around $\operatorname{im} a$ by

$$C := \{a_1 s(a_1, a), v_1, s(a, a_1)a_2 s(a_2, a), v_2, \ldots, s(a, a_{k-1})a_k s(a_k, a), v_k\}.$$

Since $w' \in C^* s(a, a_k)$, by Lemma 9, there exist $\ell \leq g(n) - 1$ and $u_1, \ldots, u_\ell \in C$ such that $M(aw) = M(aw') = M(au_1 u_2 \cdots u_\ell s(a, a_k))$. For all $v \in C$ we have $|v| \leq 2\binom{n}{r} + 1 \leq 2^{n+2}$, and $|s(a, a_k)| \leq \binom{n}{r} \leq 2^n$. Hence the lemma holds for $u := u_1 u_2 \cdots u_\ell s(a, a_k)$, as $|u| \leq 2^{n+2}(g(n) - 1) + 2^n \leq 2^{n+2}g(n) - 2$. ◀

We are ready to prove Proposition 5.

Proof of Proposition 5. Decompose the word w into $w = a_1 w_1 a_2 w_2 \cdots a_k w_k$ for $a_i \in \Sigma$ so that for all $i \in \{1, \ldots, k\}$ the vertices $\operatorname{im} a_i, \operatorname{im} w_i$ are in the same SCC, and for all $i \in \{1, \ldots, k-1\}$ the vertices $\operatorname{im} w_i, \operatorname{im} a_{i+1}$ are in different SCCs. By Lemma 6, we have $k \leq 2\binom{n}{r} \leq 2^{n+1}$. For all $i \in \{1, \ldots, k\}$, by Lemma 11, there is $u_i \in \Sigma^*$ with $|u_i| \leq 2^{n+2}g(n) - 2$ such that $M(a_i w_i) = M(a_i u_i)$. Hence the proposition holds for $u := a_1 u_1 a_2 u_2 \cdots a_k u_k$, as $|u| \leq 2^{n+1}(2^{n+2}g(n) - 2 + 1) \leq 2^{2n+3} - 1$. ◀

3.2 The General Case

In this subsection we prove Theorem 3. For $r \in \{0, \ldots, n\}$ let $d_r \in \mathbb{N}$ be the smallest number such that for any $w \in \Sigma^*$ with $\operatorname{rk} w \geq r$ there is $u \in \Sigma^*$ with $M(w) = M(u)$ and $|u| \leq d_r$. Also write h for the bound from Proposition 5.

▶ **Proposition 12.** *For any $r \in \{0, \ldots, n-1\}$ we have $d_r \leq d_{r+1} + (d_{r+1} + 1)h$.*

Proof. Let $w \in \Sigma^*$ with $\operatorname{rk} w \geq r$. We need to show that there is $u \in \Sigma^*$ with $M(w) = M(u)$ and $|u| \leq d_{r+1} + (d_{r+1} + 1)h$. Decompose w into $w = w_0 a_1 w_1 a_2 w_2 \cdots a_k w_k$ for $a_i \in \Sigma$ such that $\operatorname{rk} w_0 > r$ and for all $i \in \{1, \ldots, k\}$ we have $\operatorname{rk}(a_i w_i) = r$ and $\operatorname{rk} w_i > r$. (This decomposition is unique; in particular, $a_k w_k$ is the shortest suffix of w with rank r.) By the definition of d_{r+1}, for all $i \in \{0, \ldots, k\}$ there exists $u_i \in \Sigma^*$ with $M(w_i) = M(u_i)$ and $|u_i| \leq d_{r+1}$. Then $M(w) = M(u_0 a_1 u_1 a_2 u_2 \cdots a_k u_k)$.

Define a new alphabet Σ_r and a monoid morphism $M_r : \Sigma_r^* \to \mathbb{Q}^{n \times n}$ with $M_r(\Sigma_r) = \{M(a_i u_i) : i \in \{1, \ldots, k\}\}$, and note that $\operatorname{rk} M_r(b) = r$ for all $b \in \Sigma_r$. Then there is a word $y \in \Sigma_r^*$ such that $M_r(y) = M(a_1 u_1 \cdots a_k u_k)$. By Proposition 5, there is $x \in \Sigma_r^*$ with $M_r(y) = M_r(x)$ and $|x| \leq h$. Obtain the word $v \in \Sigma^*$ from x by replacing each letter $b \in \Sigma_r$ in x by $a_i u_i$ for $i \in \{1, \ldots, k\}$ such that $M_r(b) = M(a_i u_i)$. Then $M_r(x) = M(v)$, and thus $M(w) = M(u_0 a_1 u_1 \cdots a_k u_k) = M(u_0) M_r(y) = M(u_0) M_r(x) = M(u_0) M(v) = M(u_0 v)$, where $|u_0 v| = |u_0| + |v| \leq d_{r+1} + (d_{r+1} + 1)|x| \leq d_{r+1} + (d_{r+1} + 1)h$. ◀

We can now prove our main result.

Proof of Theorem 3. We prove by induction that for all $r \in \{0, \ldots, n\}$ we have $d_r \leq (h+1)^{n-r} d_n + (h+1)^{n-r} - 1$. For the base case, $r = n$, this is trivial. For the step, let $r < n$. We have:

$$
\begin{aligned}
d_r &\leq h + (h+1) d_{r+1} & \text{(Proposition 12)} \\
&\leq h + (h+1)\left((h+1)^{n-r-1} d_n + (h+1)^{n-r-1} - 1\right) & \text{(induction hypothesis)} \\
&= h + (h+1)^{n-r} d_n + (h+1)^{n-r} - h - 1
\end{aligned}
$$

This completes the induction proof. Hence $d_0 \leq (h+1)^n (d_n + 1) = 2^{n(2n+3)} g(n)^n (d_n + 1)$. The rank-$n$ matrices in $M(\Sigma)$ generate a finite subgroup of $GL(n, \mathbb{Q})$. So it follows by Remark 4 that $d_n + 1 \leq g(n)$. Thus $d_0 \leq 2^{n(2n+3)} g(n)^{n+1}$. ◀

4 Algorithmic Applications

Theorem 1 gives an exponential-space algorithm for deciding finiteness of a finitely generated rational matrix semigroup. In fact, the following theorem shows that deciding finiteness is in the second level of the weak EXP hierarchy (see e.g. [16] for a definition).

▶ **Theorem 13.** *Given be a finite set $\mathcal{M} \subseteq \mathbb{Q}^{n \times n}$ of rational matrices, the problem of deciding finiteness of the generated semigroup $\overline{\mathcal{M}}$ is in* $\operatorname{coNEXP}^{\operatorname{NP}}$.

Proof. For a $\operatorname{NEXP}^{\operatorname{NP}}$ algorithm deciding infiniteness, non-deterministically guess in exponential time some $M = M_1 \cdots M_\ell$, $M_i \in \mathcal{M}$, with $\ell = 2^{n(2n+3)} g(n)^{n+1} + 1$ as a witness for infiniteness. Then, using a call to an NP oracle, check whether there are $M_1', \ldots, M_r' \in \mathcal{M}$ such that $M = M_1' \cdots M_r'$ for some $0 \leq r < \ell$. If the call is successful then reject, otherwise accept.

Correctness of the algorithm immediately follows from Theorem 1: if $\overline{\mathcal{M}}$ is finite, then the $M_1', \ldots, M_r' \in \mathcal{M}$ such that $M = M_1' \cdots M_r'$ are guaranteed to exist. ◀

This is the first improvement of the non-elementary algorithm of Mandel and Simon [25].

Another immediate consequence of Theorem 1 is an upper bound on the complexity of the membership problem for finite matrix semigroups:

▶ **Theorem 14.** *Given a finite set of rational matrices $\mathcal{M} \subseteq \mathbb{Q}^{n \times n}$ such that $\overline{\mathcal{M}}$ is finite and $A \in \mathbb{Q}^{n \times n}$, the problem of deciding whether $A \in \overline{\mathcal{M}}$ is in* NEXP.

In the remainder of this section, we discuss implications of Theorem 13 to decision problems in automata theory.

4.1 Weighted Automata

The motivation for Mandel and Simon to study the finiteness problem originated from investigating the decidability of the finiteness problem (originally called boundedness problem in [25]) for weighted automata. A *weighted automaton over* $\mathbb{Q}$ is a quintuple $\mathcal{A} = (n, \Sigma, M, \alpha, \eta)$ where $n \in \mathbb{N}$ is the number of states, Σ is the finite alphabet, $M : \Sigma \to \mathbb{Q}^{n \times n}$ maps letters to transition matrices, $\alpha \in \mathbb{Q}^n$ is the initial state vector, and $\eta \in \mathbb{Q}^n$ is the final state vector. We extend M to the monoid morphism $M : \Sigma^* \to \mathbb{Q}^{n \times n}$ as before. Such an automaton defines a function $|\mathcal{A}| : \Sigma^* \to \mathbb{Q}$ by defining $|\mathcal{A}|(w) = \alpha M(w) \eta^T$, where the superscript T denotes transpose. We say, $\mathcal{A}$ is *finite* if the image of $|\mathcal{A}|$ is finite, i.e., if $|\mathcal{A}|(\Sigma^*) \subseteq \mathbb{Q}$ is a finite set. The *finiteness problem* asks whether a given automaton is finite.

It is clear that if $M(\Sigma^*)$ is finite then $\mathcal{A}$ is finite. The converse is not generally true: e.g., any automaton $\mathcal{A}$ whose initial state vector is the zero vector satisfies $|\mathcal{A}|(\Sigma^*) = \{0\}$, hence is finite, regardless of $M(\Sigma^*)$. However, it is argued in the proof of Corollary 5.4 in [25] that, given an automaton $\mathcal{A}$, one can compute, in exponential time, a polynomial-size automaton $\mathcal{B}$ with monoid morphism $M_\mathcal{B}$ such that (i) $|\mathcal{A}| = |\mathcal{B}|$, and (ii) $\mathcal{A}$ (and hence $\mathcal{B}$) is finite if and only if $M_\mathcal{B}(\Sigma^*)$ is finite.[2] Mandel and Simon use this argument to show that the finiteness problem for weighted automata over $\mathbb{Q}$ is decidable. Theorem 13 then immediately gives:

▶ **Corollary 15.** *The finiteness problem for weighted automata over $\mathbb{Q}$ can be decided in* coNEXP$^{\mathrm{NP}}$.

4.2 Affine Integer Vector Addition Systems with States

We show that Theorem 1 together with Corollary 2 imply an upper bound for the reachability problem in affine integer vector addition systems with states with the finite monoid property (afmp-$\mathbb{Z}$-VASS) studied in [5]. An affine $\mathbb{Z}$-VASS in dimension $d \in \mathbb{N}$ is a tuple $\mathcal{V} = (d, Q, T)$ such that Q is a finite set of states and $T \subseteq Q \times \mathbb{Z}^{d \times d} \times \mathbb{Z}^d \times Q$ is a finite transition relation. Setting $\mathcal{M} := \{A \in \mathbb{Z}^{d \times d} : (q, A, \vec{b}, r) \in T\}$, in afmp-$\mathbb{Z}$-VASS we additionally require that $\overline{\mathcal{M}}$ is finite. A configuration of $\mathcal{V}$ is a tuple $(q, \vec{v}) \in Q \times \mathbb{Z}^d$ which we write as $q(\vec{v})$. We define the step relation $\to \subseteq (Q \times \mathbb{Z}^d)^2$ such that $q(\vec{v}) \to r(\vec{w})$ if and only if there is a transition $(q, A, \vec{b}, r) \in T$ such that $\vec{w} = A \cdot \vec{v} + \vec{b}$. Moreover, we denote by $\to^*$ the reflexive transitive closure of $\to$. For a configuration $q(\vec{v})$, we define the reachability set of $q(\vec{v})$ as $\mathcal{R}(q(\vec{v})) := \{r(\vec{w}) : q(\vec{v}) \to^* r(\vec{w})\}$. Given configurations $q(\vec{v})$ and $r(\vec{w})$, reachability is the problem of deciding whether $r(\vec{w}) \in \mathcal{R}(q(\vec{v}))$. Note that $\mathcal{R}(q(\vec{v}))$ is in general infinite despite $\overline{\mathcal{M}}$ being finite.

---

[2] We remark that this automaton $\mathcal{B}$ has the minimal number of states among the automata defining the function $|\mathcal{A}|$. This minimal automaton goes back to [29] and has been further studied in, e.g., [7, 10].

The reachability problem for afmp-$\mathbb{Z}$-VASS was shown decidable in [5] by a reduction to reachability in $\mathbb{Z}$-VASS. A $\mathbb{Z}$-VASS is an afmp-$\mathbb{Z}$-VASS in which every transition is of the form $(q, I_d, \vec{b}, r)$. The reachability problem for $\mathbb{Z}$-VASS is known to be NP-complete, see e.g. [15]. The size of the $\mathbb{Z}$-VASS obtained in the reduction given in [5] grows in $|\overline{\mathcal{M}}|$ and hence leads to a non-elementary upper bound for reachability in afmp-$\mathbb{Z}$-VASS assuming Mandel and Simon's bound. The results of this paper enable us to significantly improve this upper bound.

▶ **Corollary 16.** *The reachability problem for afmp-$\mathbb{Z}$-VASS can be decided in* EXPSPACE.

Proof. Let $\mathcal{V} = (d, Q, T)$ be an afmp-$\mathbb{Z}$-VASS and let $\mathcal{M}$ be defined as above. Set $||\mathcal{M}|| := |\overline{\mathcal{M}}| \cdot d^2 \cdot \max\{\log(||A|| + 1) : A \in \overline{\mathcal{M}}\}$, where $||A||$ is the largest absolute value of all entries of A. Since $||A_1 \cdots A_n|| \leq d^n \cdot ||A_1|| \cdots ||A_n||$ for all $A_1, \ldots, A_n \in \mathbb{Z}^{d \times d}$ and $n \in \mathbb{N}$, by Theorem 1 and Corollary 2 we have

$$||\mathcal{M}|| \leq |T|^{2^{O(d^2 \cdot \log d)}} \cdot d^2 \cdot 2^{d(2d+3)} g(d)^{d+1} \cdot (\log d + ||T||) \leq ||T||^{2^{O(d^2 \cdot \log d)}},$$

where $||T|| := \sum_{(q,A,\vec{b},r) \in T} d^2 \cdot \lceil \log ||A|| + \log ||\vec{b}|| + 1 \rceil$. It can be deduced from the proof of [5, Thm. 7] that reachability in $\mathcal{V}$ can be decided in non-deterministic space that is polynomially bounded in the encoding of $\mathcal{V}$ and poly-logarithmically in $||\mathcal{M}||$, from which the desired exponential space upper bound follows. ◀

5 Conclusion

The main result of this paper has been to show that any element in the finite multiplicative semigroup $\overline{\mathcal{M}}$ generated by a finite set $\mathcal{M}$ of m rational $n \times n$ matrices can be obtained as a product of generators of length at most $2^{O(n^2 \log n)}$. This length bound immediately gives that $|\overline{\mathcal{M}}|$ is bounded by $m^{2^{O(n^2 \log n)}}$.

There remain two immediate questions that we did not answer in this article. The first is whether the order of growth of $|\overline{\mathcal{M}}|$ we obtained is tight. If $\overline{\mathcal{M}}$ is a group its order can be bounded by $2^n n!$ for almost all n, and this bound is attained by the group of signed permutation matrices. In contrast, in the semigroup case $|\overline{\mathcal{M}}|$ also depends on m. We conjecture that our doubly exponential upper bound is not optimal and that it is possible to establish an exponential upper bound of $|\overline{\mathcal{M}}|$ in terms of m and n. The second open question concerns the precise complexity of deciding finiteness of matrix semigroups. We have been unable to establish any non-trivial lower bounds on this problem and conjecture that our coNEXP$^{\text{NP}}$ upper bound can significantly be improved, possibly by adapting techniques of Babai et al. [2].

References

1 J. Almeida and B. Steinberg. Matrix mortality and the Černý-Pin conjecture. In *Proceedings of Developments in Language Theory (DLT)*, pages 67–80, 2009.

2 L. Babai, R. Beals, and D. Rockmore. Deciding finiteness of matrix groups in deterministic polynomial time. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 117–126, 1993.

3 N. Berry, A. Dubickas, N. D. Elkies, B. Poonen, and C. Smyth. The conjugate dimension of algebraic numbers. *The Quarterly Journal of Mathematics*, 55(3):237–252, 2004.

4 J. Berstel and C. Reutenauer. *Rational Series and Their Languages*, volume 12 of *Monographs in Theoretical Computer Science. An EATCS Series*. Springer-Verlag, 1988.

5 M. Blondin, C. Haase, and F. Mazowiecki. Affine extensions of integer vector addition systems with states. In *Proceedings of the International Conference on Concurrency Theory (CONCUR)*, pages 14:1–14:17, 2018.

6 W. Burnside. On an unsettled question in the theory of discontinuous groups. *The Quarterly Journal of Pure and Applied Mathematics*, 33:230–238, 1902.

7 J.W. Carlyle and A. Paz. Realizations by stochastic finite automata. *Journal of Computer and System Sciences*, 5(1):26–40, 1971.

8 A. de Luca and S. Varricchio. *Finiteness and Regularity in Semigroups and Formal Languages*. Monographs in Theoretical Computer Science. An EATCS Series. Springer-Verlag, 1999.

9 W. Feit. The orders of finite linear groups. Unpublished preprint.

10 M. Fliess. Matrices de Hankel. *Journal de Mathématiques Pures et Appliquées*, 53:197–222, 1974.

11 A. Freedman, R. N. Gupta, and R. M. Guralnick. Shirshov's theorem and representations of semigroups. *Pacific Journal of Mathematics*, 181(3):159–176, 1997.

12 S. Friedland. The maximal orders of finite subgroups in $GL_n(\mathbb{Q})$. *Proceedings of the American Mathematical Society*, 125(12):3519–3526, 1997.

13 E. S. Golod. On nil-algebras and finitely approximable p-groups. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:273–276, 1964.

14 E. S. Golod and I. R. Shafarevich. On the class field tower. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:261–272, 1964.

15 C. Haase and S. Halfon. Integer vector addition systems with states. In *Proceedings of Reachability Problems (RP)*, pages 112–124, 2014.

16 L. A. Hemachandra. The strong exponential hierarchy collapses. *Journal of Computer and System Sciences*, 39(3):299–322, 1989. `doi:10.1016/0022-0000(89)90025-1`.

17 E. Hrushovski, J. Ouaknine, A. Pouly, and J. Worrell. Polynomial invariants for affine programs. In *Proceedings of the Symposium on Logic in Computer Science (LICS)*, pages 530–539, 2018.

18 G. Jacob. Un algorithme calculant le cardinal, fini ou infini, des demi-groupes de matrices. *Theoretical Computer Science*, 5(2):183–204, 1977.

19 R. Kannan and R. J. Lipton. The orbit problem is decidable. In *Proceedings of the Symposium on Theory of Computing (STOC)*, pages 252–261, 1980.

20 R. Kannan and R. J. Lipton. Polynomial-time algorithm for the orbit problem. *Journal of the ACM*, 33(4):808–821, 1986.

21 I. Kaplansky. *Fields and Rings*. University of Chicago Press, second edition, 1972.

22 S. Kiefer and C. Mascle. On finite monoids over nonnegative integer matrices and short killing words. In *Proceedings of the International Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 43:1–43:13, 2019.

23 J. Kuzmanovich and A. Pavlichenkov. Finite groups of matrices whose entries are integers. *The American Mathematical Monthly*, 109(2):173–186, 2002.

24 G. Lallement. *Semigroups and combinatorial applications*. John Wiley & Sons, 1979.

25 A. Mandel and I. Simon. On finite semigroups of matrices. *Theoretical Computer Science*, 5(2):101–111, 1977.

26 R. McNaughton and Y. Zalcstein. The Burnside problem for semigroups. *Journal of Algebra*, 34:292–299, 1975.

27 M. Newman. *Integral Matrices*. Academic Press, 1972.

28 I. Schur. Über Gruppen periodischer Substitutionen. In *Sitzungsbericht Preuss. Akad. Wiss.*, pages 619–627, 1911.

29 M. P. Schützenberger. On the definition of a family of automata. *Information and Control*, 4(2–3):245–270, 1961.

30 B. Steinberg. Yet another solution to the Burnside problem for matrix semigroups. *Canadian Mathematical Bulletin*, 55(1):188–192, 2012.

31 H. Straubing. The Burnside problem for semigroups of matrices. In L. J. Cummings, editor, *Combinatorics on Words*, pages 279–295. Academic Press, 1983.

32   A. Weber and H. Seidl. On finitely generated monoids of matrices with entries in $\mathbb{N}$. *Inform-atique théorique et Applications/Theoretical Informaties and Applications*, 25:19–38, 1991.

33   B. Weisfeiler. On the size and structure of finite linear groups. Unpublished preprint. `arXiv:1203.1960`.

34   B. Weisfeiler. Post-classification version of Jordan's theorem on finite linear groups. *Proceedings of the National Academy of Sciences of the United States of America*, 81:5278–5279, 1984.