On the Size of Finite Rational Matrix Semigroups

Christoph Haase
University of Oxford, UK

based on joint work with
Georgina Bumpus, Stefan Kiefer, Paul-Ioan Stoienescu and Jonathan Tanner from Oxford

Los Angeles Combinatorics and Complexity Seminar
10 November 2020

Matrix semigroups

Given a finite set $\mathcal{M}$ of $n \times n$ matrices, denote by $\overline{\mathcal{M}}$ the semigroup generated by $\mathcal{M}$

Examples

- For $\mathcal{M} = \{A, B\}$ with $A = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix}$ have $\overline{\mathcal{M}} = \{A, A^2, B, B^2, AB, A^2B, \mathbf{0}\}$
- For $\mathcal{M}$ being the set of all (signed) $n \times n$ permutation matrices, $\overline{\mathcal{M}} = \mathcal{M}$
- For $\mathcal{M} = \{S, T\}$ with $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ have $\overline{\mathcal{M}} = \mathrm{SL}_2(\mathbb{Z})$

Properties of finite matrix semigroups

For $\mathcal{M} \subseteq \mathbb{Q}^{n \times n}$ generating a finite semigroup, we are interested in bounding as a function of $\mathcal{M}$:

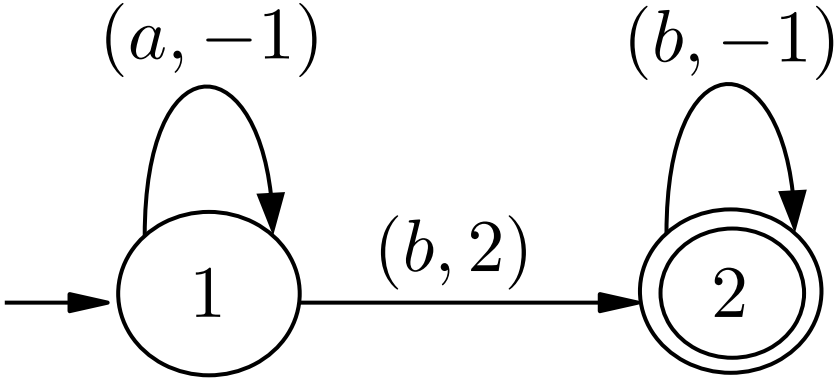
- The length of a given $M \in \overline{\mathcal{M}}$, i.e. the smallest ℓ s.t.

$$M = M_1 \cdots M_\ell, \;\; M_i \in \mathcal{M}$$

- The cardinality of $\overline{\mathcal{M}}$

Trivially, a length upper bound ℓ implies $|\overline{\mathcal{M}}| \leq |\mathcal{M}|^\ell$

Motivation from automata theory



$$M_a = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} \qquad M_b = \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix}$$

$$\mathcal{A}(a) = 0 \quad \mathcal{A}(bb) = \mathcal{A}(ab) = -2 \quad \mathcal{A}(b) = \mathcal{A}(aab) = 2$$

- A weighted automaton $\mathcal{A}$ is a finite-state automaton with weights along edges
- Maps a word $w \in \Sigma^*$ to value $\mathcal{A}(w) \in \mathbb{Q}$
- Boundedness, is $\mathcal{A}(\Sigma^*)$ finite, reduces to deciding finiteness of a matrix semigroup

Main result

Theorem
For $\mathcal{M} \subseteq \mathbb{Q}^{n \times n}$ generating a finite semigroup, the length of every $M \in \overline{\mathcal{M}}$ is at most

$$2^{n(2n+3)} g(n)^{n+1} = 2^{O(n^2 \log n)}$$

order of the largest finite subgroup of $\mathrm{GL}(n, \mathbb{Q})$ bounded by $(2n)!$

no dependence on $|\mathcal{M}|$

- For $\mathcal{M} \subseteq \mathbb{N}^{n \times n}$, Weber and Seidl (1991) give a length bound of $2^{n \log n}$
- They also give a lower bound of 2^{n-2}

Size bounds

The implied upper bound on $|\overline{\mathcal{M}}|$ is

$$|\overline{\mathcal{M}}| \leq |\mathcal{M}|^{\left(2^{n(2n+3)} g(n)^{n+1}\right)}$$

$|\overline{\mathcal{M}}|$ must depend on $|\mathcal{M}|$:

$$\mathcal{M}_k := \left\{ \begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix} : i \in \{1, \ldots, k\} \right\}$$

$$\overline{\mathcal{M}_k} = \mathcal{M}_k \cup \{\mathbf{0}\}, \ |\overline{\mathcal{M}_k}| = k + 1$$

No real analogue:

$$R_k := \begin{pmatrix} \cos \frac{2\pi}{k} & -\sin \frac{2\pi}{k} \\ \sin \frac{2\pi}{k} & \cos \frac{2\pi}{k} \end{pmatrix}$$

Have $(R_k)^k = I_2$ and hence $|\overline{\{R_k\}}| = k$

Complexity considerations

- Size bounds give trivial algorithm for deciding finiteness of $|\overline{\mathcal{M}}|$
- Decidability first shown by Mandel and Simon (1977), and Jacob (1977)
- Size bound of Mandel and Simon grows non-elementary for $n \times n$ matrices, lower bounded by:

$$2^{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}} \Big\} n$$

- Our results give a $\mathrm{coNEXP}^{\mathrm{NP}} \subseteq \text{2-EXP}$ upper bound

Finite rational matrix groups

Still the group case is much better understood:

- Let $g(n)$ be the size of the largest subgroup of $\mathrm{GL}(\mathbb{Q}, n)$
- Elementary proof that $g(n) \leq (2n)!$
- Friedland (1997), building upon Weisfeiler (1984), established $g(n) = 2^n n!$ for n large enough
- Tight for group of signed permutation matrices
- Feit (unpublished), building upon Weisfeiler (unpublished), showed $g(n) = 2^n n!$ for $n \in \mathbb{N} \setminus \{2, 4, 6, 7, 8, 9, 10\}$

Finite rational matrix groups

Even though $g(n) = \Theta(2^n n!)$, it is known that:

Theorem (Babai, Beals, Rockmore, 1993)
Finiteness of a group of matrices given by a list of generators is decidable in deterministic polynomial time.

- Better complexity upper bounds for the semigroup case likely
- No non-trivial complexity lower bounds known for deciding finiteness in the semigroup case

Techniques for the upper bound

Our length upper bound for rational matrix semigroups mainly relies on:

- The size bound(s) for the group case
- A graph of vector spaces associated to a generating set introduced by Hrushovski et al. (2017)
- Basic properties of the exterior algebra

A graph of vector spaces

Given $\mathcal{M} \subseteq \mathbb{Q}^{n \times n}$ of maximum rank r, define a directed labeled graph $G = (V, E)$:

- $V = \{\text{im } M : M \in \mathcal{M}, \text{rk } M = r\}$
- $(V_1, M, V_2) \in E \iff V_1 M = V_2$

due to maximum rank have $V_1 \cap \ker M = \{\mathbf{0}\}$

and in particular $V_2 = \text{im } M$

For a path $M_1 \cdots M_k$ of rank r with $M_i \in \overline{\mathcal{M}}$ and all $\text{im } M_i$ in different SCCs, have

- $\text{im } M_i \cap \ker M_{i+1} = \{\mathbf{0}\}$
- $\text{im } M_j \cap \ker M_i \neq \{\mathbf{0}\}$ for $j < i$

Allows to bound number of SCCs of G by $2\binom{n}{r}$

Bounding paths in an SCC

- Similar reasoning bounds shortest path between two vertices of G as $\binom{n}{r}$
- Cycles in G generate a group
- Rewrite arbitrary path in an SCC as initial segment of cycles and final loop-free path
- Obtain length bound for path in $\overline{\mathcal{M}}$ staying in the same SCC of $2^{n+2}g(n) - 2$
- Finally consider smaller ranks and combine bounds to obtain overall bound of $2^{n(2n+3)}g(n)^{n+1}$

More on length bounds

Deciding $M \in \overline{\mathcal{M}}$ is in NEXP:

- Almeida and Steinberg (2009) give $2^{n^2 \log n}$ length bound for the zero matrix
- For $\mathcal{M} \subseteq \mathbb{N}^{n \times n}$, Kiefer and Mascle (2019) give a n^5 length bound for the zero matrix, and $M_1, \ldots, M_{n^5} \in \mathcal{M}$ such that $\mathbf{0} = M_1 \cdots M_{n^5}$ can be computed in polynomial time
- A polynomial upper bound for the zero matrix in the rational case is an open problem

Concluding remarks

Some open problems:

- Can the size bound be reduced by one exponential?
- Is there a polynomial-time algorithm for deciding finitness?
- What is the complexity of the membership problem?