The asymptotic size of finite irreducible semigroups of rational matrices

Stefan Kiefer[1] Andrew Ryzhikov[2]

[1]University of Oxford

[2]University of Warsaw

STACS

Grenoble, 11 March 2026

How large can finite matrix semigroups get?

Linear loop and associated 2×2 generators

```
while (*)
  if (*)
    x = -y
    y = x - y
  else
    x = x - y
    y = -y
```

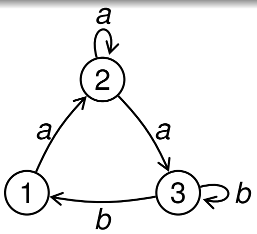
$$\left\{ \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \right\}$$

The two matrices generate the finite semigroup

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \right\}.$$

These matrices show the loop's possible actions on $\begin{pmatrix} \mathtt{x} \\ \mathtt{y} \end{pmatrix}$.

Unambiguous NFA and associated generators



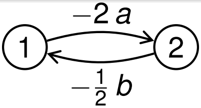
$$M(a) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad M(b) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

The NFA is unambiguous.
The two matrices generate the finite semigroup

$$\left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \right\}.$$

These matrices encode all transition matrices induced by all words in $\{a, b\}^+$.
There are at most $|\{0, 1\}^{Q \times Q}| = 2^{n^2}$ such matrices.

$\mathbb{Q}$-weighted automata



$$M(a) = \begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix}, \; M(b) = \begin{pmatrix} 0 & 0 \\ -\frac{1}{2} & 0 \end{pmatrix}$$

For $w = w_1 \cdots w_k \in \{a, b\}^+$ write $M(w) := M(w_1) \cdots M(w_k)$.

Matrices $M(a), M(b)$ generate the (here: finite) semigroup $\{M(w) : w \in \{a, b\}^+\}$ of weighted transition matrices

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ -\frac{1}{2} & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Given also an initial state vector $\alpha \in \mathbb{Q}^2$ and a final state vector $\eta \in \mathbb{Q}^2$, the automaton maps a word $w \in \{a, b\}^+$ to its weight $\alpha^\top M(w)\eta \in \mathbb{Q}$.

Decision problem:

given an automaton, is $\{\alpha^\top M(w)\eta : w \in \{a, b\}^+\}$ finite?

A large 0/1 matrix semigroup

Consider the set of 0/1 matrices that are nonzero only in the top-right quadrant:

$$\left\{ \begin{pmatrix} 0 & 0 & b_1 & b_2 \\ 0 & 0 & b_3 & b_4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} : b_1, b_2, b_3, b_4 \in \{0, 1\} \right\} .$$

There are $2^{n^2/4}$ such matrices.

$$\left\{ \begin{array}{cccc}
\begin{pmatrix} 0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&0&0\\0&0&0&1\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&0&0\\0&0&1&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&0&0\\0&0&1&1\\0&0&0&0\\0&0&0&0 \end{pmatrix}, \\
\begin{pmatrix} 0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&0&1\\0&0&0&1\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&0&1\\0&0&1&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&0&1\\0&0&1&1\\0&0&0&0\\0&0&0&0 \end{pmatrix}, \\
\begin{pmatrix} 0&0&1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&1&0\\0&0&0&1\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&1&0\\0&0&1&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&1&0\\0&0&1&1\\0&0&0&0\\0&0&0&0 \end{pmatrix}, \\
\begin{pmatrix} 0&0&1&1\\0&0&0&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&1&1\\0&0&0&1\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&1&1\\0&0&1&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, & \begin{pmatrix} 0&0&1&1\\0&0&1&1\\0&0&0&0\\0&0&0&0 \end{pmatrix}
\end{array} \right\} .$$

Any product of two such matrices is zero ➔ semigroup

A large $0/1$ matrix semigroup

Consider the set of $0/1$ matrices that are nonzero only in the top-right quadrant:

$$\left\{ \begin{pmatrix} 0 & 0 & b_1 & b_2 \\ 0 & 0 & b_3 & b_4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} : b_1, b_2, b_3, b_4 \in \{0, 1\} \right\} .$$

There are $2^{n^2/4}$ such matrices.

This semigroup (viewed as NFA) is not strongly connected.

One can make it strongly connected by adding all matrix units (matrices with a single nonzero entry) and taking the closure.

Proposition

For every n there is a strongly connected $0/1$ *matrix semigroup of size at least* $2^{\lfloor n^2/4 \rfloor}$*.*

How large can 0/1 matrix semigroups get?

lower bound: $2^{\lfloor n^2/4 \rfloor}$

upper bound: 2^{n^2}

This leaves a gap. We don't know how to fill it.

How large can 0/1 matrix semigroups get?

lower bound: $2^{\lfloor n^2/4 \rfloor}$

upper bound: 2^{n^2}

This leaves a gap. We don't know how to fill it.
Or perhaps we do: persistent prompting of chatGPT led to a nice combinatorial argument for an upper bound $2^{n^2/4+o(n^2)}$.

How large can 0/1 matrix semigroups get?

lower bound: $2^{\lfloor n^2/4 \rfloor}$

upper bound: 2^{n^2}

This leaves a gap. We don't know how to fill it.
Or perhaps we do: persistent prompting of chatGPT led to a nice combinatorial argument for an upper bound $2^{n^2/4+o(n^2)}$.

How large can finite matrix semigroups get?

Are there even larger finite matrix semigroups?

By allowing entries other than 0/1 we can have arbitrarily large finite matrix semigroups:

$$\left\{ \begin{pmatrix} 0 & 0 & b_1 & b_2 \\ 0 & 0 & b_3 & b_4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} : b_1, b_2, b_3, b_4 \in \{-2, -1, 0, +1, +2\} \right\}$$

Upper bound after imposing strong connectedness?

Being strongly connected is less meaningful in the rationals.

The "right" notion is irreducibility:

Definition

Let $S \subseteq \mathbb{Q}^{n \times n}$ be a semigroup.
A vector space $\mathcal{V} \subseteq \mathbb{Q}^n$ is S-invariant if $X\mathcal{V} \subseteq \mathcal{V}$ for all $X \in S$.
The semigroup S is irreducible if the only S-invariant subspaces of $\mathbb{Q}^n$ are $\mathbb{Q}^n$ and $\{\vec{0}\}$.

Irreducibility

The semigroup from before

$$\left\{ \begin{pmatrix} 0 & 0 & b_1 & b_2 \\ 0 & 0 & b_3 & b_4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} : b_1, b_2, b_3, b_4 \in \{-2, -1, 0, +1, +2\} \right\}$$

is not irreducible because it has non-trivial invariant spaces such as

$$\mathcal{V} := \left\{ \begin{pmatrix} q \\ q \\ 0 \\ 0 \end{pmatrix} : q \in \mathbb{Q} \right\} .$$

Indeed, $\begin{pmatrix} 0 & 0 & b_1 & b_2 \\ 0 & 0 & b_3 & b_4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} q \\ q \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \in \mathcal{V}.$

Irreducibility

The semigroup from before

$$\left\{ \begin{pmatrix} 0 & 0 & b_1 & b_2 \\ 0 & 0 & b_3 & b_4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} : b_1, b_2, b_3, b_4 \in \{-2, -1, 0, +1, +2\} \right\}$$

is not irreducible.

We can make it irreducible similarly as before: adjoin all matrix units and consider the generated matrix semigroup.

This (now irreducible) semigroup is infinite.

It is finite if we restrict the entries to $-1, 0, +1$. This gives:

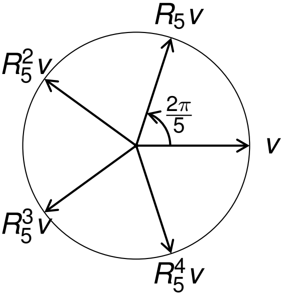
Proposition

For every n there is an irreducible $0/\pm 1$ *matrix semigroup of size at least* $3^{\lfloor n^2/4 \rfloor}$.

Cyclic finite matrix semigroups (over $\mathbb{R}$!)

For any integer $k \geq 1$, let

$$R_k := \begin{pmatrix} \cos(2\pi/k) & -\sin(2\pi/k) \\ \sin(2\pi/k) & \cos(2\pi/k) \end{pmatrix}.$$



Then R_k is rotation by angle $2\pi/k$, and for every $m \geq 1$,

$$R_k^m = \begin{pmatrix} \cos(2\pi m/k) & -\sin(2\pi m/k) \\ \sin(2\pi m/k) & \cos(2\pi m/k) \end{pmatrix}.$$

So R_k generates a finite matrix semigroup of size k:

$$\{R_k, R_k^2, \ldots, R_k^k = I\}$$

So there is no bound on the size of finite irreducible 2×2 matrix groups!

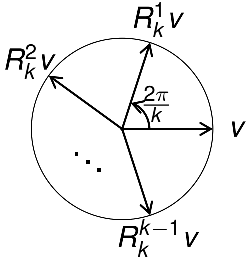
But R_k is irrational (unless $k \in \{1, 2, 4\}$).

How large can finite matrix semigroups get?

Without irreducibility arbitrarily large:

$$\left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \{0, 1, \ldots, k\} \right\}$$

Without rationality arbitrarily large:



With both irreducibility and rationality: at least $3^{\lfloor n^2/4 \rfloor}$.

Is there an upper bound?

Finite irreducible rational matrix semigroups

Upper bound from [Berstel, Reutenauer: Rational Series and Their Languages, 1988], going back to [Schützenberger, 1962]:

$$\text{at most } (2n+1)^{n^2} \in 2^{O(n^2 \log n)} .$$

Technique: analyse the traces of the characteristic polynomials of the matrices. The quantity $2n+1$ in the bound above is the number of possible traces in the set $\{-n, -n+1, \ldots, n\}$.

Theorem (the main contribution of our paper)

Any finite irreducible semigroup of rational $n \times n$ matrices has at most 3^{n^2} elements.

"Asymptotically", this matches the lower bound $3^{\lfloor n^2/4 \rfloor}$.
Technique: Group case + semigroup theory + linear algebra.

The maximal order of finite rational matrix groups

A folklore result says: any finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$ is conjugate to a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$.

An elementary proof shows: the size ("order") of any finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$ divides $(2n)!$,
so the order is at most $(2n)! \in 2^{O(n \log n)}$.

This matches asymptotically a lower bound $2^n n!$ via signed permutation matrices:

$$\begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & +1 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & +1 & 0 & 0 & 0 \end{pmatrix}$$

The maximal order of finite rational matrix groups

[Friedland, 1997] showed that the lower bound $2^n n!$ is tight for almost all n.

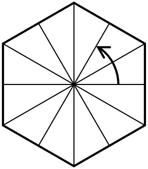
Rests on [Weisfeiler, 1984], which in turn is based on the classification of finite simple groups.

[Feit, unpublished] showed that $2^n n!$ is tight for all n except $2, 4, 6, 7, 8, 9, 10$.

Rests on [Weisfeiler, unpublished, left behind], also based on the classification of finite simple groups.

The largest group for $n = 2$: dihedral group of order 12,

generated by $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$.



➔ The largest ($2^{\Theta(n \log n)}$) groups are explicitly known for all n.

Summary

Proposition (lower bound)

There is an irreducible semigroup of $n \times n$ matrices over $\{-1, 0, +1\}$ with at least $3^{\lfloor n^2/4 \rfloor}$ elements.

Theorem (the main contribution of our paper)

Any finite irreducible semigroup of rational $n \times n$ matrices has at most 3^{n^2} elements.

Technique: Group case + semigroup theory + linear algebra.

[Steinberg, 2026, arxiv] (referencing our paper) has a 4-page proof.

Diameter

Let S be a finite semigroup, generated by $S_0 \subseteq S$.

The depth of $X \in S$ is the length of the shortest product of elements from S_0 resulting in X.

The diameter of S is the maximum depth, taken over all S_0 and all $X \in S$.

[Bumpus et al., 2020] proved that the diameter of finite rational semigroups is $2^{O(n^2 \log n)}$, not requiring irreducibility.

[Almeida/Steinberg, 2009] proved that the depth of the 0-matrix is at most $(2n-1)n^2 \in 2^{O(n^2 \log n)}$, not requiring irreducibility.

Our main result implies that the depth of the 0-matrix is at most 3^{n^2}, not requiring irreducibility.

Lower bound on the diameter: $2^{n+\Omega(\sqrt{n \log n})}$ [Panteleev, 2015]

Lower bound on the depth of the 0 matrix: $\Omega(n^2)$ [Rystsov, 1997]