Finite Rational Matrix Semigroups have at most Exponential Size

Rida Ait El Manssour, Roland Guttenberg, Nathan Lhote, Mahsa Shirmohammadi, James Worrell

Workshop on Loop Invariants and Algebraic Reasoning

July 7 2025

Motivation: Synthesizing Loop Invariants

Motivation: Synthesizing Loop Invariants

$x = 0$
$y = 0$
while true do
  if $x > 0$ **then**
    x=2x-y-1
    y=y-1
  else
    x=2y-x+1
    y=y+1
  end if
end while

Motivation: Synthesizing Loop Invariants

$x = 0$
$y = 0$
while true do
    if $x > 0$ **then**
        x=2x-y-1
        y=y-1
    else
        x=2y-x+1
        y=y+1
    end if
end while

Can we ever have $x = y + 2$?

Motivation: Synthesizing Loop Invariants

$x = 0$
$y = 0$
while true do
  if $x > 0$ **then**
    x=2x-y-1
    y=y-1
  else
    x=2y-x+1
    y=y+1
  end if
end while

Can we ever have $x = y + 2$? No. Loop Invariant "$x = y$"

Motivation: Synthesizing Loop Invariants

$x = 0$
$y = 0$
while true do
  if $x > 0$ **then**
    x=2x-y-1
    y=y-1
  else
    x=2y-x+1
    y=y+1
  end if
end while

$x = 0$
$y = 0$
while true do
  Non-Det.Choice:
  Option 1: x=2x-y-1; y=y-1
  Option 2: x=2y-x+1; y=y+1
end while

Can we ever have $x = y + 2$? No. Loop Invariant "$x = y$"

Motivation: Synthesizing Loop Invariants

$x = 0$
$y = 0$
while true do
  if $x > 0$ **then**
    x=2x-y-1
    y=y-1
  else
    x=2y-x+1
    y=y+1
  end if
end while

$x = 0$
$y = 0$
while true do
  Non-Det.Choice:
  Option 1: x=2x-y-1; y=y-1
  Option 2: x=2y-x+1; y=y+1
end while

For programs with only linear updates $\mathbf{x} := A\mathbf{x} + \mathbf{b}$ and no conditional branching,

Can we ever have $x = y + 2$? No. Loop Invariant "$x = y$"

Motivation: Synthesizing Loop Invariants

$x = 0$
$y = 0$
while true do
    if $x > 0$ **then**
        x=2x-y-1
        y=y-1
    else
        x=2y-x+1
        y=y+1
    end if
end while

$x = 0$
$y = 0$
while true do
    Non-Det.Choice:
    Option 1: x=2x-y-1; y=y-1
    Option 2: x=2y-x+1; y=y+1
end while

For programs with only linear updates $\mathbf{x} := A\mathbf{x} + \mathbf{b}$ and no conditional branching, *all* polynomial loop invariants can be automatically synthesized.

Can we ever have $x = y + 2$? No. Loop Invariant "$x = y$"

Matrix Semigroups

Matrix Semigroups

We can simulate states and constants using additional variables.

Matrix Semigroups

We can simulate states and constants using additional variables.

Therefore programs as before can be reduced to matrix vector multiplication

Matrix Semigroups

We can simulate states and constants using additional variables.

Therefore programs as before can be reduced to matrix vector multiplication

while true do

  Non-Det.Choice:

  Option 1: $\mathbf{x} = A_1\mathbf{x}$

  Option 2: $\ldots$

  Option r: $\mathbf{x} = A_r\mathbf{x}$

end while

Matrix Semigroups

We can simulate states and constants using additional variables.

Therefore programs as before can be reduced to matrix vector multiplication

while true do

Non-Det.Choice:

Option 1: $\mathbf{x} = A_1\mathbf{x}$

Option 2: $\ldots$

Option r: $\mathbf{x} = A_r\mathbf{x}$

end while

Hence we study matrix semigroups, i.e. sets of the form

Matrix Semigroups

We can simulate states and constants using additional variables.

Therefore programs as before can be reduced to matrix vector multiplication

while true do

  Non-Det.Choice:

  Option 1: $\mathbf{x} = A_1\mathbf{x}$

  Option 2: $\dots$

  Option r: $\mathbf{x} = A_r\mathbf{x}$

end while

Hence we study matrix semigroups, i.e. sets of the form

$$\langle A_1, \dots, A_r \rangle := \{A_{i_1} \circ \dots \circ A_{i_n} \mid n \in \mathbb{N}, i_j \in \{1, \dots, r\}\}$$

Prior Work

Prior Work

Theorem (Derksen, Jeandel, Koiran 2005)

Given invertible matrices $A_1, \ldots, A_r \in GL_n(\overline{\mathbb{Q}})$, the Zariski closure of $\langle A_1, \ldots, A_r \rangle$/the optimal polynomial invariants can be computed.

Prior Work

Theorem (Derksen, Jeandel, Koiran 2005)

Given invertible matrices $A_1, \ldots, A_r \in GL_n(\overline{\mathbb{Q}})$, the Zariski closure of $\langle A_1, \ldots, A_r \rangle$/the optimal polynomial invariants can be computed.

Theorem (Hrushovski, Ouaknine, Pouly, Worrell, 2018)

Given not necessarily invertible matrices $A_1, \ldots, A_r \in \overline{\mathbb{Q}}^{n \times n}$ for some n, the Zariski closure of $\langle A_1, \ldots, A_r \rangle$ can be computed.

Prior Work

Theorem (Derksen, Jeandel, Koiran 2005)

Given invertible matrices $A_1, \ldots, A_r \in GL_n(\overline{\mathbb{Q}})$, the Zariski closure of $\langle A_1, \ldots, A_r \rangle$/the optimal polynomial invariants can be computed.

Theorem (Hrushovski, Ouaknine, Pouly, Worrell, 2018)

Given not necessarily invertible matrices $A_1, \ldots, A_r \in \overline{\mathbb{Q}}^{n \times n}$ for some n, the Zariski closure of $\langle A_1, \ldots, A_r \rangle$ can be computed.

Theorem (Nosan, Pouly, Shirmohammadi, Worrell 2022)

Given invertible matrices $A_1, \ldots, A_r \in GL_n(\overline{\mathbb{Q}})$, the Zariski closure can be computed in 7-EXPTIME.

Prior Work

Theorem (Derksen, Jeandel, Koiran 2005)

Given invertible matrices $A_1, \dots, A_r \in GL_n(\overline{\mathbb{Q}})$*, the Zariski closure of* $\langle A_1, \dots, A_r \rangle$*/the optimal polynomial invariants can be computed.*

Theorem (Hrushovski, Ouaknine, Pouly, Worrell, 2018)

Given not necessarily invertible matrices $A_1, \dots, A_r \in \overline{\mathbb{Q}}^{n \times n}$ *for some* n*, the Zariski closure of* $\langle A_1, \dots, A_r \rangle$ *can be computed.*

Theorem (Nosan, Pouly, Shirmohammadi, Worrell 2022)

Given invertible matrices $A_1, \dots, A_r \in GL_n(\overline{\mathbb{Q}})$*, the Zariski closure can be computed in 7-EXPTIME.*

Our goal is to reduce the complexity/generalize to semigroups.

Subject + Context of This Talk

Subject + Context of This Talk

First Step: Identify and solve easy cases.

Subject + Context of This Talk

First Step: Identify and solve easy cases.

First such case and subject of this talk: Finite matrix semigroups.

Subject + Context of This Talk

First Step: Identify and solve easy cases.

First such case and subject of this talk: Finite matrix semigroups.

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Subject + Context of This Talk

First Step: Identify and solve easy cases.
First such case and subject of this talk: Finite matrix semigroups.

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp.)

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp.)

Corollary

The membership problem in finite semigroups is PSPACE-complete:

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp.)

Corollary

The membership problem in finite semigroups is PSPACE-complete:
Input: Finite semigroup $S = \langle A_1, \ldots, A_r \rangle$, matrix A.

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq \exp.$)

Corollary

The membership problem in finite semigroups is PSPACE-complete:
Input: Finite semigroup $S = \langle A_1, \ldots, A_r \rangle$, matrix A.
Output: Is $A \in \langle A_1, \ldots, A_r \rangle$?

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp.)

Corollary

The membership problem in finite semigroups is PSPACE-complete:
Input: Finite semigroup $S = \langle A_1, \ldots, A_r \rangle$, matrix A.
Output: Is $A \in \langle A_1, \ldots, A_r \rangle$?

Proof.

$\square$

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \dots, A_r \rangle \subseteq \mathbb{Q}^{n\times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \dots, A_r$. (I.e. semigroups have $|S| \leq \exp$.)

Corollary

The membership problem in finite semigroups is PSPACE-complete:
Input: Finite semigroup $S = \langle A_1, \dots, A_r \rangle$, matrix A.
Output: Is $A \in \langle A_1, \dots, A_r \rangle$?

Proof.

For the upper bound, simply guess the product leading to A.
(NPSPACE=PSPACE)

$\square$

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp.)

Corollary

The membership problem in finite semigroups is PSPACE-complete:
Input: Finite semigroup $S = \langle A_1, \ldots, A_r \rangle$, matrix A.
Output: Is $A \in \langle A_1, \ldots, A_r \rangle$?

Proof.

For the upper bound, simply guess the product leading to A. (NPSPACE=PSPACE)
For the lower bound, reduce from DFA-intersection-emptiness. □

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n\times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp.)

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp.)

Theorem (Folklore)

If the group $G = \langle A_1, \ldots, A_r \rangle \subseteq GL_n(\mathbb{Q})$ is finite, then $|G| \leq 2^n \cdot n!$.

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ *is finite, then every matrix* $A \in S$ *has polynomial bitsize in terms of* $A_1, \ldots, A_r$. *(I.e. semigroups have* $|S| \leq$ *exp.)*

Theorem (Folklore)

If the group $G = \langle A_1, \ldots, A_r \rangle \subseteq GL_n(\mathbb{Q})$ *is finite, then* $|G| \leq 2^n \cdot n!$.

Theorem (Bumpus, Haase, Kiefer, Stoienescu, Tanner 2020)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle$ *is finite, then every element can be obtained by an exponential length product.*

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp.)

Theorem (Folklore)

If the group $G = \langle A_1, \ldots, A_r \rangle \subseteq GL_n(\mathbb{Q})$ is finite, then $|G| \leq 2^n \cdot n!$.

Theorem (Bumpus, Haase, Kiefer, Stoienescu, Tanner 2020)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle$ is finite, then every element can be obtained by an exponential length product. (I.e. semigroups have $|S| \leq$ 2-exp.)

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp.)

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n\times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp.)

Developed a tool which is applicable for general semigroups.

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ *is finite, then every matrix* $A \in S$ *has polynomial bitsize in terms of* $A_1, \ldots, A_r$. *(I.e. semigroups have* $|S| \leq$ *exp.)*

Developed a tool which is applicable for general semigroups.

Theorem (Our Main Tool)

Given a number field K *and semigroup* $S = \langle A_1, \ldots, A_r \rangle \subseteq K^{n \times n}$, *we can in PTIME compute an irreducible component decomposition of* S *over* K.

Subject + Context of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp.)

Developed a tool which is applicable for general semigroups.

Theorem (Our Main Tool)

Given a number field K and semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq K^{n \times n}$, we can in PTIME compute an irreducible component decomposition of S over K.

Rest of this talk: Explains irreducible components + theorems

Irreducible Semigroups

Irreducible Semigroups

We usually represent matrix semigroups as follows.

Irreducible Semigroups

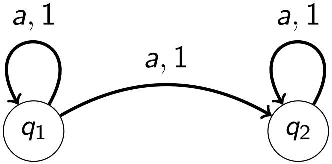
We usually represent matrix semigroups as follows.

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

Irreducible Semigroups

We usually represent matrix semigroups as follows.

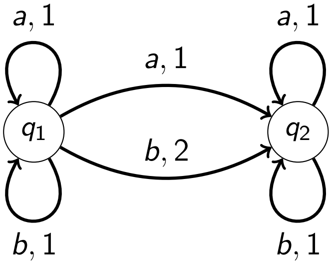
$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



Irreducible Semigroups

We usually represent matrix semigroups as follows.

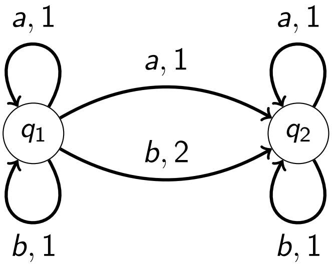
$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



We usually represent matrix semigroups as follows.

$n \times n \leftrightarrow n$ states of a finite automaton.

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



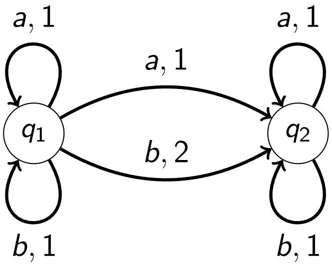
Irreducible Semigroups

We usually represent matrix semigroups as follows.

$n \times n \leftrightarrow n$ states of a finite automaton.

r (number of matrices) $\leftrightarrow |\Sigma| = r$

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



Irreducible Semigroups

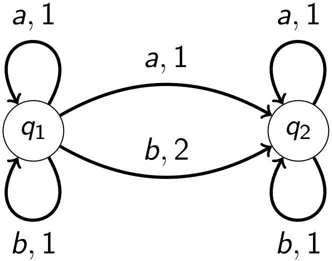
We usually represent matrix semigroups as follows.

$n \times n \leftrightarrow n$ states of a finite automaton.

r (number of matrices) $\leftrightarrow |\Sigma| = r$

$A_i \leftrightarrow$ transition matrix on letter a_i

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



Irreducible Semigroups

We usually represent matrix semigroups as follows.

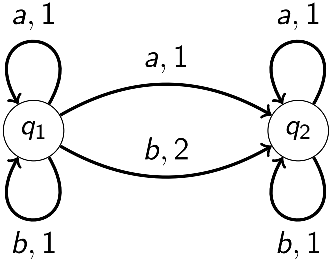
$n \times n \leftrightarrow n$ states of a finite automaton.

r (number of matrices) $\leftrightarrow |\Sigma| = r$

$A_i \leftrightarrow$ transition matrix on letter a_i

Multiplication $A_i \cdot A_j \leftrightarrow$ Composing letters

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



Irreducible Semigroups

We usually represent matrix semigroups as follows.

$n \times n \leftrightarrow n$ states of a finite automaton.

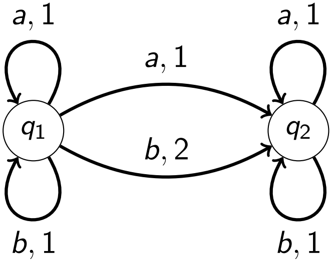
r (number of matrices) $\leftrightarrow |\Sigma| = r$

$A_i \leftrightarrow$ transition matrix on letter a_i

Multiplication $A_i \cdot A_j \leftrightarrow$ Composing letters

Does strongly-connected have a meaning for the semigroup?

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



Irreducible Semigroups

Irreducible Semigroups

Does strongly-connected have a meaning for the semigroup?

Irreducible Semigroups

Does strongly-connected have a meaning for the semigroup?

Not immediately. If $P \in GL_n(K)$ is some base change, then

Irreducible Semigroups

Does strongly-connected have a meaning for the semigroup?

Not immediately. If $P \in GL_n(K)$ is some base change, then $S \simeq PSP^{-1}$, but S might be strongly-connected and PSP^{-1} is not.

Irreducible Semigroups

Does strongly-connected have a meaning for the semigroup?

Not immediately. If $P \in GL_n(K)$ is some base change, then $S \simeq PSP^{-1}$, but S might be strongly-connected and PSP^{-1} is not.

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

Irreducible Semigroups

Does strongly-connected have a meaning for the semigroup?

Not immediately. If $P \in GL_n(K)$ is some base change, then $S \simeq PSP^{-1}$, but S might be strongly-connected and PSP^{-1} is not.

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

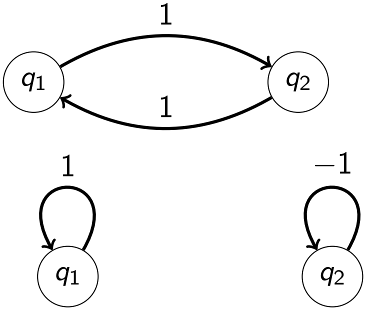
$$\begin{tikzcd} q_1 \arrow[rr, bend left, "1"] & & q_2 \arrow[ll, bend left, "1"] \end{tikzcd}$$

Irreducible Semigroups

Does strongly-connected have a meaning for the semigroup?

Not immediately. If $P \in GL_n(K)$ is some base change, then $S \simeq PSP^{-1}$, but S might be strongly-connected and PSP^{-1} is not.

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



Irreducible Semigroups

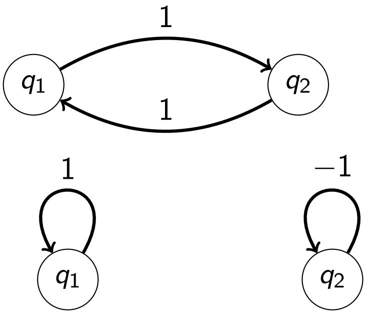
Does strongly-connected have a meaning for the semigroup?

Not immediately. If $P \in GL_n(K)$ is some base change, then $S \simeq PSP^{-1}$, but S might be strongly-connected and PSP^{-1} is not.

Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



Irreducible Semigroups

Does strongly-connected have a meaning for the semigroup?

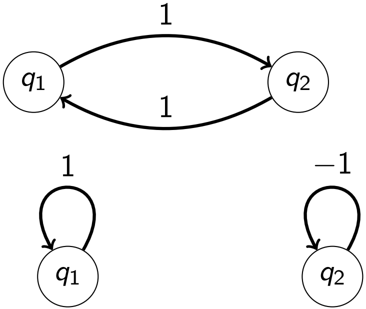
Not immediately. If $P \in GL_n(K)$ is some base change, then $S \simeq PSP^{-1}$, but S might be strongly-connected and PSP^{-1} is not.

Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

Mainly for non-unary alphabet, otherwise Jordan normal form.

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



Irreducible Semigroups

Does strongly-connected have a meaning for the semigroup?

Not immediately. If $P \in GL_n(K)$ is some base change, then $S \simeq PSP^{-1}$, but S might be strongly-connected and PSP^{-1} is not.

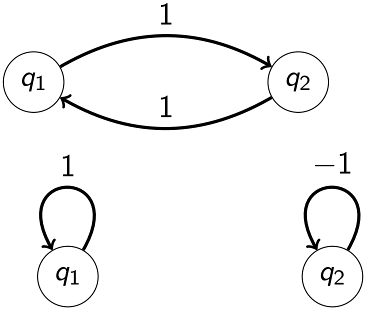
Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

Mainly for non-unary alphabet, otherwise Jordan normal form.

Remark: Stably-strongly-connected depends on the number field.

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



Irreducible Semigroups

Does strongly-connected have a meaning for the semigroup?

Not immediately. If $P \in GL_n(K)$ is some base change, then $S \simeq PSP^{-1}$, but S might be strongly-connected and PSP^{-1} is not.

Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

Mainly for non-unary alphabet, otherwise Jordan normal form.

Remark: Stably-strongly-connected depends on the number field.

Irreducible Semigroups

Does strongly-connected have a meaning for the semigroup?

Not immediately. If $P \in GL_n(K)$ is some base change, then $S \simeq PSP^{-1}$, but S might be strongly-connected and PSP^{-1} is not.

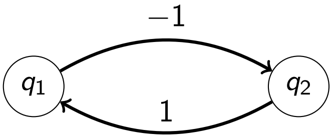
Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

Mainly for non-unary alphabet, otherwise Jordan normal form.

Remark: Stably-strongly-connected depends on the number field.

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$



Irreducible Semigroups

Does strongly-connected have a meaning for the semigroup?

Not immediately. If $P \in GL_n(K)$ is some base change, then $S \simeq PSP^{-1}$, but S might be strongly-connected and PSP^{-1} is not.

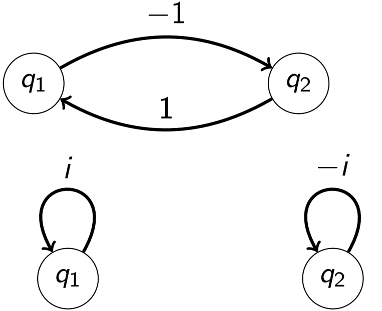
Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

Mainly for non-unary alphabet, otherwise Jordan normal form.

Remark: Stably-strongly-connected depends on the number field.

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$



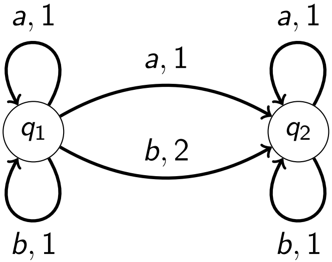
Irreducible Semigroups

Irreducible Semigroups

Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

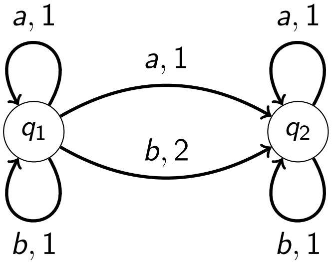


Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

S is irreducible if there is no vector space $\{0\} \neq V \subsetneq \mathbb{Q}^n$ s.t. $S \cdot V \subseteq V$.

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



Irreducible Semigroups

Definition

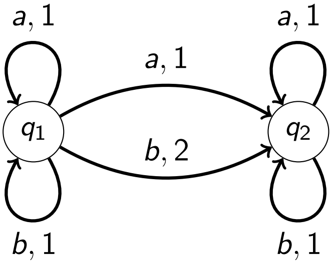
S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

S is irreducible if there is no vector space $\{0\} \neq V \subsetneq \mathbb{Q}^n$ s.t. $S \cdot V \subseteq V$.

Lemma

Let S be a semigroup. T.F.A.E.:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



Irreducible Semigroups

Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

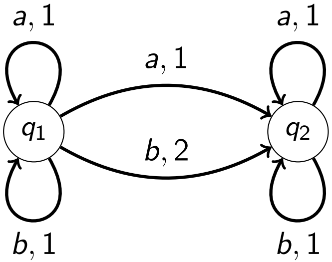
S is irreducible if there is no vector space $\{0\} \neq V \subsetneq \mathbb{Q}^n$ s.t. $S \cdot V \subseteq V$.

Lemma

Let S be a semigroup. T.F.A.E.:

1. *S is not stably-strongly-connected.*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



Irreducible Semigroups

Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

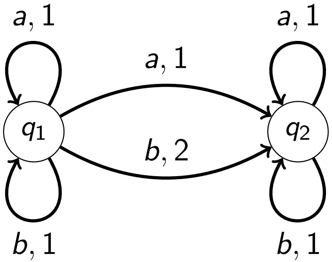
S is irreducible if there is no vector space $\{0\} \neq V \subsetneq \mathbb{Q}^n$ s.t. $S \cdot V \subseteq V$.

Lemma

Let S be a semigroup. T.F.A.E.:

1. *S is not stably-strongly-connected.*
2. *S is not irreducible.*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

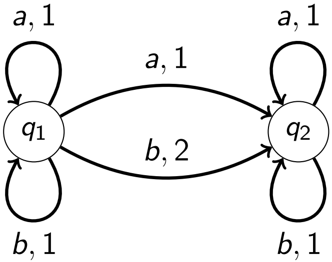
S is irreducible if there is no vector space $\{0\} \neq V \subsetneq \mathbb{Q}^n$ s.t. $S \cdot V \subseteq V$.

Lemma

Let S be a semigroup. T.F.A.E.:

1. *S is not stably-strongly-connected.*
2. *S is not irreducible.*
3. *$\exists P \in GL_n(\mathbb{Q})$ s.t. all $A \in PSP^{-1}$ are block-upper-triangular with ≥ 2 blocks.*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



Irreducible Semigroups

Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

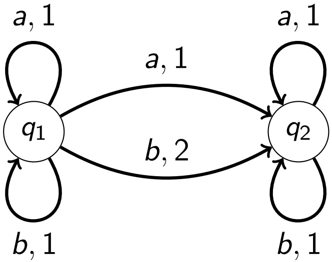
S is irreducible if there is no vector space $\{0\} \neq V \subsetneq \mathbb{Q}^n$ s.t. $S \cdot V \subseteq V$.

Lemma

Let S be a semigroup. T.F.A.E.:

1. *S is not stably-strongly-connected.*
2. *S is not irreducible.*
3. *$\exists P \in GL_n(\mathbb{Q})$ s.t. all $A \in PSP^{-1}$ are block-upper-triangular with ≥ 2 blocks.*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



$$C = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

Irreducible Semigroups

Definition

S is stably-strongly-connected if every base change PSP^{-1} is strongly-connected.

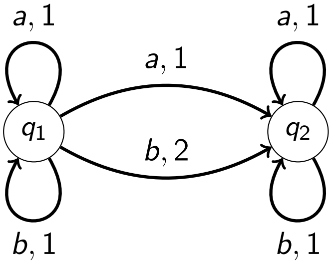
S is irreducible if there is no vector space $\{0\} \neq V \subsetneq \mathbb{Q}^n$ s.t. $S \cdot V \subseteq V$.

Lemma

Let S be a semigroup. T.F.A.E.:

1. *S is not stably-strongly-connected.*
2. *S is not irreducible.*
3. *$\exists P \in GL_n(\mathbb{Q})$ s.t. all $A \in PSP^{-1}$ are block-upper-triangular with ≥ 2 blocks.*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



$$C = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

Irreducible Component Decomposition

Irreducible Component Decomposition

Definition

Let $S \subseteq \mathbb{Q}^{n \times n}$ be a semigroup.

Irreducible Component Decomposition

Definition

Let $S \subseteq \mathbb{Q}^{n \times n}$ be a semigroup. A conjugated semigroup $S' = PSP^{-1}$ is an irreducible component decomposition (ICD)

Irreducible Component Decomposition

Definition

Let $S \subseteq \mathbb{Q}^{n \times n}$ be a semigroup. A conjugated semigroup $S' = PSP^{-1}$ is an irreducible component decomposition (ICD) if all $A \in S'$ are block-upper-triangular with irreducible diagonal blocks.

$$\begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & 0 & \ddots & * \\ 0 & \dots & 0 & * \end{pmatrix}$$

Irreducible Component Decomposition

Definition

Let $S \subseteq \mathbb{Q}^{n\times n}$ be a semigroup. A conjugated semigroup $S' = PSP^{-1}$ is an irreducible component decomposition (ICD) if all $A \in S'$ are block-upper-triangular with irreducible diagonal blocks.

$$\begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & 0 & \ddots & * \\ 0 & \dots & 0 & * \end{pmatrix}$$

Irreducible Component Decomposition

Definition

Let $S \subseteq \mathbb{Q}^{n\times n}$ be a semigroup. A conjugated semigroup $S' = PSP^{-1}$ is an irreducible component decomposition (ICD) if all $A \in S'$ are block-upper-triangular with irreducible diagonal blocks.

$$\begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & 0 & \ddots & * \\ 0 & \dots & 0 & * \end{pmatrix}$$

Intuition: ICD$\simeq$Jordan normal form for semigroups instead of single matrices.

Irreducible Component Decomposition

Definition

Let $S \subseteq \mathbb{Q}^{n\times n}$ be a semigroup. A conjugated semigroup $S' = PSP^{-1}$ is an irreducible component decomposition (ICD) if all $A \in S'$ are block-upper-triangular with irreducible diagonal blocks.

Intuition: ICD$\simeq$Jordan normal form for semigroups instead of single matrices.

Lemma

An ICD always exists.

$$\begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & 0 & \ddots & * \\ 0 & \dots & 0 & * \end{pmatrix}$$

Irreducible Component Decomposition

Definition

Let $S \subseteq \mathbb{Q}^{n\times n}$ be a semigroup. A conjugated semigroup $S' = PSP^{-1}$ is an irreducible component decomposition (ICD) if all $A \in S'$ are block-upper-triangular with irreducible diagonal blocks.

$$\begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & 0 & \ddots & * \\ 0 & \dots & 0 & * \end{pmatrix}$$

Intuition: ICD$\simeq$Jordan normal form for semigroups instead of single matrices.

Lemma

An ICD always exists.

Proof.

By induction on n. $\square$

Irreducible Component Decomposition

Definition

Let $S \subseteq \mathbb{Q}^{n\times n}$ be a semigroup. A conjugated semigroup $S' = PSP^{-1}$ is an irreducible component decomposition (ICD) if all $A \in S'$ are block-upper-triangular with irreducible diagonal blocks.

Intuition: ICD$\simeq$Jordan normal form for semigroups instead of single matrices.

Lemma

An ICD always exists.

$$\begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & 0 & \ddots & * \\ 0 & \dots & 0 & * \end{pmatrix}$$

Proof.

By induction on n.
If S is irreducible, then S is an ICD. $\square$

Irreducible Component Decomposition

Definition

Let $S \subseteq \mathbb{Q}^{n\times n}$ be a semigroup. A conjugated semigroup $S' = PSP^{-1}$ is an irreducible component decomposition (ICD) if all $A \in S'$ are block-upper-triangular with irreducible diagonal blocks.

Intuition: ICD$\simeq$Jordan normal form for semigroups instead of single matrices.

Lemma

An ICD always exists.

$$\begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & 0 & \ddots & * \\ 0 & \dots & 0 & * \end{pmatrix}$$

Proof.

By induction on n.

If S is irreducible, then S is an ICD.

If S is reducible, then let V be s.t. $S \cdot V \subseteq V$. $\square$

Irreducible Component Decomposition

Definition

Let $S \subseteq \mathbb{Q}^{n \times n}$ be a semigroup. A conjugated semigroup $S' = PSP^{-1}$ is an irreducible component decomposition (ICD) if all $A \in S'$ are block-upper-triangular with irreducible diagonal blocks.

Intuition: ICD$\simeq$Jordan normal form for semigroups instead of single matrices.

Lemma

An ICD always exists.

$$\begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & 0 & \ddots & * \\ 0 & \dots & 0 & * \end{pmatrix}$$

Proof.

By induction on n.
If S is irreducible, then S is an ICD.
If S is reducible, then let V be s.t. $S \cdot V \subseteq V$. Decompose $S\mid_V$ and $S\mid_{V^\perp}$ recursively. $\square$

Reminder: Goal of This Talk

Reminder: Goal of This Talk

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq \exp.$)

Developed a tool which is applicable for general semigroups.

Theorem (Our Main Tool)

Given a number field K and semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq K^{n \times n}$, we can in PTIME compute an irreducible component decomposition of S over K.

Finite Semigroups: Bound on Bitsize

Finite Semigroups: Bound on Bitsize

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq$ exp).

Finite Semigroups: Bound on Bitsize

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n\times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq exp$).

Step 1: W.l.o.g. $S = PSP^{-1}$ is in ICD.

Finite Semigroups: Bound on Bitsize

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \le \exp$).

Step 1: W.l.o.g. $S = PSP^{-1}$ is in ICD.

$$\begin{pmatrix} * & * & \ldots & * \\ 0 & * & \ldots & * \\ \vdots & 0 & \ddots & * \\ 0 & \ldots & 0 & * \end{pmatrix}$$

Finite Semigroups: Bound on Bitsize

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq exp$).

Step 1: W.l.o.g. $S = PSP^{-1}$ is in ICD.

Step 2+3: Separately deal with block-diagonal + above.

$$\begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & 0 & \ddots & * \\ 0 & \cdots & 0 & * \end{pmatrix}$$

Finite Semigroups: Bound on Bitsize

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq \exp$).

Step 1: W.l.o.g. $S = PSP^{-1}$ is in ICD.

Step 2+3: Separately deal with block-diagonal + above.

$$\begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & 0 & \ddots & * \\ 0 & \cdots & 0 & * \end{pmatrix}$$

Finite Semigroups: Bound on Bitsize

Theorem (This Talk)

If the semigroup $S = \langle A_1, \dots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \dots, A_r$. (I.e. semigroups have $|S| \leq exp$).

Step 1: W.l.o.g. $S = PSP^{-1}$ is in ICD.

Step 2+3: Separately deal with block-diagonal + above.

Above block-diagonal is easier, hence here I only explain the block-diagonal itself.

$$\begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & 0 & \ddots & * \\ 0 & \dots & 0 & * \end{pmatrix}$$

Finite Semigroups: Bound on Bitsize

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq \exp$).

Step 1: W.l.o.g. $S = PSP^{-1}$ is in ICD.

$$\begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & 0 & \ddots & * \\ 0 & \cdots & 0 & * \end{pmatrix}$$

Step 2+3: Separately deal with block-diagonal + above.

Above block-diagonal is easier, hence here I only explain the block-diagonal itself.

Hence w.l.o.g. S is irreducible.

Finite Semigroups: Bound on Bitsize

Theorem (This Talk)

If the semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$ is finite, then every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. semigroups have $|S| \leq \exp$).

Step 1: W.l.o.g. $S = PSP^{-1}$ is in ICD.

$$\begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & 0 & \ddots & * \\ 0 & \cdots & 0 & * \end{pmatrix}$$

Step 2+3: Separately deal with block-diagonal + above.

Above block-diagonal is easier, hence here I only explain the block-diagonal itself.

Hence w.l.o.g. S is irreducible.

In other words: We spent a large amount of this talk reducing to irreducible semigroups.

Finite Semigroups: Bound on Bitsize

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$*, every matrix* $A \in S$ *has polynomial bitsize in terms of* $A_1, \ldots, A_r$.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$*, every matrix* $A \in S$ *has polynomial bitsize in terms of* $A_1, \ldots, A_r$*.*

The technique is as follows:

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, *every matrix* $A \in S$ *has polynomial bitsize in terms of* $A_1, \ldots, A_r$.

The technique is as follows:

Lemma

Let V, V' *vector spaces, let* $T \colon V \to V'$ *linear*, $\mathbf{x} \in V$. *If*

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T\colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \dots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \dots, A_r$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Proof.

T polysize $\Rightarrow$ T^{-1} polysize. $\square$

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \dots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \dots, A_r$.

Proof.

T polysize $\Rightarrow$ T^{-1} polysize. Hence the product $\mathbf{x} = T^{-1} \cdot T(\mathbf{x})$ has polysize. □

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T\colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Therefore main difficulty: Finding the map T.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T\colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Therefore main difficulty: Finding the map T.

Every eigenvalue λ of $A \in S$ fulfills $\lambda = 0$ or $\lambda^q = 1$ for some $q \in \mathbb{N}$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Therefore main difficulty: Finding the map T.

Every eigenvalue λ of $A \in S$ fulfills $\lambda = 0$ or $\lambda^q = 1$ for some $q \in \mathbb{N}$.

Proof: From $|\{A, A^2, \ldots\}| < \infty$ we obtain $A^m = A^k$ for some $m > k$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T\colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n\times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Therefore main difficulty: Finding the map T.

Every eigenvalue λ of $A \in S$ fulfills $\lambda = 0$ or $\lambda^q = 1$ for some $q \in \mathbb{N}$.

Proof: From $|\{A, A^2, \ldots\}| < \infty$ we obtain $A^m = A^k$ for some $m > k$.
Therefore $\lambda^m = \lambda^k$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T: V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \dots, A_r \rangle \subseteq \mathbb{Q}^{n\times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \dots, A_r$.

Therefore main difficulty: Finding the map T.

Every eigenvalue λ of $A \in S$ fulfills
$\lambda = 0$ or $\lambda^q = 1$ for some $q \in \mathbb{N}$.

Proof: From $|\{A, A^2, \dots\}| < \infty$ we obtain
$A^m = A^k$ for some $m > k$.
Therefore $\lambda^m = \lambda^k$.
Hence either $\lambda = 0$ or $\lambda^{m-k} = 1$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T\colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Therefore main difficulty: Finding the map T.

Every eigenvalue λ of $A \in S$ fulfills $\lambda = 0$ or $\lambda^q = 1$ for some $q \in \mathbb{N}$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T\colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Therefore main difficulty: Finding the map T.

Every eigenvalue λ of $A \in S$ fulfills $\lambda = 0$ or $\lambda^q = 1$ for some $q \in \mathbb{N}$.

Remember that the trace is linear: $tr(A) := a_{11} + \cdots + a_{nn} = \lambda_1 + \cdots + \lambda_n$

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Therefore main difficulty: Finding the map T.

Every eigenvalue λ of $A \in S$ fulfills $\lambda = 0$ or $\lambda^q = 1$ for some $q \in \mathbb{N}$.

Remember that the trace is linear:
$tr(A) := a_{11} + \cdots + a_{nn} = \lambda_1 + \cdots + \lambda_n$
Claim: $tr(A) \in \{-n, \ldots, n\}$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Therefore main difficulty: Finding the map T.

Every eigenvalue λ of $A \in S$ fulfills $\lambda = 0$ or $\lambda^q = 1$ for some $q \in \mathbb{N}$.

Remember that the trace is linear:
$tr(A) := a_{11} + \cdots + a_{nn} = \lambda_1 + \cdots + \lambda_n$
Claim: $tr(A) \in \{-n, \ldots, n\}$.

To show: $|tr(A)| \leq n$ and $tr(A) \in \mathbb{Q} \cap \overline{\mathbb{Z}}$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Therefore main difficulty: Finding the map T.

Every eigenvalue λ of $A \in S$ fulfills $\lambda = 0$ or $\lambda^q = 1$ for some $q \in \mathbb{N}$.

Remember that the trace is linear:
$tr(A) := a_{11} + \cdots + a_{nn} = \lambda_1 + \cdots + \lambda_n$
Claim: $tr(A) \in \{-n, \ldots, n\}$.

To show: $|tr(A)| \leq n$ and $tr(A) \in \mathbb{Q} \cap \overline{\mathbb{Z}}$.
Obvious by the above.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$*, every matrix* $A \in S$ *has polynomial bitsize in terms of* $A_1, \ldots, A_r$*.*

Main difficulty: Finding the map T.
$tr(A) \in \{-n, \ldots, n\}$ for all $A \in S$.

The technique is as follows:

Lemma

Let V, V' *vector spaces, let* $T \colon V \to V'$ *linear,* $\mathbf{x} \in V$*. If*

- *Matrix of* T *has polysize,*
- T *is invertible,*
- *and* $T(\mathbf{x})$ *has polysize,*

then $\mathbf{x}$ *has polysize.*

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Main difficulty: Finding the map T.
$tr(A) \in \{-n, \ldots, n\}$ for all $A \in S$.

Fix basis $B \subseteq S$ of $VSp(S)$.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T: V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Main difficulty: Finding the map T.
$tr(A) \in \{-n, \ldots, n\}$ for all $A \in S$.

Fix basis $B \subseteq S$ of $VSp(S)$.

$T\colon VSp(S) \to \mathbb{Q}^{|B|}$,

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T\colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$*, every matrix* $A \in S$ *has polynomial bitsize in terms of* $A_1, \ldots, A_r$*.*

Main difficulty: Finding the map T.
$tr(A) \in \{-n, \ldots, n\}$ for all $A \in S$.

Fix basis $B \subseteq S$ of $VSp(S)$.

$T\colon VSp(S) \to \mathbb{Q}^{|B|}$, $A \mapsto (tr(A \cdot M))_{M \in B}$

The technique is as follows:

Lemma

Let V, V' *vector spaces, let* $T\colon V \to V'$ *linear,* $\mathbf{x} \in V$*. If*

- *Matrix of* T *has polysize,*
- T *is invertible,*
- *and* $T(\mathbf{x})$ *has polysize,*

then $\mathbf{x}$ *has polysize.*

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n\times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Main difficulty: Finding the map T.
$tr(A) \in \{-n, \ldots, n\}$ for all $A \in S$.

Fix basis $B \subseteq S$ of $VSp(S)$.

$T \colon VSp(S) \to \mathbb{Q}^{|B|}$, $A \mapsto (tr(A \cdot M))_{M \in B}$
Linear: Since tr is linear.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Main difficulty: Finding the map T.
$tr(A) \in \{-n, \ldots, n\}$ for all $A \in S$.

Fix basis $B \subseteq S$ of $VSp(S)$.

$T\colon VSp(S) \to \mathbb{Q}^{|B|}$, $A \mapsto (tr(A \cdot M))_{M \in B}$
Linear: Since tr is linear.
T Polysize: Choose small basis B.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T\colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Main difficulty: Finding the map T.
$tr(A) \in \{-n, \ldots, n\}$ for all $A \in S$.

Fix basis $B \subseteq S$ of $VSp(S)$.

$T : VSp(S) \to \mathbb{Q}^{|B|}$, $A \mapsto (tr(A \cdot M))_{M \in B}$
Linear: Since tr is linear.
T Polysize: Choose small basis B.

T invertible by irreducibility.

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T : V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Main difficulty: Finding the map T.
$tr(A) \in \{-n, \ldots, n\}$ for all $A \in S$.

Fix basis $B \subseteq S$ of $VSp(S)$.

$T\colon VSp(S) \to \mathbb{Q}^{|B|}$, $A \mapsto (tr(A \cdot M))_{M \in B}$
Linear: Since tr is linear.
T Polysize: Choose small basis B.

T invertible by irreducibility.
$T(A)$ polysize: $\in \{-n, \ldots, n\}^{\leq n^2}$

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T\colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \ldots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \ldots, A_r$.

Main difficulty: Finding the map T.
$tr(A) \in \{-n, \ldots, n\}$ for all $A \in S$.

Fix basis $B \subseteq S$ of $VSp(S)$.

$T\colon VSp(S) \to \mathbb{Q}^{|B|}$, $A \mapsto (tr(A \cdot M))_{M \in B}$
Linear: Since tr is linear.
T Polysize: Choose small basis B.

T invertible by irreducibility.
$T(A)$ polysize: $\in \{-n, \ldots, n\}^{\leq n^2}$

Hence we can apply the lemma. $\square$

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T\colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.

Finite Semigroups: Bound on Bitsize

Theorem

In an irreducible finite semigroup $S = \langle A_1, \dots, A_r \rangle \subseteq \mathbb{Q}^{n \times n}$, every matrix $A \in S$ has polynomial bitsize in terms of $A_1, \dots, A_r$.

$tr(A) \in \{-n, \dots, n\}$ for all $A \in S$.

Fix basis $B \subseteq S$ of $VSp(S)$.

$T \colon VSp(S) \to \mathbb{Q}^{|B|}$, $A \mapsto (tr(A \cdot M))_{M \in B}$
Linear: Since tr is linear.
T Polysize: Choose small basis B.

T invertible by irreducibility.
$T(A)$ polysize: $\in \{-n, \dots, n\}^{\leq n^2}$

Hence we can apply the lemma. □
Thank you for your attention!

The technique is as follows:

Lemma

Let V, V' vector spaces, let $T \colon V \to V'$ linear, $\mathbf{x} \in V$. If

- *Matrix of T has polysize,*
- *T is invertible,*
- *and $T(\mathbf{x})$ has polysize,*

then $\mathbf{x}$ has polysize.