Revisiting Finiteness of Matrix Monoids

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

SAMSA Workshop 2026

15. July 2025

Matrix Monoids + Problem of Interest

Matrix Monoids + Problem of Interest

Definition

The matrix monoid generated by $A_1, \ldots, A_r \in \mathbb{Q}^{n \times n}$ is the set

Matrix Monoids + Problem of Interest

Definition

The matrix monoid generated by $A_1, \ldots, A_r \in \mathbb{Q}^{n \times n}$ is the set $\langle A_1, \ldots, A_r \rangle := \{A_{i_1} \ldots A_{i_k} \mid k \in \mathbb{N}_0, i_j \in \{1, \ldots, r\}\}$,

Matrix Monoids + Problem of Interest

Definition

The matrix monoid generated by $A_1, \ldots, A_r \in \mathbb{Q}^{n \times n}$ is the set $\langle A_1, \ldots, A_r \rangle := \{A_{i_1} \ldots A_{i_k} \mid k \in \mathbb{N}_0, i_j \in \{1, \ldots, r\}\}$,

We are interested in the following problem.

Matrix Monoids + Problem of Interest

Definition

The matrix monoid generated by $A_1, \ldots, A_r \in \mathbb{Q}^{n \times n}$ is the set $\langle A_1, \ldots, A_r \rangle := \{A_{i_1} \ldots A_{i_k} \mid k \in \mathbb{N}_0, i_j \in \{1, \ldots, r\}\}$,

We are interested in the following problem.

Definition (Finiteness Problem)

Given $A_1, \ldots, A_r$, is $\langle A_1, \ldots, A_r \rangle$ finite?

Matrix Monoids + Problem of Interest

Definition

The matrix monoid generated by $A_1, \ldots, A_r \in \mathbb{Q}^{n \times n}$ is the set $\langle A_1, \ldots, A_r \rangle := \{A_{i_1} \ldots A_{i_k} \mid k \in \mathbb{N}_0, i_j \in \{1, \ldots, r\}\}$,

We are interested in the following problem.

Definition (Finiteness Problem)

Given $A_1, \ldots, A_r$, is $\langle A_1, \ldots, A_r \rangle$ finite?

$$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle =$$

Matrix Monoids + Problem of Interest

Definition

The matrix monoid generated by $A_1, \ldots, A_r \in \mathbb{Q}^{n \times n}$ is the set $\langle A_1, \ldots, A_r \rangle := \{A_{i_1} \ldots A_{i_k} \mid k \in \mathbb{N}_0, i_j \in \{1, \ldots, r\}\}$,

We are interested in the following problem.

Definition (Finiteness Problem)

Given $A_1, \ldots, A_r$, is $\langle A_1, \ldots, A_r \rangle$ finite?

$$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle = \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{N} \}$$

Infinite

Matrix Monoids + Problem of Interest

Definition

The matrix monoid generated by $A_1, \ldots, A_r \in \mathbb{Q}^{n \times n}$ is the set $\langle A_1, \ldots, A_r \rangle := \{A_{i_1} \ldots A_{i_k} \mid k \in \mathbb{N}_0, i_j \in \{1, \ldots, r\}\}$,

We are interested in the following problem.

Definition (Finiteness Problem)

Given $A_1, \ldots, A_r$, is $\langle A_1, \ldots, A_r \rangle$ finite?

$$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle = \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{N} \}$$

$$\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle =.$$

Infinite

Matrix Monoids + Problem of Interest

Definition

The matrix monoid generated by $A_1, \ldots, A_r \in \mathbb{Q}^{n \times n}$ is the set $\langle A_1, \ldots, A_r \rangle := \{A_{i_1} \ldots A_{i_k} \mid k \in \mathbb{N}_0, i_j \in \{1, \ldots, r\}\}$,

We are interested in the following problem.

Definition (Finiteness Problem)

Given $A_1, \ldots, A_r$, is $\langle A_1, \ldots, A_r \rangle$ finite?

$$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle = \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{N} \}$$

Infinite

$$\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle = \{ I, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \}.$$

Finite

Prior Work

Prior Work

Theorem (Minkowski, Friedman, Weisfeiler)

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

Prior Work

Theorem (Minkowski, Friedman, Weisfeiler)

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

Theorem (Schützenberger 1962)

If $M = \langle A_1, \ldots, A_r \rangle$ *is finite and semi-simple, then* $|M| \leq (2n+1)^{n^2}$.

Prior Work

Theorem (Minkowski, Friedman, Weisfeiler)

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

Theorem (Schützenberger 1962)

If $M = \langle A_1, \ldots, A_r \rangle$ *is finite and semi-simple, then* $|M| \leq (2n+1)^{n^2}$.

Corollary (Mandel and Simon 1977, Jacob 1978)

If $M = \langle A_1, \ldots, A_r \rangle$ *is finite, then* $|M| \leq Tower(n \cdot r)$.

Prior Work

Theorem (Minkowski, Friedman, Weisfeiler)

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

Theorem (Schützenberger 1962)

If $M = \langle A_1, \ldots, A_r \rangle$ *is finite and semi-simple, then* $|M| \leq (2n+1)^{n^2}$.

Corollary (Mandel and Simon 1977, Jacob 1978)

If $M = \langle A_1, \ldots, A_r \rangle$ *is finite, then* $|M| \leq Tower(n \cdot r)$.

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

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

This Talk

This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Corollary

Finiteness is in PSPACE.

This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Corollary

Finiteness is in PSPACE.

Proof.

Guess the product leading to a matrix A exceeding the bound (co-NPSPACE=PSPACE) □

This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Corollary

The membership problem in finite monoids is PSPACE-complete:

This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Corollary

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

This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Corollary

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

This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Corollary

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

Theorem

If $M = \langle A_1, \ldots, A_r \rangle$ can be conjugated to the integers, then a corresponding matrix P with $PMP^{-1} \subseteq \mathbb{Z}^{n \times n}$ can be found in PTIME.

Visual Representation

Visual Representation

We usually represent matrix monoids as follows.

Visual Representation

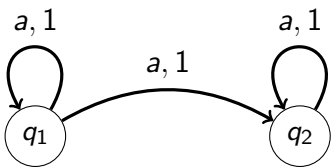
We usually represent matrix monoids as follows.

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

Visual Representation

We usually represent matrix monoids as follows.

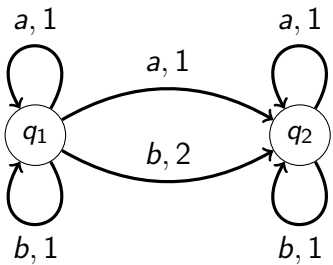
$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$



Visual Representation

We usually represent matrix monoids as follows.

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

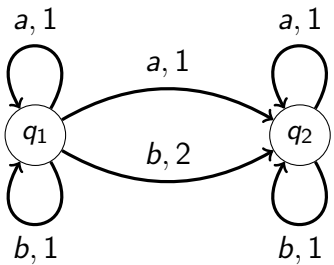


Visual Representation

We usually represent matrix monoids as follows.

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

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



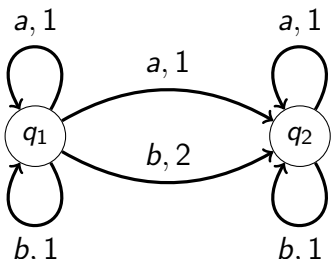
Visual Representation

We usually represent matrix monoids as follows.

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

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

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



Visual Representation

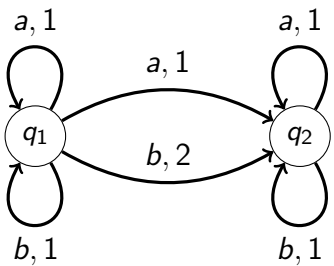
We usually represent matrix monoids as follows.

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

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

$A_i \leftrightarrow$ transition matrix on letter a_i

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



Visual Representation

We usually represent matrix monoids as follows.

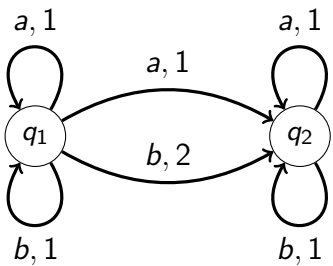
$n \times n \leftrightarrow n$ states of a finite automaton.

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

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



Visual Representation

We usually represent matrix monoids as follows.

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

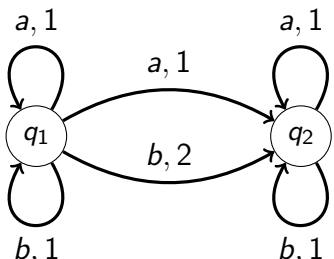
r (number of matrices) $\leftrightarrow |\Sigma| = r$

$A_i \leftrightarrow$ transition matrix on letter a_i

Multiplication $A_i \cdot A_j \leftrightarrow$ Composing letters

Does strong-connectedness have a meaning for the monoid?

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



Semi-Simple Monoids: Intuition

Semi-Simple Monoids: Intuition

Does strong-connectedness have a meaning for the monoid?

Semi-Simple Monoids: Intuition

Does strong-connectedness have a meaning for the monoid?

No. If $P \in GL_n(\mathbb{Q})$ is some base change,

Semi-Simple Monoids: Intuition

Does strong-connectedness have a meaning for the monoid?

No. If $P \in GL_n(\mathbb{Q})$ is some base change, then $M \simeq PMP^{-1}$, but M might be strongly-connected and PMP^{-1} is not.

Semi-Simple Monoids: Intuition

Does strong-connectedness have a meaning for the monoid?

No. If $P \in GL_n(\mathbb{Q})$ is some base change, then $M \simeq PMP^{-1}$, but M might be strongly-connected and PMP^{-1} is not.

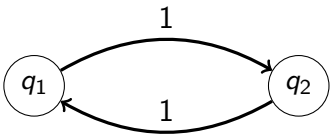
$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

Semi-Simple Monoids: Intuition

Does strong-connectedness have a meaning for the monoid?

No. If $P \in GL_n(\mathbb{Q})$ is some base change, then $M \simeq PMP^{-1}$, but M might be strongly-connected and PMP^{-1} is not.

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

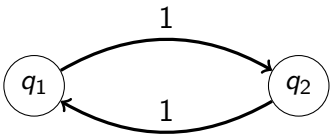


Semi-Simple Monoids: Intuition

Does strong-connectedness have a meaning for the monoid?

No. If $P \in GL_n(\mathbb{Q})$ is some base change, then $M \simeq PMP^{-1}$, but M might be strongly-connected and PMP^{-1} is not.

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

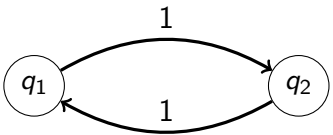


Semi-Simple Monoids: Intuition

Does strong-connectedness have a meaning for the monoid?

No. If $P \in GL_n(\mathbb{Q})$ is some base change, then $M \simeq PMP^{-1}$, but M might be strongly-connected and PMP^{-1} is not.

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



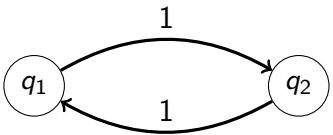
Semi-Simple Monoids: Intuition

Does strong-connectedness have a meaning for the monoid?

No. If $P \in GL_n(\mathbb{Q})$ is some base change, then $M \simeq PMP^{-1}$, but M might be strongly-connected and PMP^{-1} is not.

Idea: M is semi-simple if it is a disjoint union of SCCs.

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



Semi-Simple Monoids: The Actual Definition

Semi-Simple Monoids: The Actual Definition

Definition

$span(M) :=$vector space generated by M.

Semi-Simple Monoids: The Actual Definition

Definition

$span(M) :=$vector space generated by M.
Let $B = \{B_1, \ldots, B_m\} \subseteq M$ be a basis.

Semi-Simple Monoids: The Actual Definition

Definition

$span(M) :=$vector space generated by M.
Let $B = \{B_1, \ldots, B_m\} \subseteq M$ be a basis.
$Tr_B \colon span(M) \to \mathbb{Q}^m, A \mapsto (tr(A \cdot B_i))_{i=1}^m$.

Semi-Simple Monoids: The Actual Definition

Definition

$span(M) :=$vector space generated by M.
Let $B = \{B_1, \ldots, B_m\} \subseteq M$ be a basis.
$Tr_B \colon span(M) \to \mathbb{Q}^m, A \mapsto (tr(A \cdot B_i))_{i=1}^m$.
M is called semi-simple if Tr_B is injective.

Semi-Simple Monoids: The Actual Definition

Definition

$span(M) :=$vector space generated by M.
Let $B = \{B_1, \ldots, B_m\} \subseteq M$ be a basis.
$Tr_B : span(M) \to \mathbb{Q}^m, A \mapsto (tr(A \cdot B_i))_{i=1}^m$.
M is called semi-simple if Tr_B is injective.

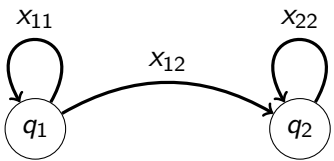
$$\begin{pmatrix} x_{11} & x_{12} \\ 0 & x_{22} \end{pmatrix}$$

Semi-Simple Monoids: The Actual Definition

Definition

$span(M) :=$ vector space generated by M.
Let $B = \{B_1, \ldots, B_m\} \subseteq M$ be a basis.
$Tr_B : span(M) \to \mathbb{Q}^m, A \mapsto (tr(A \cdot B_i))_{i=1}^m$.
M is called semi-simple if Tr_B is injective.

$$\begin{pmatrix} x_{11} & x_{12} \\ 0 & x_{22} \end{pmatrix}$$



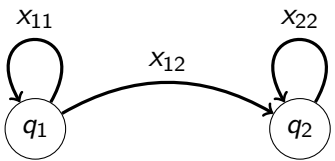
Semi-Simple Monoids: The Actual Definition

Definition

$span(M) :=$vector space generated by M.
Let $B = \{B_1, \ldots, B_m\} \subseteq M$ be a basis.
$Tr_B : span(M) \to \mathbb{Q}^m, A \mapsto (tr(A \cdot B_i))_{i=1}^m$.
M is called semi-simple if Tr_B is injective.

$$\begin{pmatrix} x_{11} & x_{12} \\ 0 & x_{22} \end{pmatrix}$$

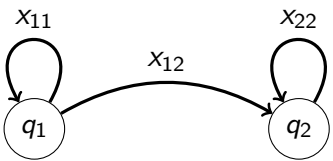
The Tr_B map is independent of x_{12}.



Semi-Simple Monoids: The Actual Definition

Definition

$span(M) :=$ vector space generated by M.
Let $B = \{B_1, \ldots, B_m\} \subseteq M$ be a basis.
$Tr_B : span(M) \to \mathbb{Q}^m, A \mapsto (tr(A \cdot B_i))_{i=1}^m$.
M is called semi-simple if Tr_B is injective.



$$\begin{pmatrix} x_{11} & x_{12} \\ 0 & x_{22} \end{pmatrix}$$

The Tr_B map is independent of x_{12}.

$$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle = \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{N} \}$$

Semi-Simple Monoids: The Actual Definition

Definition

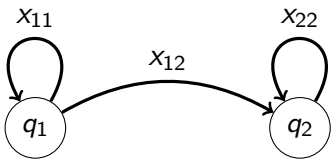
$span(M) :=$ vector space generated by M.
Let $B = \{B_1, \ldots, B_m\} \subseteq M$ be a basis.
$Tr_B : span(M) \to \mathbb{Q}^m, A \mapsto (tr(A \cdot B_i))_{i=1}^m$.
M is called semi-simple if Tr_B is injective.

$$\begin{pmatrix} x_{11} & x_{12} \\ 0 & x_{22} \end{pmatrix}$$

The Tr_B map is independent of x_{12}.

$$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle = \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{N} \}$$

is not semi-simple.



Semi-Simple Monoids: The Actual Definition

Definition

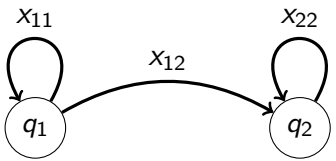
$span(M) :=$ vector space generated by M.
Let $B = \{B_1, \ldots, B_m\} \subseteq M$ be a basis.
$Tr_B : span(M) \to \mathbb{Q}^m, A \mapsto (tr(A \cdot B_i))_{i=1}^m$.
M is called semi-simple if Tr_B is injective.

$$\begin{pmatrix} x_{11} & x_{12} \\ 0 & x_{22} \end{pmatrix}$$

The Tr_B map is independent of x_{12}.

$$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle = \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{N} \}$$

is not semi-simple.



$$\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle = \{ I, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \}.$$

Semi-Simple Monoids: The Actual Definition

Definition

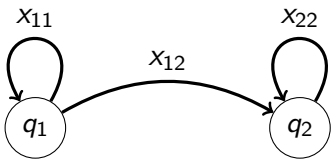
$span(M) :=$ vector space generated by M.
Let $B = \{B_1, \ldots, B_m\} \subseteq M$ be a basis.
$Tr_B : span(M) \to \mathbb{Q}^m, A \mapsto (tr(A \cdot B_i))_{i=1}^m$.
M is called semi-simple if Tr_B is injective.

$$\begin{pmatrix} x_{11} & x_{12} \\ 0 & x_{22} \end{pmatrix}$$

The Tr_B map is independent of x_{12}.

$$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle = \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{N} \}$$

is not semi-simple.



$$\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle = \{ I, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \}.$$

is semi-simple.

Wedderburn-Malcev Decomposition

Wedderburn-Malcev Decomposition

Definition

Let $M \subseteq \mathbb{Q}^{n \times n}$ be a monoid.

Wedderburn-Malcev Decomposition

Definition

Let $M \subseteq \mathbb{Q}^{n \times n}$ be a monoid. A base change $P \in GL_n(\mathbb{Q})$ s.t. PMP^{-1} is block-upper-triangular

Wedderburn-Malcev Decomposition

Definition

Let $M \subseteq \mathbb{Q}^{n \times n}$ be a monoid. A base change $P \in GL_n(\mathbb{Q})$ s.t. PMP^{-1} is block-upper-triangular

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

Wedderburn-Malcev Decomposition

Definition

Let $M \subseteq \mathbb{Q}^{n \times n}$ be a monoid. A base change $P \in GL_n(\mathbb{Q})$ s.t. PMP^{-1} is block-upper-triangular with semi-simple block-diagonal is called Wedderburn-Malcev Decomposition (WM-D).

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

Wedderburn-Malcev Decomposition

Definition

Let $M \subseteq \mathbb{Q}^{n\times n}$ be a monoid. A base change $P \in GL_n(\mathbb{Q})$ s.t. PMP^{-1} is block-upper-triangular with semi-simple block-diagonal is called Wedderburn-Malcev Decomposition (WM-D).

Intuition: WM-D$\simeq$Jordan basis for monoids instead of single matrices.

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

Wedderburn-Malcev Decomposition

Definition

Let $M \subseteq \mathbb{Q}^{n \times n}$ be a monoid. A base change $P \in GL_n(\mathbb{Q})$ s.t. PMP^{-1} is block-upper-triangular with semi-simple block-diagonal is called Wedderburn-Malcev Decomposition (WM-D).

Intuition: WM-D$\simeq$Jordan basis for monoids instead of single matrices.

Theorem (Wedderburn 1908)

A WM-D always exists and can be computed in PTIME.

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

Wedderburn-Malcev Decomposition

Definition

Let $M \subseteq \mathbb{Q}^{n \times n}$ be a monoid. A base change $P \in GL_n(\mathbb{Q})$ s.t. PMP^{-1} is block-upper-triangular with semi-simple block-diagonal is called Wedderburn-Malcev Decomposition (WM-D).

Intuition: WM-D$\simeq$Jordan basis for monoids instead of single matrices.

Theorem (Wedderburn 1908)

A WM-D always exists and can be computed in PTIME.

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

$$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle = \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{N} \}$$

Wedderburn-Malcev Decomposition

Definition

Let $M \subseteq \mathbb{Q}^{n \times n}$ be a monoid. A base change $P \in GL_n(\mathbb{Q})$ s.t. PMP^{-1} is block-upper-triangular with semi-simple block-diagonal is called Wedderburn-Malcev Decomposition (WM-D).

Intuition: WM-D$\simeq$Jordan basis for monoids instead of single matrices.

Theorem (Wedderburn 1908)

A WM-D always exists and can be computed in PTIME.

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

$$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle = \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{N} \}$$

is already in WM-D.

Reminder: Goal of This Talk

Reminder: Goal of This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq$ exp.)

Theorem (Schützenberger 1962)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite and semi-simple, then $|M| \leq (2n+1)^{n^2}$.

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

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

Reminder: Goal of This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq$ exp.)

Theorem (Schützenberger 1962)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite and semi-simple, then $|M| \leq (2n+1)^{n^2}$.

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

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

Proof Strategy: W.l.o.g. M is in WM-D Form.

Reminder: Goal of This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Theorem (Schützenberger 1962)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite and semi-simple, then $|M| \leq (2n+1)^{n^2}$.

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

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

Proof Strategy: W.l.o.g. M is in WM-D Form.
Let $A \in M$. To bound entries on the block-diagonal use Schützenberger's result.

Reminder: Goal of This Talk

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Theorem (Schützenberger 1962)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite and semi-simple, then $|M| \leq (2n+1)^{n^2}$.

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

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

Proof Strategy: W.l.o.g. M is in WM-D Form.
Let $A \in M$. To bound entries on the block-diagonal use Schützenberger's result.
To bound entries above the diagonal, use BHKST'20.

Proof Sketch

Proof Sketch

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Proof Sketch

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Lemma (Schützenberger 1962)

If M is finite, then $Tr_B(M) \subseteq \{-n, \ldots, n\}^{\dim(span(M))}$.

Proof Sketch

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Lemma (Schützenberger 1962)

If M is finite, then $Tr_B(M) \subseteq \{-n, \ldots, n\}^{\dim(span(M))}$.

Lemma

Let $A \in \mathbb{Q}^{n \times n}$ be a matrix of finite order. Then $tr(A) \in \{-n, \ldots, n\}$.

Proof Sketch

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Lemma (Schützenberger 1962)

If M is finite, then $Tr_B(M) \subseteq \{-n, \ldots, n\}^{\dim(span(M))}$.

Lemma

Let $A \in \mathbb{Q}^{n \times n}$ be a matrix of finite order. Then $tr(A) \in \{-n, \ldots, n\}$.

Proof Sketch

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Proof Sketch

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Proof.

Write $A = A_1 \ldots A_{2^n}$. Write $A_i = D_i + U_i$.

□

Proof Sketch

Theorem (This Talk)

If $M = \langle A_1, \ldots, A_r \rangle$ is finite, then every $A \in M$ has polynomial bitsize in terms of $A_1, \ldots, A_r$. (I.e. $|M| \leq exp.$)

Proof.

Write $A = A_1 \ldots A_{2^n}$. Write $A_i = D_i + U_i$.
$A = \sum_{\{i_1,\ldots,i_n\} \subseteq \{1,\ldots,2^n\}} (D_1 \ldots D_{i_1-1}) U_{i_1} \ldots U_{i_n} (D_{i_n+1} \ldots D_{2^n})$ □