Computational Complexity of Matrix Semigroup Properties

Trevor Jack

Joint work with Peter Mayr

Mathematics
UNIVERSITY OF COLORADO BOULDER

Update for BLAST 2018 Presentation

Transformation Semigroups

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME?}$$

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}?$$

Theorem (Fleischer, TJ, 2019)

The complexity of determining the following properties of transformation semigroups are in NL:

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}?$$

Theorem (Fleischer, TJ, 2019)

The complexity of determining the following properties of transformation semigroups are in NL: is a band;

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}?$$

Theorem (Fleischer, TJ, 2019)

The complexity of determining the following properties of transformation semigroups are in NL: is a band; all idempotents commute;

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}?$$

Theorem (Fleischer, TJ, 2019)

The complexity of determining the following properties of transformation semigroups are in NL: is a band; all idempotents commute; is Clifford;

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}?$$

Theorem (Fleischer, TJ, 2019)

The complexity of determining the following properties of transformation semigroups are in NL: is a band; all idempotents commute; is Clifford; and, generally, any property that can be defined by a fixed equation.

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}?$$

Theorem (Fleischer, TJ, 2019)

The complexity of determining the following properties of transformation semigroups are in NL: is a band; all idempotents commute; is Clifford; and, generally, any property that can be defined by a fixed equation.
The following problems are NL-complete:

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}?$$

Theorem (Fleischer, TJ, 2019)

The complexity of determining the following properties of transformation semigroups are in NL: is a band; all idempotents commute; is Clifford; and, generally, any property that can be defined by a fixed equation. The following problems are NL-complete: existence of left/right zeroes;

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}?$$

Theorem (Fleischer, TJ, 2019)

The complexity of determining the following properties of transformation semigroups are in NL: is a band; all idempotents commute; is Clifford; and, generally, any property that can be defined by a fixed equation. The following problems are NL-complete: existence of left/right zeroes; nilpotence;

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME?}$$

Theorem (Fleischer, TJ, 2019)

The complexity of determining the following properties of transformation semigroups are in NL: is a band; all idempotents commute; is Clifford; and, generally, any property that can be defined by a fixed equation. The following problems are NL-complete: existence of left/right zeroes; nilpotence; $\mathbb{R}$-triviality;

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME?}$$

Theorem (Fleischer, TJ, 2019)

The complexity of determining the following properties of transformation semigroups are in NL: is a band; all idempotents commute; is Clifford; and, generally, any property that can be defined by a fixed equation. The following problems are NL-complete: existence of left/right zeroes; nilpotence; $\mathbb{R}$-triviality; and all idempotents are central.

Update for BLAST 2018 Presentation

Transformation Semigroups

- $[n] := \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S = \langle a_1, \ldots, a_k \rangle \leq T_n$

General Inquiry: Given generators $a_1, \ldots, a_k \in T_n$, what is the complexity of verifying certain properties about $S = \langle a_1, \ldots, a_n \rangle$ within:

$$\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}?$$

Theorem (Mayr, TJ, 2019)

The left and right identities of a transformation semigroup can be enumerated in polynomial time.

Notation

Matrix Semigroups

- $\mathbb{F}^n$ is the set of row vectors of length n over a field $\mathbb{F}$

Notation

Matrix Semigroups

- $\mathbb{F}^n$ is the set of row vectors of length n over a field $\mathbb{F}$
- $S = \langle a_1, \ldots, a_k \rangle \leq \mathbb{F}^{n \times n}$ under multiplication

Notation

Matrix Semigroups

- $\mathbb{F}^n$ is the set of row vectors of length n over a field $\mathbb{F}$
- $S = \langle a_1, \ldots, a_k \rangle \leq \mathbb{F}^{n \times n}$ under multiplication

Note that $\mathbb{F}^{n \times n}$ acts as a transformation semigroup on the set $\mathbb{F}^n$ by multiplication on the right.

Notation

Matrix Semigroups

- $\mathbb{F}^n$ is the set of row vectors of length n over a field $\mathbb{F}$
- $S = \langle a_1, \ldots, a_k \rangle \leq \mathbb{F}^{n \times n}$ under multiplication

Note that $\mathbb{F}^{n \times n}$ acts as a transformation semigroup on the set $\mathbb{F}^n$ by multiplication on the right.
Space to store a_i as a matrix $= n^2 \log(|\mathbb{F}|)$.
Space to store representation of a_i as a transformation $= |\mathbb{F}|^n \log(n|\mathbb{F}|)$.

Notation

- $\mathrm{Row}(a_i)$ is the rowspace of a_i.

Notation

- $\mathrm{Row}(a_i)$ is the rowspace of a_i.
- $\mathrm{Row}(S)$ is the sum of the rowspaces of the generators of S.

Notation

- $\mathrm{Row}(a_i)$ is the rowspace of a_i.
- $\mathrm{Row}(S)$ is the sum of the rowspaces of the generators of S.
- $\mathrm{Null}(S) := \bigcap_{i\in[k]} \mathrm{Null}(a_i)$

Notation

- $\mathrm{Row}(a_i)$ is the rowspace of a_i.
- $\mathrm{Row}(S)$ is the sum of the rowspaces of the generators of S.
- $\mathrm{Null}(S) := \bigcap_{i\in[k]} \mathrm{Null}(a_i)$
- $[\![x]\!] := x + \mathrm{Null}(S)$

Notation

- $\mathrm{Row}(a_i)$ is the rowspace of a_i.
- $\mathrm{Row}(S)$ is the sum of the rowspaces of the generators of S.
- $\mathrm{Null}(S) := \bigcap_{i \in [k]} \mathrm{Null}(a_i)$
- $[\![x]\!] := x + \mathrm{Null}(S)$
- $S \to \mathrm{End}(\mathbb{F}^n/\mathrm{Null}(S)), s \mapsto \bar{s}$ where $[\![x]\!]\bar{s} = [\![xs]\!]$ for $x \in [n]$

Notation

- $\mathrm{Row}(a_i)$ is the rowspace of a_i.
- $\mathrm{Row}(S)$ is the sum of the rowspaces of the generators of S.
- $\mathrm{Null}(S) := \bigcap_{i\in[k]} \mathrm{Null}(a_i)$
- $[\![x]\!] := x + \mathrm{Null}(S)$
- $S \to \mathrm{End}(\mathbb{F}^n/\mathrm{Null}(S)), s \mapsto \overline{s}$ where $[\![x]\!]\overline{s} = [\![xs]\!]$ for $x \in [n]$
- $\overline{S} := \{\overline{s} : s \in S\}$

Notation

- $\mathrm{Row}(a_i)$ is the rowspace of a_i.
- $\mathrm{Row}(S)$ is the sum of the rowspaces of the generators of S.
- $\mathrm{Null}(S) := \bigcap_{i\in[k]} \mathrm{Null}(a_i)$
- $[\![x]\!] := x + \mathrm{Null}(S)$
- $S \to \mathrm{End}(\mathbb{F}^n/\mathrm{Null}(S)), s \mapsto \bar{s}$ where $[\![x]\!]\bar{s} = [\![xs]\!]$ for $x \in [n]$
- $\overline{S} := \{\bar{s} : s \in S\}$

Note that $\bar{s}$ is well-defined. For any $y \in [\![x]\!]$, there is a $z \in \mathrm{Null}(S)$ such that $y = x + z$ and thus $[\![y]\!]\bar{s} = [\![ys]\!] = [\![(x+z)s]\!] = [\![xs]\!] = [\![x]\!]\bar{s}$.

Notation

- $\mathrm{Row}(a_i)$ is the rowspace of a_i.
- $\mathrm{Row}(S)$ is the sum of the rowspaces of the generators of S.
- $\mathrm{Null}(S) := \bigcap_{i\in[k]} \mathrm{Null}(a_i)$
- $[\![x]\!] := x + \mathrm{Null}(S)$
- $S \to \mathrm{End}(\mathbb{F}^n/\mathrm{Null}(S)), s \mapsto \overline{s}$ where $[\![x]\!]\overline{s} = [\![xs]\!]$ for $x \in [n]$
- $\overline{S} := \{\overline{s} : s \in S\}$

Note that $\overline{s}$ is well-defined. For any $y \in [\![x]\!]$, there is a $z \in \mathrm{Null}(S)$ such that $y = x + z$ and thus $[\![y]\!]\overline{s} = [\![ys]\!] = [\![(x+z)s]\!] = [\![xs]\!] = [\![x]\!]\overline{s}$.

LeftIdentities

Input: $a_1, \ldots, a_k \in \mathbb{F}^{n\times n}$

Problem: Enumerate the left identities of $\langle a_1, \ldots, a_k\rangle$.

Proof of Left Identities Lemma

Left Identities Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in F^{n\times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $\ell \in S$ is a left identity of S iff there is an $i \in [k]$ such that $\overline{a_i}$ permutes $\mathbb{F}^n/\mathrm{Null}(S)$ and ℓ equals the idempotent power of a_i.

Proof.

Proof of Left Identities Lemma

Left Identities Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in F^{n \times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $\ell \in S$ is a left identity of S iff there is an $i \in [k]$ such that $\overline{a_i}$ permutes $\mathbb{F}^n/\mathrm{Null}(S)$ and ℓ equals the idempotent power of a_i.

Proof.

$\Leftarrow$:

- Let $\overline{a_i}$ permute $\mathbb{F}^n/\mathrm{Null}(S)$ and let $(a_i^m)^2 = a_i^m$.

Proof of Left Identities Lemma

Left Identities Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in F^{n\times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $\ell \in S$ is a left identity of S iff there is an $i \in [k]$ such that $\overline{a_i}$ permutes $\mathbb{F}^n/\mathrm{Null}(S)$ and ℓ equals the idempotent power of a_i.

Proof.

$\Leftarrow$:

- Let $\overline{a_i}$ permute $\mathbb{F}^n/\mathrm{Null}(S)$ and let $(a_i^m)^2 = a_i^m$.
- Then $\overline{a_i}^m = \overline{1}$, so $\forall x \in \mathbb{F}^n : [\![x a_i^m]\!] = [\![x]\!] \overline{a_i}^m = [\![x]\!]$.

Proof of Left Identities Lemma

Left Identities Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in F^{n\times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $\ell \in S$ is a left identity of S iff there is an $i \in [k]$ such that $\overline{a_i}$ permutes $\mathbb{F}^n/\mathrm{Null}(S)$ and ℓ equals the idempotent power of a_i.

Proof.

$\Leftarrow$:

- Let $\overline{a_i}$ permute $\mathbb{F}^n/\mathrm{Null}(S)$ and let $(a_i^m)^2 = a_i^m$.
- Then $\overline{a_i}^m = \overline{1}$, so $\forall x \in \mathbb{F}^n : [\![xa_i^m]\!] = [\![x]\!]\overline{a_i}^m = [\![x]\!]$.
- Thus, $xa_i^m = x + z$ for some $z \in \mathrm{Null}(S)$ so that $xa_i^m s = (x+z)s = xs$ for every $s \in S$.

□

Proof of Left Identities Lemma

Left Identities Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in F^{n \times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $\ell \in S$ is a left identity of S iff there is an $i \in [k]$ such that $\overline{a_i}$ permutes $\mathbb{F}^n/\mathrm{Null}(S)$ and ℓ equals the idempotent power of a_i.

Proof.

Proof of Left Identities Lemma

Left Identities Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in F^{n \times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $\ell \in S$ is a left identity of S iff there is an $i \in [k]$ such that $\overline{a_i}$ permutes $\mathbb{F}^n / \mathrm{Null}(S)$ and ℓ equals the idempotent power of a_i.

Proof.

$\Rightarrow$:

- Let $\ell \in S$ satisfy $x\ell s = xs$ for every $x \in \mathbb{F}^n$ and every $s \in S$.

Proof of Left Identities Lemma

Left Identities Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in F^{n \times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $\ell \in S$ is a left identity of S iff there is an $i \in [k]$ such that $\overline{a_i}$ permutes $\mathbb{F}^n/\mathrm{Null}(S)$ and ℓ equals the idempotent power of a_i.

Proof.

$\Rightarrow$:

- Let $\ell \in S$ satisfy $x\ell s = xs$ for every $x \in \mathbb{F}^n$ and every $s \in S$.
- Then $(x\ell - x)s = 0$, $x\ell - x \in \mathrm{Null}(S)$, $[\![x\ell]\!] = [\![x]\!]$, and $\overline{\ell} = \overline{1}$.

Proof of Left Identities Lemma

Left Identities Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in F^{n \times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $\ell \in S$ is a left identity of S iff there is an $i \in [k]$ such that $\overline{a_i}$ permutes $\mathbb{F}^n/\mathrm{Null}(S)$ and ℓ equals the idempotent power of a_i.

Proof.

$\Rightarrow$:

- Let $\ell \in S$ satisfy $x\ell s = xs$ for every $x \in \mathbb{F}^n$ and every $s \in S$.
- Then $(x\ell - x)s = 0$, $x\ell - x \in \mathrm{Null}(S)$, $[\![x\ell]\!] = [\![x]\!]$, and $\overline{\ell} = \overline{1}$.
- So, $\ell = ba_i$ for some permutations $\overline{b}, \overline{a_i} \in \overline{S}$.

Proof of Left Identities Lemma

Left Identities Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in F^{n\times n}$, and $S := \langle a_1, \ldots, a_k\rangle$. Then an element $\ell \in S$ is a left identity of S iff there is an $i \in [k]$ such that $\overline{a_i}$ permutes $\mathbb{F}^n/\mathrm{Null}(S)$ and ℓ equals the idempotent power of a_i.

Proof.

$\Rightarrow$:

- Let $\ell \in S$ satisfy $x\ell s = xs$ for every $x \in \mathbb{F}^n$ and every $s \in S$.
- Then $(x\ell - x)s = 0$, $x\ell - x \in \mathrm{Null}(S)$, $[\![x\ell]\!] = [\![x]\!]$, and $\overline{\ell} = \overline{1}$.
- So, $\ell = ba_i$ for some permutations $\overline{b}, \overline{a_i} \in \overline{S}$.
- Since $\overline{a_i}^m = \overline{1}$, $\forall x \in \mathbb{F}^n : [\![xb]\!]\overline{a_i} = [\![x]\!]\overline{ba_i} = [\![x]\!]\overline{a_i}^m = [\![xa_i^{m-1}]\!]\overline{a_i}$.

Proof of Left Identities Lemma

Left Identities Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in F^{n\times n}$, and $S := \langle a_1, \ldots, a_k\rangle$. Then an element $\ell \in S$ is a left identity of S iff there is an $i \in [k]$ such that $\overline{a_i}$ permutes $\mathbb{F}^n/\mathrm{Null}(S)$ and ℓ equals the idempotent power of a_i.

Proof.

$\Rightarrow$:

- Let $\ell \in S$ satisfy $x\ell s = xs$ for every $x \in \mathbb{F}^n$ and every $s \in S$.
- Then $(x\ell - x)s = 0$, $x\ell - x \in \mathrm{Null}(S)$, $[\![x\ell]\!] = [\![x]\!]$, and $\overline{\ell} = \overline{1}$.
- So, $\ell = ba_i$ for some permutations $\overline{b}, \overline{a_i} \in \overline{S}$.
- Since $\overline{a_i}^m = \overline{1}$, $\forall x \in \mathbb{F}^n : [\![xb]\!]\overline{a_i} = [\![x]\!]\overline{ba_i} = [\![x]\!]\overline{a_i}^m = [\![xa_i^{m-1}]\!]\overline{a_i}$.
- Since $\overline{a_i}$ is a permutation, $[\![xb]\!] = [\![xa_i^{m-1}]\!]$ so that, for any $s \in S$, $xbs = xa_i^{m-1}s$. In particular, $xba_i = xa_i^m$.

$\square$

Left Identities Theorem

Left Identities Theorem

LeftIdentities can be solved in polynomial time.

Left Identities Theorem

Left Identities Theorem

LeftIdentities can be solved in polynomial time.

Proof.

- Let $S = \langle a_1, \ldots, a_k \rangle \leq \mathbb{F}^{n \times n}$. Recall $\mathrm{Null}(S) := \bigcap \mathrm{Null}(a_i)$.

Left Identities Theorem

Left Identities Theorem

LeftIdentities can be solved in polynomial time.

Proof.

- Let $S = \langle a_1, \ldots, a_k \rangle \leq \mathbb{F}^{n\times n}$. Recall $\mathrm{Null}(S) := \bigcap \mathrm{Null}(a_i)$.
- Generate $\mathbb{F}^n/\mathrm{Null}(S)$ and enumerate each $\overline{a_i}$ that permutes $\mathbb{F}^n$.

Left Identities Theorem

Left Identities Theorem

LeftIdentities can be solved in polynomial time.

Proof.

- Let $S = \langle a_1, \ldots, a_k \rangle \leq \mathbb{F}^{n\times n}$. Recall $\mathrm{Null}(S) := \bigcap \mathrm{Null}(a_i)$.
- Generate $\mathbb{F}^n/\mathrm{Null}(S)$ and enumerate each $\overline{a_i}$ that permutes $\mathbb{F}^n$.
- By Lemma, the idempotent powers $a_i^{m_i}$'s are left identities.

Left Identities Theorem

Left Identities Theorem

LeftIdentities can be solved in polynomial time.

Proof.

- Let $S = \langle a_1, \ldots, a_k \rangle \leq \mathbb{F}^{n \times n}$. Recall $\mathrm{Null}(S) := \bigcap \mathrm{Null}(a_i)$.
- Generate $\mathbb{F}^n/\mathrm{Null}(S)$ and enumerate each $\overline{a_i}$ that permutes $\mathbb{F}^n$.
- By Lemma, the idempotent powers $a_i^{m_i}$'s are left identities.
- Note that $\mathrm{Null}(a_i) = \mathrm{Null}(S)$, so $\mathrm{Row}(a_i) \cap \mathrm{Null}(a_i) = \emptyset$.

Left Identities Theorem

Left Identities Theorem

LeftIdentities can be solved in polynomial time.

Proof.

- Let $S = \langle a_1, \ldots, a_k \rangle \leq \mathbb{F}^{n \times n}$. Recall $\mathrm{Null}(S) := \bigcap \mathrm{Null}(a_i)$.
- Generate $\mathbb{F}^n/\mathrm{Null}(S)$ and enumerate each $\overline{a_i}$ that permutes $\mathbb{F}^n$.
- By Lemma, the idempotent powers $a_i^{m_i}$'s are left identities.
- Note that $\mathrm{Null}(a_i) = \mathrm{Null}(S)$, so $\mathrm{Row}(a_i) \cap \mathrm{Null}(a_i) = \emptyset$.
- A basis B of $\mathrm{Row}(a_i)$ and a basis C of $\mathrm{Null}(a_i)$ forms a basis for $\mathbb{F}^n$.

Left Identities Theorem

Left Identities Theorem

LeftIdentities can be solved in polynomial time.

Proof.

- Let $S = \langle a_1, \ldots, a_k \rangle \leq \mathbb{F}^{n \times n}$. Recall $\mathrm{Null}(S) := \bigcap \mathrm{Null}(a_i)$.
- Generate $\mathbb{F}^n / \mathrm{Null}(S)$ and enumerate each $\overline{a_i}$ that permutes $\mathbb{F}^n$.
- By Lemma, the idempotent powers $a_i^{m_i}$'s are left identities.
- Note that $\mathrm{Null}(a_i) = \mathrm{Null}(S)$, so $\mathrm{Row}(a_i) \cap \mathrm{Null}(a_i) = \emptyset$.
- A basis B of $\mathrm{Row}(a_i)$ and a basis C of $\mathrm{Null}(a_i)$ forms a basis for $\mathbb{F}^n$.
- Let P be the matrix with rows from B followed by rows from C.

Left Identities Theorem

Left Identities Theorem

LeftIdentities can be solved in polynomial time.

Proof.

- Let $S = \langle a_1, \ldots, a_k \rangle \leq \mathbb{F}^{n \times n}$. Recall $\mathrm{Null}(S) := \bigcap \mathrm{Null}(a_i)$.
- Generate $\mathbb{F}^n / \mathrm{Null}(S)$ and enumerate each $\overline{a_i}$ that permutes $\mathbb{F}^n$.
- By Lemma, the idempotent powers $a_i^{m_i}$'s are left identities.
- Note that $\mathrm{Null}(a_i) = \mathrm{Null}(S)$, so $\mathrm{Row}(a_i) \cap \mathrm{Null}(a_i) = \emptyset$.
- A basis B of $\mathrm{Row}(a_i)$ and a basis C of $\mathrm{Null}(a_i)$ forms a basis for $\mathbb{F}^n$.
- Let P be the matrix with rows from B followed by rows from C.
- $a_i = P^{-1}DP$ for some block diagonal D with zeroes outside of the top corner block of dimension $|B| \times |B|$.

Left Identities Theorem

Left Identities Theorem

LeftIdentities can be solved in polynomial time.

Proof.

- Let $S = \langle a_1, \ldots, a_k \rangle \leq \mathbb{F}^{n \times n}$. Recall $\mathrm{Null}(S) := \bigcap \mathrm{Null}(a_i)$.
- Generate $\mathbb{F}^n/\mathrm{Null}(S)$ and enumerate each $\overline{a_i}$ that permutes $\mathbb{F}^n$.
- By Lemma, the idempotent powers $a_i^{m_i}$'s are left identities.
- Note that $\mathrm{Null}(a_i) = \mathrm{Null}(S)$, so $\mathrm{Row}(a_i) \cap \mathrm{Null}(a_i) = \emptyset$.
- A basis B of $\mathrm{Row}(a_i)$ and a basis C of $\mathrm{Null}(a_i)$ forms a basis for $\mathbb{F}^n$.
- Let P be the matrix with rows from B followed by rows from C.
- $a_i = P^{-1}DP$ for some block diagonal D with zeroes outside of the top corner block of dimension $|B| \times |B|$.
- $a_i^{m_i} = P^{-1}D^{m_i}P$ where D^{m_i} is diagonal with 1's in the first $|B|$ diagonal entries and zeroes elsewhere.

Right Identities Problem

RightIdentities

Input: $a_1, \ldots, a_k \in T_n$
Problem: Enumerate the right identities of $\langle a_1, \ldots, a_k \rangle$.

Proof of Right Identities Lemma

Right Identity Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in \mathbb{F}^{n \times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $r \in S$ is a right identity of S iff there is an $i \in [k]$ such that $\mathrm{Null}(a_i) \cap \mathrm{Row}(S) = \{0\}$ and r equals the idempotent power of a_i.

Proof of Right Identities Lemma

Right Identity Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in \mathbb{F}^{n \times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $r \in S$ is a right identity of S iff there is an $i \in [k]$ such that $\mathrm{Null}(a_i) \cap \mathrm{Row}(S) = \{0\}$ and r equals the idempotent power of a_i.

Proof.

$\Leftarrow$: Let $\mathrm{Null}(a_i) \cap \mathrm{Row}(S) = \{0\}$ and $(a_i^m)^2 = a_i^m$.

Proof of Right Identities Lemma

Right Identity Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in \mathbb{F}^{n \times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $r \in S$ is a right identity of S iff there is an $i \in [k]$ such that $\mathrm{Null}(a_i) \cap \mathrm{Row}(S) = \{0\}$ and r equals the idempotent power of a_i.

Proof.

$\Leftarrow$: Let $\mathrm{Null}(a_i) \cap \mathrm{Row}(S) = \{0\}$ and $(a_i^m)^2 = a_i^m$.
So, a_i embeds $\mathrm{Row}(S)$ into $\mathbb{F}^n$ and $a_i|_{\mathrm{Row}(S)}$ is bijective.

Proof of Right Identities Lemma

Right Identity Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in \mathbb{F}^{n\times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $r \in S$ is a right identity of S iff there is an $i \in [k]$ such that $\mathrm{Null}(a_i) \cap \mathrm{Row}(S) = \{0\}$ and r equals the idempotent power of a_i.

Proof.

$\Leftarrow$: Let $\mathrm{Null}(a_i) \cap \mathrm{Row}(S) = \{0\}$ and $(a_i^m)^2 = a_i^m$.
So, a_i embeds $\mathrm{Row}(S)$ into $\mathbb{F}^n$ and $a_i|_{\mathrm{Row}(S)}$ is bijective.
Then a_i^m fixes $\mathrm{Row}(S)$. That is, $\forall x \in \mathbb{F}^n, \forall s \in S : xsa_i^m = xs$.

Proof of Right Identities Lemma

Right Identity Lemma

Let $k, n \in \mathbb{N}$, $a_1, \ldots, a_k \in \mathbb{F}^{n\times n}$, and $S := \langle a_1, \ldots, a_k \rangle$. Then an element $r \in S$ is a right identity of S iff there is an $i \in [k]$ such that $\mathrm{Null}(a_i) \cap \mathrm{Row}(S) = \{0\}$ and r equals the idempotent power of a_i.

Proof.

$\Leftarrow$: Let $\mathrm{Null}(a_i) \cap \mathrm{Row}(S) = \{0\}$ and $(a_i^m)^2 = a_i^m$.
So, a_i embeds $\mathrm{Row}(S)$ into $\mathbb{F}^n$ and $a_i|_{\mathrm{Row}(S)}$ is bijective.
Then a_i^m fixes $\mathrm{Row}(S)$. That is, $\forall x \in \mathbb{F}^n, \forall s \in S : xsa_i^m = xs$.

$\Rightarrow$: Let r satisfy $xsr = xs$ for every $x \in \mathbb{F}^n$ and every $s \in S$. Then r fixes $\mathrm{Row}(S)$ and $r = a_i b$ for some $a_i, b \in S$ that permute $\mathrm{Row}(S)$.

Proof of Right Identities Lemma

Right Identity Lemma

Let $k, n \in \mathbb{N}$, $a_1, \dots, a_k \in \mathbb{F}^{n \times n}$, and $S := \langle a_1, \dots, a_k \rangle$. Then an element $r \in S$ is a right identity of S iff there is an $i \in [k]$ such that $\mathrm{Null}(a_i) \cap \mathrm{Row}(S) = \{0\}$ and r equals the idempotent power of a_i.

Proof.

$\Leftarrow$: Let $\mathrm{Null}(a_i) \cap \mathrm{Row}(S) = \{0\}$ and $(a_i^m)^2 = a_i^m$.
So, a_i embeds $\mathrm{Row}(S)$ into $\mathbb{F}^n$ and $a_i|_{\mathrm{Row}(S)}$ is bijective.
Then a_i^m fixes $\mathrm{Row}(S)$. That is, $\forall x \in \mathbb{F}^n, \forall s \in S : xsa_i^m = xs$.

$\Rightarrow$: Let r satisfy $xsr = xs$ for every $x \in \mathbb{F}^n$ and every $s \in S$. Then r fixes $\mathrm{Row}(S)$ and $r = a_i b$ for some $a_i, b \in S$ that permute $\mathrm{Row}(S)$.
Since a_i^m fixes $\mathrm{Row}(S)$, $\forall x \in \mathbb{F}^n : xa_i b = xa_i a_i^m b = xa_i^m a_i b = xa_i^m$. □

Right Identity Theorem

Right Identity Theorem

RightIdentities can be solved in polynomial time.

Right Identity Theorem

Right Identity Theorem

RightIdentities can be solved in polynomial time.

Proof.

- Generate $\mathrm{Row}(S)$ and enumerate the a_i's that permute $\mathrm{Row}(S)$.

Right Identity Theorem

Right Identity Theorem

RightIdentities can be solved in polynomial time.

Proof.

- Generate $\mathrm{Row}(S)$ and enumerate the a_i's that permute $\mathrm{Row}(S)$.
- By Lemma, the idempotent powers $a_i^{m_i}$ are the right identities.

Right Identity Theorem

Right Identity Theorem

RightIdentities can be solved in polynomial time.

Proof.

- Generate $\mathrm{Row}(S)$ and enumerate the a_i's that permute $\mathrm{Row}(S)$.
- By Lemma, the idempotent powers $a_i^{m_i}$ are the right identities.
- As with left identities, $\mathrm{Null}(a_i) = \mathrm{Null}(S)$, so we can build these idempotents simply from knowing a basis B of $\mathrm{Row}(a_i)$ and a basis C of $\mathrm{Null}(a_i)$.

$\square$

Matrix Nilpotence

Notation

A matrix semigroup $S \leq \mathbb{F}^{n \times n}$ is said to be **nilpotent** if it has a zero element, $0 \in S$, satisfying $0S = \{0\}$ and there exists $d \in \mathbb{N}$ such that $S^d = \{0\}$. If $S^d = \{0\}$, we say S is $d-$nilpotent.

Matrix Nilpotence

Notation

A matrix semigroup $S \leq \mathbb{F}^{n \times n}$ is said to be **nilpotent** if it has a zero element, $0 \in S$, satisfying $0S = \{0\}$ and there exists $d \in \mathbb{N}$ such that $S^d = \{0\}$. If $S^d = \{0\}$, we say S is $d-$nilpotent.

Nilpotence

Input: $a_1, ..., a_k \in T_n$
Output: Whether $\langle a_1, ..., a_k \rangle$ is nilpotent.

Matrix Nilpotence

Notation

A matrix semigroup $S \leq \mathbb{F}^{n \times n}$ is said to be **nilpotent** if it has a zero element, $0 \in S$, satisfying $0S = \{0\}$ and there exists $d \in \mathbb{N}$ such that $S^d = \{0\}$. If $S^d = \{0\}$, we say S is $d-$nilpotent.

Nilpotence

Input: $a_1, ..., a_k \in T_n$
Output: Whether $\langle a_1, ..., a_k \rangle$ is nilpotent.

Lemma

A matrix semigroup $S \leq \mathbb{F}^{n \times n}$ is nilpotent iff it is $n-$nilpotent.

Proof of Lemma (1)

Lemma

A matrix semigroup $S \leq \mathbb{F}^{n \times n}$ is nilpotent iff it is $n-$nilpotent.

Proof of Lemma (1)

Lemma

A matrix semigroup $S \leq \mathbb{F}^{n \times n}$ is nilpotent iff it is $n-$nilpotent.

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i S)$.

Proof of Lemma (1)

Lemma

A matrix semigroup $S \leq \mathbb{F}^{n\times n}$ is nilpotent iff it is $n-$nilpotent.

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i S)$.
- By linearity, $V_i = \mathrm{span}(V_0 S^i)$.

Proof of Lemma (1)

Lemma

A matrix semigroup $S \leq \mathbb{F}^{n \times n}$ is nilpotent iff it is $n-$nilpotent.

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i S)$.
- By linearity, $V_i = \mathrm{span}(V_0 S^i)$.
- Then, if S has nilpotency degree d, $V_d = \mathrm{span}(V_0 S^d) = \mathrm{span}(V_0 0) = \mathbb{F}^n 0$.

Proof of Lemma (1)

Lemma

A matrix semigroup $S \leq \mathbb{F}^{n\times n}$ is nilpotent iff it is $n-$nilpotent.

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i S)$.
- By linearity, $V_i = \mathrm{span}(V_0 S^i)$.
- Then, if S has nilpotency degree d, $V_d = \mathrm{span}(V_0 S^d) = \mathrm{span}(V_0 0) = \mathbb{F}^n 0$.
- Let m be minimal s.t. $V_m = V_{m+1}$. We prove $V_m = V_j$ for $j \geq m$.

Proof of Lemma (1)

Lemma

A matrix semigroup $S \leq \mathbb{F}^{n \times n}$ is nilpotent iff it is $n-$nilpotent.

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i S)$.
- By linearity, $V_i = \mathrm{span}(V_0 S^i)$.
- Then, if S has nilpotency degree d,
  $V_d = \mathrm{span}(V_0 S^d) = \mathrm{span}(V_0 0) = \mathbb{F}^n 0$.
- Let m be minimal s.t. $V_m = V_{m+1}$. We prove $V_m = V_j$ for $j \geq m$.
- If $V_m = V_j$. Then $V_m = V_{m+1} = \mathrm{span}(V_m S) = \mathrm{span}(V_j S) = V_{j+1}$.

Proof of Lemma (1)

Lemma

A matrix semigroup $S \leq \mathbb{F}^{n \times n}$ is nilpotent iff it is $n-$nilpotent.

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i S)$.
- By linearity, $V_i = \mathrm{span}(V_0 S^i)$.
- Then, if S has nilpotency degree d, $V_d = \mathrm{span}(V_0 S^d) = \mathrm{span}(V_0 0) = \mathbb{F}^n 0$.
- Let m be minimal s.t. $V_m = V_{m+1}$. We prove $V_m = V_j$ for $j \geq m$.
- If $V_m = V_j$. Then $V_m = V_{m+1} = \mathrm{span}(V_m S) = \mathrm{span}(V_j S) = V_{j+1}$.
- Certainly $m \leq d$, so $\mathrm{span}(V_0 S^m) = V_m = V_d = \mathbb{F}^n 0$, so $m = d$.

Proof of Lemma (1)

Lemma

A matrix semigroup $S \leq \mathbb{F}^{n\times n}$ is nilpotent iff it is $n-$nilpotent.

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i S)$.
- By linearity, $V_i = \mathrm{span}(V_0 S^i)$.
- Then, if S has nilpotency degree d,
  $V_d = \mathrm{span}(V_0 S^d) = \mathrm{span}(V_0 0) = \mathbb{F}^n 0$.
- Let m be minimal s.t. $V_m = V_{m+1}$. We prove $V_m = V_j$ for $j \geq m$.
- If $V_m = V_j$. Then $V_m = V_{m+1} = \mathrm{span}(V_m S) = \mathrm{span}(V_j S) = V_{j+1}$.
- Certainly $m \leq d$, so $\mathrm{span}(V_0 S^m) = V_m = V_d = \mathbb{F}^n 0$, so $m = d$.
- Note, $\mathbb{F}^n S^{i+1} \subseteq \mathbb{F}^n S^i$ implies $V^{i+1} \leq V^i$ and $V_{i+1} \neq V_i$ for $i < d$.

Proof of Lemma (1)

Lemma

A matrix semigroup $S \leq \mathbb{F}^{n\times n}$ is nilpotent iff it is $n-$nilpotent.

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i S)$.
- By linearity, $V_i = \mathrm{span}(V_0 S^i)$.
- Then, if S has nilpotency degree d, $V_d = \mathrm{span}(V_0 S^d) = \mathrm{span}(V_0 0) = \mathbb{F}^n 0$.
- Let m be minimal s.t. $V_m = V_{m+1}$. We prove $V_m = V_j$ for $j \geq m$.
- If $V_m = V_j$. Then $V_m = V_{m+1} = \mathrm{span}(V_m S) = \mathrm{span}(V_j S) = V_{j+1}$.
- Certainly $m \leq d$, so $\mathrm{span}(V_0 S^m) = V_m = V_d = \mathbb{F}^n 0$, so $m = d$.
- Note, $\mathbb{F}^n S^{i+1} \subseteq \mathbb{F}^n S^i$ implies $V^{i+1} \leq V^i$ and $V_{i+1} \neq V_i$ for $i < d$.
- Then $n = \dim(V_0) > \dim(V_0 S) > \cdots > \dim(V_0 S^d) = 0$ and $n \geq d$.

Nilpotence Theorem

Matrix Nilpotence Theorem

Nilpotence is in P.

Proof

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i a_j | j \in [k])$.

Nilpotence Theorem

Matrix Nilpotence Theorem

Nilpotence is in P.

Proof

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i a_j | j \in [k])$.
- Let $0 = a_1^n$. We claim S is nilpotent iff:
  (1) $V_n = \mathbb{F}^n 0$ and (2) $0a_j = a_j 0 = 0$ for every $j \in [k]$.

Nilpotence Theorem

Matrix Nilpotence Theorem

Nilpotence is in P.

Proof

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i a_j | j \in [k])$.
- Let $0 = a_1^n$. We claim S is nilpotent iff:
  (1) $V_n = \mathbb{F}^n 0$ and (2) $0a_j = a_j 0 = 0$ for every $j \in [k]$.
- One direction is clear. For the other, assume (1) and (2) hold.

Nilpotence Theorem

Matrix Nilpotence Theorem

Nilpotence is in P.

Proof

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i a_j | j \in [k])$.
- Let $0 = a_1^n$. We claim S is nilpotent iff:
  (1) $V_n = \mathbb{F}^n 0$ and (2) $0a_j = a_j 0 = 0$ for every $j \in [k]$.
- One direction is clear. For the other, assume (1) and (2) hold.
- Pick any $x \in \mathbb{F}^n$ and any $s_1, \ldots, s_n \in \{a_1, \ldots, a_k\}$.

Nilpotence Theorem

Matrix Nilpotence Theorem

Nilpotence is in P.

Proof

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i a_j | j \in [k])$.
- Let $0 = a_1^n$. We claim S is nilpotent iff:
  (1) $V_n = \mathbb{F}^n 0$ and (2) $0a_j = a_j 0 = 0$ for every $j \in [k]$.
- One direction is clear. For the other, assume (1) and (2) hold.
- Pick any $x \in \mathbb{F}^n$ and any $s_1, \ldots, s_n \in \{a_1, \ldots, a_k\}$.
- By (1), $xs_1 \cdots s_n \in \mathbb{F}^n 0$.

Nilpotence Theorem

Matrix Nilpotence Theorem

Nilpotence is in P.

Proof

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i a_j | j \in [k])$.
- Let $0 = a_1^n$. We claim S is nilpotent iff:
  (1) $V_n = \mathbb{F}^n 0$ and (2) $0a_j = a_j 0 = 0$ for every $j \in [k]$.
- One direction is clear. For the other, assume (1) and (2) hold.
- Pick any $x \in \mathbb{F}^n$ and any $s_1, \ldots, s_n \in \{a_1, \ldots, a_k\}$.
- By (1), $xs_1 \cdots s_n \in \mathbb{F}^n 0$.
- By (2), $xs_1 \cdots s_n = xs_1 \cdots s_n 0 = x0$.

Nilpotence Theorem

Matrix Nilpotence Theorem

Nilpotence is in P.

Proof

- Let $V_0 = \mathbb{F}^n$ and $V_{i+1} = \mathrm{span}(V_i a_j | j \in [k])$.
- Let $0 = a_1^n$. We claim S is nilpotent iff: (1) $V_n = \mathbb{F}^n 0$ and (2) $0a_j = a_j 0 = 0$ for every $j \in [k]$.
- One direction is clear. For the other, assume (1) and (2) hold.
- Pick any $x \in \mathbb{F}^n$ and any $s_1, \ldots, s_n \in \{a_1, \ldots, a_k\}$.
- By (1), $xs_1 \cdots s_n \in \mathbb{F}^n 0$.
- By (2), $xs_1 \cdots s_n = xs_1 \cdots s_n 0 = x0$.
- By Lemma, we need only produce V_n and check (1) and (2). These can be done in polynomial time by methods like Gaussian elimination.