Computational Complexity of Semigroup Properties

Trevor Jack

Joint work with Lukas Fleischer and Peter Mayr

Mathematics
UNIVERSITY OF COLORADO **BOULDER**

Introduction

Recently published paper

Lukas Fleischer, TJ, The Complexity of Properties of Transformation Semigroups, IJAC, 2019

Introduction

Recently published paper

Lukas Fleischer, TJ, The Complexity of Properties of Transformation Semigroups, IJAC, 2019

Transformation Semigroups

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

Introduction

Recently published paper

Lukas Fleischer, TJ, The Complexity of Properties of Transformation Semigroups, IJAC, 2019

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:

$$AC^0 \subseteq NL \subseteq P \subseteq NP \subseteq PSPACE \subseteq EXPTIME?$$

AC^0 Problems

AC^0 Problems

Definition

AC^0 is the class of sets decidable by unbounded fan-in Boolean circuits of constant depth.

AC^0 Problems

Definition

AC^0 is the class of sets decidable by unbounded fan-in Boolean circuits of constant depth.

Theorem (Fleischer, TJ, 2019)

Testing for the following properties is in AC^0.

- S is commutative.

AC^0 Problems

Definition

AC^0 is the class of sets decidable by unbounded fan-in Boolean circuits of constant depth.

Theorem (Fleischer, TJ, 2019)

Testing for the following properties is in AC^0.

- S is commutative.
- S is a semilattice.

AC^0 Problems

Definition

AC^0 is the class of sets decidable by unbounded fan-in Boolean circuits of constant depth.

Theorem (Fleischer, TJ, 2019)

Testing for the following properties is in AC^0.

- S is commutative.
- S is a semilattice.
- S is a group.

AC^0 Problems

Definition

AC^0 is the class of sets decidable by unbounded fan-in Boolean circuits of constant depth.

Theorem (Fleischer, TJ, 2019)

Testing for the following properties is in AC^0.

- S is commutative.
- S is a semilattice.
- S is a group.

Consequences of $FO = AC^0$. Each of these properties can be characterized by first order formulas with quantification over generators and points.

AC^0 Problems

Definition

AC^0 is the class of sets decidable by unbounded fan-in Boolean circuits of constant depth.

Theorem (Fleischer, TJ, 2019)

Testing for the following properties is in AC^0.

- S is commutative.
- S is a semilattice.
- S is a group.

Consequences of $FO = AC^0$. Each of these properties can be characterized by first order formulas with quantification over generators and points. For example, a commutative semigroup is characterized by $\forall x \in [n], \forall a_i, a_j (x a_i a_j = x a_j a_i)$.

NL-Complete Problems

NL-Complete Problems

Definition

A semigroup S is $\mathcal{R}$-**trivial** if Green's $\mathcal{R}$ relation is equality.

NL-Complete Problems

Definition

A semigroup S is $\mathcal{R}$-**trivial** if Green's $\mathcal{R}$ relation is equality.

Theorem (Fleischer, TJ, 2019)

Testing for the following properties is in NL-complete.

- S contains a left zero.

NL-Complete Problems

Definition

A semigroup S is $\mathcal{R}$-**trivial** if Green's $\mathcal{R}$ relation is equality.

Theorem (Fleischer, TJ, 2019)

Testing for the following properties is in NL-complete.

- S contains a left zero.
- S contains a right zero.

NL-Complete Problems

Definition

A semigroup S is $\mathcal{R}$-**trivial** if Green's $\mathcal{R}$ relation is equality.

Theorem (Fleischer, TJ, 2019)

Testing for the following properties is in NL-complete.

- S contains a left zero.
- S contains a right zero.
- S contains a zero.

NL-Complete Problems

Definition

A semigroup S is $\mathcal{R}$-**trivial** if Green's $\mathcal{R}$ relation is equality.

Theorem (Fleischer, TJ, 2019)

Testing for the following properties is in NL-complete.

- S contains a left zero.
- S contains a right zero.
- S contains a zero.
- S is nilpotent.

NL-Complete Problems

Definition

A semigroup S is $\mathcal{R}$-**trivial** if Green's $\mathcal{R}$ relation is equality.

Theorem (Fleischer, TJ, 2019)

Testing for the following properties is in NL-complete.

- S contains a left zero.
- S contains a right zero.
- S contains a zero.
- S is nilpotent.
- S is $\mathcal{R}$-trivial.

NL Problems

NL Problems

Model-Checking

Let u and v be semigroup words over variables $x_1, \ldots, x_m$.

NL Problems

Model-Checking

Let u and v be semigroup words over variables $x_1, \ldots, x_m$.

Model$(u = v)$

- Input: $a_1, \ldots, a_k \in T_n$
- Problem: Does $\langle a_1, \ldots, a_k \rangle$ satisfy $u = v$?

NL Problems

Model-Checking

Let u and v be semigroup words over variables $x_1, \ldots, x_m$.

Model$(u = v)$

- Input: $a_1, \ldots, a_k \in T_n$
- Problem: Does $\langle a_1, \ldots, a_k \rangle$ satisfy $u = v$?

Theorem (Fleischer, TJ, 2019)

For fixed u and v, Model$(u = v)$ is in NL.

NL Problems

Model-Checking

Let u and v be semigroup words over variables $x_1, \dots, x_m$.

Model$(u = v)$

- Input: $a_1, \dots, a_k \in T_n$
- Problem: Does $\langle a_1, \dots, a_k \rangle$ satisfy $u = v$?

Theorem (Fleischer, TJ, 2019)

For fixed u and v, Model$(u = v)$ is in NL.

Note: This problem is dual to the well-known identity checking problem in which the semigroup is fixed and the identity is given.

NL Problems

Model-Checking

Let u and v be semigroup words over variables $x_1, \ldots, x_m$.

Model$(u = v)$

- Input: $a_1, \ldots, a_k \in T_n$
- Problem: Does $\langle a_1, \ldots, a_k \rangle$ satisfy $u = v$?

Theorem (Fleischer, TJ, 2019)

For fixed u and v, Model$(u = v)$ is in NL.

Note: This problem is dual to the well-known identity checking problem in which the semigroup is fixed and the identity is given. There are semigroups for which the identity checking problem is coNP-complete.

Sketch of algorithm by example

- Let $u = xyx$ and $v = yx$.

Sketch of algorithm by example

- Let $u = xyx$ and $v = yx$.
- Nondeterministically guess points p, px, pxy, $pxyx$, py, $pyx \in [n]$ such that $pxyx \neq pyx$.

Sketch of algorithm by example

- Let $u = xyx$ and $v = yx$.
- Nondeterministically guess points p, px, pxy, $pxyx$, py, $pyx \in [n]$ such that $pxyx \neq pyx$.
- Nondeterministically guess generators for elements x and y until they correspond to the guessed points.

NL Problems

Model-Checking

Let u and v be semigroup words over variables $x_1, \ldots, x_m$.

Model$(u = v)$

- Input: $a_1, \ldots, a_k \in T_n$
- Problem: Does $\langle a_1, \ldots, a_k \rangle$ model $u = v$?

Theorem (Fleischer, TJ, 2019)

For fixed u and v, Model$(u = v)$ is in NL.

Hardness

NL Problems

Model-Checking

Let u and v be semigroup words over variables $x_1, \ldots, x_m$.

Model$(u = v)$

- Input: $a_1, \ldots, a_k \in T_n$
- Problem: Does $\langle a_1, \ldots, a_k \rangle$ model $u = v$?

Theorem (Fleischer, TJ, 2019)

For fixed u and v, Model$(u = v)$ is in NL.

Hardness

- Model$(x = x)$ is always true.

NL Problems

Model-Checking

Let u and v be semigroup words over variables $x_1, \ldots, x_m$.

Model$(u = v)$

- Input: $a_1, \ldots, a_k \in T_n$
- Problem: Does $\langle a_1, \ldots, a_k \rangle$ model $u = v$?

Theorem (Fleischer, TJ, 2019)

For fixed u and v, Model$(u = v)$ is in NL.

Hardness

- Model$(x = x)$ is always true.
- Model$(xy = yx)$ is in AC^0.

NL Problems

Model-Checking

Let u and v be semigroup words over variables $x_1, \ldots, x_m$.

Model$(u = v)$

- Input: $a_1, \ldots, a_k \in T_n$
- Problem: Does $\langle a_1, \ldots, a_k \rangle$ model $u = v$?

Theorem (Fleischer, TJ, 2019)

For fixed u and v, Model$(u = v)$ is in NL.

Hardness

- Model$(x = x)$ is always true.
- Model$(xy = yx)$ is in AC^0.
- Theorem (Fleischer, TJ, 2019): Model$(x^2 y = x^2)$ is NL-complete.

NL and P Problems

Theorem (Fleischer, TJ, 2019)

Model$(x_1 = x_1^2, \ldots, x_s = x_s^2 \Rightarrow u = v)$ is in NL.
Thus, the following problems are also in NL.

NL and P Problems

Theorem (Fleischer, TJ, 2019)

Model($x_1 = x_1^2, \ldots, x_s = x_s^2 \Rightarrow u = v$) is in NL.
Thus, the following problems are also in NL.

- S is a band;

NL and P Problems

Theorem (Fleischer, TJ, 2019)

$\mathrm{Model}(x_1 = x_1^2, \ldots, x_s = x_s^2 \Rightarrow u = v)$ is in NL.
Thus, the following problems are also in NL.

- S is a band;
- all idempotents of S commute;

NL and P Problems

Theorem (Fleischer, TJ, 2019)

Model($x_1 = x_1^2, \ldots, x_s = x_s^2 \Rightarrow u = v$) is in NL.
Thus, the following problems are also in NL.

- S is a band;
- all idempotents of S commute;
- the product of any two idempotents in S is idempotent.

NL and P Problems

Theorem (Fleischer, TJ, 2019)

Model$(x_1 = x_1^2, \ldots, x_s = x_s^2 \Rightarrow u = v)$ is in NL.
Thus, the following problems are also in NL.

- S is a band;
- all idempotents of S commute;
- the product of any two idempotents in S is idempotent.

Determining if every idempotent of a semigroup is central is NL-complete.

NL and P Problems

Theorem (Fleischer, TJ, 2019)

Model($x_1 = x_1^2, \ldots, x_s = x_s^2 \Rightarrow u = v$) is in NL.
Thus, the following problems are also in NL.

- S is a band;
- all idempotents of S commute;
- the product of any two idempotents in S is idempotent.

Determining if every idempotent of a semigroup is central is NL-complete.

Theorem (Fleischer, TJ, 2019)

Determining if a semigroup is completely regular is in NL.

NL and P Problems

Theorem (Fleischer, TJ, 2019)

Model($x_1 = x_1^2, \ldots, x_s = x_s^2 \Rightarrow u = v$) is in NL.
Thus, the following problems are also in NL.

- S is a band;
- all idempotents of S commute;
- the product of any two idempotents in S is idempotent.

Determining if every idempotent of a semigroup is central is NL-complete.

Theorem (Fleischer, TJ, 2019)

Determining if a semigroup is completely regular is in NL.

Theorem (Fleischer, TJ, 2019

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

PSPACE-Complete Problem

Regular Element

- Input: $a_1, \ldots, a_k \in T_n$
- Problem: Is there $s \in \langle a_1, \ldots, a_k \rangle$ such that $a_k s a_k = a_k$?

PSPACE-Complete Problem

Regular Element

- Input: $a_1, \ldots, a_k \in T_n$
- Problem: Is there $s \in \langle a_1, \ldots, a_k \rangle$ such that $a_k s a_k = a_k$?

Theorem (Fleischer, TJ, 2019)

Regular Element is PSPACE-complete:

PSPACE-Complete Problem

Regular Element

- Input: $a_1, \ldots, a_k \in T_n$
- Problem: Is there $s \in \langle a_1, \ldots, a_k \rangle$ such that $a_k s a_k = a_k$?

Theorem (Fleischer, TJ, 2019)

Regular Element is PSPACE-complete:

Proof reduces from the following problem shown to be PSPACE-complete by Kozen in 1977.

PSPACE-Complete Problem

Regular Element

- Input: $a_1, \ldots, a_k \in T_n$
- Problem: Is there $s \in \langle a_1, \ldots, a_k \rangle$ such that $a_k s a_k = a_k$?

Theorem (Fleischer, TJ, 2019)

Regular Element is PSPACE-complete:

Proof reduces from the following problem shown to be PSPACE-complete by Kozen in 1977.

Finite Automata Intersection

- Input: Automata $A_1, \ldots, A_m$ over a shared alphabet $a_1, \ldots, a_k$.
- Problem: Is there a $w \in \{a_1, \ldots, a_k\}^*$ accepted by each automaton?

Proof Sketch

- Extend the states of the automata to include a new state 0.

Proof Sketch

- Extend the states of the automata to include a new state 0.
- Define $a_1, \ldots, a_k$ to act on the automata states naturally and to fix 0.

Proof Sketch

- Extend the states of the automata to include a new state 0.
- Define $a_1, \ldots, a_k$ to act on the automata states naturally and to fix 0.
- Define a new transition b that: (1) sends accepting states for each automata to corresponding start states and (2) sends every other state to 0.

Proof Sketch

- Extend the states of the automata to include a new state 0.
- Define $a_1, \ldots, a_k$ to act on the automata states naturally and to fix 0.
- Define a new transition b that: (1) sends accepting states for each automata to corresponding start states and (2) sends every other state to 0.
- An accepting word exists iff there exists $c \in \langle a_1, \ldots, a_k, b \rangle$ such that $bcb = b$.

Matrix Semigroups

Notation

Matrix Semigroups

Notation

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

Matrix Semigroups

Notation

- $\mathbb{F}^n$ 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

Matrix Semigroups

Notation

- $\mathbb{F}^n$ 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

Theorem (TJ 2020)

The following can be solved in polynomial time:

Matrix Semigroups

Notation

- $\mathbb{F}^n$ 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

Theorem (TJ 2020)

The following can be solved in polynomial time:

- enumerate left identities;

Matrix Semigroups

Notation

- $\mathbb{F}^n$ 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

Theorem (TJ 2020)

The following can be solved in polynomial time:

- enumerate left identities;
- enumerate right identities; and

Matrix Semigroups

Notation

- $\mathbb{F}^n$ 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

Theorem (TJ 2020)

The following can be solved in polynomial time:

- enumerate left identities;
- enumerate right identities; and
- determine nilpotence.

Partial Bijection Semigroups

Partial Bijection Semigroups

Notation

- P_n is the semigroup of all unary partial functions on [n]

Partial Bijection Semigroups

Notation

- P_n is the semigroup of all unary partial functions on [n]
- $\mathrm{dom}(ab) := \{x \in [n] : xa \in \mathrm{dom}(b)\}$

Partial Bijection Semigroups

Notation

- P_n is the semigroup of all unary partial functions on [n]
- $\mathrm{dom}(ab) := \{x \in [n] : xa \in \mathrm{dom}(b)\}$
- $S = \langle a_1, \ldots, a_k \rangle \leq P_n$

Partial Bijection Semigroups

Notation

- P_n is the semigroup of all unary partial functions on [n]
- $\mathrm{dom}(ab) := \{x \in [n] : xa \in \mathrm{dom}(b)\}$
- $S = \langle a_1, \ldots, a_k \rangle \leq P_n$

Theorem (TJ 2020)

Checking if S is a band is in AC^0.

Partial Bijection Semigroups

Notation

- P_n is the semigroup of all unary partial functions on [n]
- $\mathrm{dom}(ab) := \{x \in [n] : xa \in \mathrm{dom}(b)\}$
- $S = \langle a_1, \ldots, a_k \rangle \leq P_n$

Theorem (TJ 2020)

Checking if S is a band is in AC^0.

Membership

- Input: $a_1, \ldots, a_k, b \in P_n$
- Output: $b \in \langle a_1, \ldots, a_k \rangle$?

Partial Bijection Semigroups

Notation

- P_n is the semigroup of all unary partial functions on [n]
- $\mathrm{dom}(ab) := \{x \in [n] : xa \in \mathrm{dom}(b)\}$
- $S = \langle a_1, \ldots, a_k \rangle \leq P_n$

Theorem (TJ 2020)

Checking if S is a band is in AC^0.

Membership

- Input: $a_1, \ldots, a_k, b \in P_n$
- Output: $b \in \langle a_1, \ldots, a_k \rangle$?

Theorem (TJ 2020)

Membership is PSPACE-complete

Partial Bijection Semigroups

Notation

- P_n is the semigroup of all unary partial functions on [n]
- $\mathrm{dom}(ab) := \{x \in [n] : xa \in \mathrm{dom}(b)\}$
- $S = \langle a_1, \ldots, a_k \rangle \leq P_n$

Theorem (TJ 2020)

Checking if S is a band is in AC^0.

Membership

- Input: $a_1, \ldots, a_k, b \in P_n$
- Output: $b \in \langle a_1, \ldots, a_k \rangle$?

Theorem (TJ 2020)

Membership is PSPACE-complete

Really Rough Sketch of Proof

Really Rough Sketch of Proof

PSPACE-hardness: Reduce from membership problem for $S \leq T_n$.

Really Rough Sketch of Proof

PSPACE-hardness: Reduce from membership problem for $S \leq T_n$.

Given $a_1, \ldots, a_\ell \in T_n$, define points Q to be acted upon.

$Q := \{(0,0,0)\} \bigcup \{(s,t,0) : s \in [n-1], t \in [\ell]\} \bigcup \{(q,r,1) : q, r \in [n]\}$

Really Rough Sketch of Proof

PSPACE-hardness: Reduce from membership problem for $S \leq T_n$.

Given $a_1, \ldots, a_\ell \in T_n$, define points Q to be acted upon.

$Q := \{(0,0,0)\} \bigcup \{(s,t,0) : s \in [n-1], t \in [\ell]\} \bigcup \{(q,r,1) : q, r \in [n]\}$

Define $\overline{S} := \langle a_{1,1,1}, \ldots, a_{n,n,\ell} \rangle \leq P_Q$ as follows:

Really Rough Sketch of Proof

PSPACE-hardness: Reduce from membership problem for $S \leq T_n$.

Given $a_1, \ldots, a_\ell \in T_n$, define points Q to be acted upon.

$Q := \{(0,0,0)\} \bigcup \{(s,t,0) : s \in [n-1], t \in [\ell]\} \bigcup \{(q,r,1) : q, r \in [n]\}$

Define $\overline{S} := \langle a_{1,1,1}, \ldots, a_{n,n,\ell} \rangle \leq P_Q$ as follows:

$$(s,t,0)a_{i,j,k} := \begin{cases} (1,k,0) & \text{if } s = t = 0 \text{ and } j = 1 \\ (s+1,k,0) & \text{if } t = k \text{ and } j - 1 = s < n-1 \\ (0,0,0) & \text{if } t = k \text{ and } j - 1 = s = n-1 \end{cases}$$

$$(q,r,1)a_{i,j,k} := \begin{cases} (qa_k, r, 1) & \text{if } q = i \text{ and } r = j \\ (q,r,1) & \text{if } r \neq j \end{cases}$$

Really Rough Sketch of Proof

Claim: $s \in S$ iff $\exists \bar{s} \in \overline{S}$ such that: $(0,0,0)\bar{s} = (0,0,0)$, $(x,x,1)\bar{s} = (xs,x,1)$ for each $x \in [n]$, and all other points are excluded from the domain of $\bar{s}$.

Really Rough Sketch of Proof

Claim: $s \in S$ iff $\exists \overline{s} \in \overline{S}$ such that: $(0,0,0)\overline{s} = (0,0,0)$, $(x,x,1)\overline{s} = (xs,x,1)$ for each $x \in [n]$, and all other points are excluded from the domain of $\overline{s}$.

Assume $s \in S$, with $s = a_{k_1} \cdots a_{k_p}$. Let $s_\ell = a_{k_1} \cdots a_{k_\ell}$.

Really Rough Sketch of Proof

Claim: $s \in S$ iff $\exists \overline{s} \in \overline{S}$ such that: $(0,0,0)\overline{s} = (0,0,0)$, $(x,x,1)\overline{s} = (xs, x, 1)$ for each $x \in [n]$, and all other points are excluded from the domain of $\overline{s}$.

Assume $s \in S$, with $s = a_{k_1} \cdots a_{k_p}$. Let $s_\ell = a_{k_1} \cdots a_{k_\ell}$.

$\overline{s} = a_{1,1,k_1} \cdots a_{n,n,k_1} a_{1s_1,1,k_2} \cdots a_{ns_1,n,k_2} \cdots a_{1s_{p-1},1,k_p} \cdots a_{ns_{p-1},n,k_p}$

Really Rough Sketch of Proof

Claim: $s \in S$ iff $\exists \overline{s} \in \overline{S}$ such that: $(0,0,0)\overline{s} = (0,0,0)$, $(x,x,1)\overline{s} = (xs,x,1)$ for each $x \in [n]$, and all other points are excluded from the domain of $\overline{s}$.

Assume $s \in S$, with $s = a_{k_1} \cdots a_{k_p}$. Let $s_\ell = a_{k_1} \cdots a_{k_\ell}$.

$\overline{s} = a_{1,1,k_1} \cdots a_{n,n,k_1} a_{1s_1,1,k_2} \cdots a_{ns_1,n,k_2} \cdots a_{1s_{p-1},1,k_p} \cdots a_{ns_{p-1},n,k_p}$

$(0,0,0)\overline{s} = (0,0,0)$ and $(x,x,1)\overline{s} = (xs,x,1)$ for each $x \in [n]$.

Really Rough Sketch of Proof

Claim: $s \in S$ iff $\exists \overline{s} \in \overline{S}$ such that: $(0,0,0)\overline{s} = (0,0,0)$, $(x,x,1)\overline{s} = (xs,x,1)$ for each $x \in [n]$, and all other points are excluded from the domain of $\overline{s}$.

Assume $s \in S$, with $s = a_{k_1} \cdots a_{k_p}$. Let $s_\ell = a_{k_1} \cdots a_{k_\ell}$.

$\overline{s} = a_{1,1,k_1} \cdots a_{n,n,k_1} a_{1s_1,1,k_2} \cdots a_{ns_1,n,k_2} \cdots a_{1s_{p-1},1,k_p} \cdots a_{ns_{p-1},n,k_p}$

$(0,0,0)\overline{s} = (0,0,0)$ and $(x,x,1)\overline{s} = (xs,x,1)$ for each $x \in [n]$.

For the converse, the a_{ijk} are defined such that $\overline{s}$ must have the specific structure above, allowing us to find $s = a_{k_1} \cdots a_{k_p}$.