Computational Complexity of Semigroup Properties

Trevor Jack

Joint work with Peter Mayr
Notation and Regularity Problem

Transformation Semigroups

- \([n] := \{1, \ldots, n\}\)
- \(T_n\) is the semigroup of all unary functions on \([n]\)
- \(S \leq T_n\)
Notation and Regularity Problem

Transformation Semigroups

- \([n] := \{1, \ldots, n\}\)
- \(T_n\) is the semigroup of all unary functions on \([n]\)
- \(S \leq T_n\)

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:

\[
P \subseteq NP \subseteq PSPACE \subseteq EXPTIME?
\]
Regularity

Preliminaries

Notation and Regularity Problem

Transformation Semigroups

- \([n] := \{1, \ldots, n\}\)
- \(T_n\) is the semigroup of all unary functions on \([n]\)
- \(S \leq T_n\)

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:

\[
P \subseteq NP \subseteq \text{PSPACE} \subseteq \text{EXPTIME}\
\]

Definition

\(b \in T_n\) is regular in \(S\) if for some \(s \in S\), \(bsb = b\).
Notation and Regularity Problem

Transformation Semigroups

- \([n] := \{1, \ldots, n\}\)
- \(T_n\) is the semigroup of all unary functions on \([n]\)
- \(S \leq T_n\)

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:

\[ P \subseteq NP \subseteq PSPACE \subseteq EXPTIME? \]

Definition

\(b \in T_n\) is regular in \(S\) if for some \(s \in S\), \(bsb = b\).

RegularElement

Input: \(a_1, \ldots, a_k, b \in T_n\)
Output: Is \(b\) regular in \(\langle a_1, \ldots, a_k \rangle\)?
Theorem

RegularElement is PSPACE-Complete.
RegularElement Theorem and Proof

Theorem

RegularElement is PSPACE-Complete.

Definition

A deterministic finite automata (DFA) has:
1. a set of states $Z$ with a start state and an accept state; and
2. a set of transformations $\Sigma$, which map states to states.
RegularElement Theorem and Proof

Theorem
RegularElement is PSPACE-Complete.

Definition
A deterministic finite automata (DFA) has:
1. a set of states $Z$ with a start state and an accept state; and
2. a set of transformations $\Sigma$, which map states to states.

The proof uses the following PSPACE-complete problem (Kozen, 1970):

Finite Automata Intersection (FAI)
Input: DFA’s $A_1, \ldots, A_\ell$ with shared transitions $\Sigma$
Output: Whether there is $w \in \Sigma^*$ accepted by each $A_i$. 
Proof Sketch

Proof.

Given DFAs $A_1, ..., A_\ell$ with sets of states $Z_1, ..., Z_\ell$ and shared transitions $\Sigma$, define the following transformation semigroup:

- Transformed Set: $Z = \bigcup_{i=1}^{\ell} Z_i$ along with new state 0.
- Generators: $\Sigma$ defined naturally on $Z$ and fixing 0.
- Add generator $h$ that sends accept states to start states and sends every other state to 0.

Then $h$ is regular in this semigroup iff there is a $w \in \Sigma^*$ accepted by each $A_1, ..., A_\ell$. Hence, RegularElement is PSPACE-hard.

RegularElement is in NPSPACE because we can nondeterministically guess the generators that produce an $s$ satisfying $bsb = b$. So, by Savitch’s Theorem, RegularElement is in PSPACE, and thus PSPACE-complete.
Open Problem

How hard is it to check that every element in $S$ is regular?
Regular Semigroup

Open Problem
How hard is it to check that every element in \( S \) is regular?

A semigroup is **completely regular** if each element generates a subgroup.

Theorem
Determining if \( \langle a_1, \ldots, a_k \rangle \leq T_n \) is completely regular is in P.

Proof requires use of "transformation graphs"
Fix $u, v$ semigroup words over variables $z_1, \ldots, z_m$
Model Checking

Fix $u, v$ semigroup words over variables $z_1, \ldots, z_m$

**Model($u \approx v$)**

**Input:** $a_1, \ldots, a_k \in T_n$

**Output:** Whether $\langle a_1, \ldots, a_k \rangle$ models $u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$. 
Model Checking

Fix $u, v$ semigroup words over variables $z_1, \ldots, z_m$

Model($u \approx v$)

Input: $a_1, \ldots, a_k \in T_n$
Output: Whether $\langle a_1, \ldots, a_k \rangle$ models $u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$.

Example: Band Identity

$z_1 z_1 \approx z_1$
Model Checking

Fix $u, v$ semigroup words over variables $z_1, \ldots, z_m$

**Model($u \approx v$)**

Input: $a_1, \ldots, a_k \in T_n$

Output: Whether $\langle a_1, \ldots, a_k \rangle$ models $u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$.

**Example: Band Identity**

$z_1z_1 \approx z_1$

**Theorem**

Model($u \approx v$) is in $P$. 
Let $W$ be the set of all prefixes of $u$ and $v$ including the empty word 1. For $x \in \mathbb{N}$, $s_1, \ldots, s_m \in S$ define evaluations,

$$e(x, s_1, \ldots, s_m): W \rightarrow \mathbb{N}, \quad w \mapsto xw(s_1, \ldots, s_m).$$

$$E(W, S) := \{e(x, s_1, \ldots, s_m) : x \in \mathbb{N}, s_1, \ldots, s_m \in S\} \subseteq \mathbb{N}^W.$$

Then $S$ models $u \approx v$ iff $f(u) = f(v)$ for all $f \in E(W, S)$. 
Let $W$ be the set of all prefixes of $u$ and $v$ including the empty word $1$. For $x \in [n], s_1, \ldots, s_m \in S$ define evaluations,

$$e(x, s_1, \ldots, s_m): W \rightarrow [n], \ w \mapsto xw(s_1, \ldots, s_m).$$

$$E(W, S) := \{ e(x, s_1, \ldots, s_m) : x \in [n], s_1, \ldots, s_m \in S \} \subseteq [n]^W.$$ 

Then $S$ models $u \sim v$ iff $f(u) = f(v)$ for all $f \in E(W, S)$.

**Example: Band Identity**

$$E(W, S) := \{ (x, xs, xs^2) : x \in [n], s \in S \}$$
Lemma

Let $S = \langle a_1, \ldots, a_k \rangle \subseteq T_n$, $d \in \mathbb{N}$, and $f \in [n]^d$. Then $fS$ can be enumerated in $O(n^d k)$ time.
Lemmas

Lemma

Let $S = \langle a_1, \ldots, a_k \rangle \subseteq T_n$, $d \in \mathbb{N}$, and $f \in [n]^d$. Then $fS$ can be enumerated in $O(n^d k)$ time.

Definition

The degree-d transformation graph of $S = \langle a_1, \ldots, a_k \rangle$ is $G^d = (V, E)$ having vertices $V = [n]^d$ and edges $E = \{(x, y) \in V^2 : \exists i \in [k](xa_i = y)\}$, where $S$ acts on $[n]^d$ component-wise.

Enumerate $fS$ using depth-first search algorithm. There are a maximum of $n^d k$ edges and the algorithm traverses each once, hence $O(n^d k)$ time.
**Lemma**

Let $S = \langle a_1, ..., a_k \rangle \subseteq T_n$, $d \in \mathbb{N}$, and $f \in [n]^d$. Then $fS$ can be enumerated in $O(n^d k)$ time.

**Definition**

The **degree-$d$ transformation graph** of $S = \langle a_1, ..., a_k \rangle$ is $G^d = (V, E)$ having vertices $V = [n]^d$ and edges $E = \{(x, y) \in V^2 : \exists i \in [k] (xa_i = y)\}$, where $S$ acts on $[n]^d$ component-wise.

Enumerate $fS$ using depth-first search algorithm. There are a maximum of $n^d k$ edges and the algorithm traverses each once, hence $O(n^d k)$ time.

**Lemma**

Let $f \in [n]^W$. Then $f \in E(W, S)$ iff

$\forall i \in [m] \exists g \in fS \ \forall wz_i \in W : f(wz_i) = g(w).$
Extension of Model($u \approx v$) strategy

We now return to the problem of determining if $S := \langle a_1, \ldots, a_k \rangle \leq T_n$ is completely regular.

**Lemma**

$a \in T_n$ generates a subgroup iff $a|_{\text{Im}(a)}$ is a permutation.

[Proof of lemma omitted]
Extension of Model($u \approx v$) strategy

We now return to the problem of determining if $S := \langle a_1, \ldots, a_k \rangle \leq T_n$ is completely regular.

**Lemma**

$a \in T_n$ generates a subgroup iff $a|_{\text{Im}(a)}$ is a permutation.

[Proof of lemma omitted]

Let $W = \{1, z, z^2\}$ and define:

$$e((x, y), s) : W \to [n]^2, w \mapsto (x, y)w(s)$$

$$E(W, S) := \{e((x, y), s) : (x, y) \in [n]^2, s \in S\} \subseteq [n]^6$$

Then every element of $S$ permutes its images iff for every $f \in E(W, S)$,

$$f(z) \notin \{(x, x) : x \in [n]\} \implies f(z^2) \notin \{(x, x) : x \in [n]\}.$$
Quasi-Identities

Open Problem: Quasi-Identities

Complexity of whether $S$ models

$u_1(z_1, \ldots, z_m) \approx v_1(z_1, \ldots, z_m) \Rightarrow u_2(z_1, \ldots, z_m) \approx v_2(z_1, \ldots, z_m)$?
Quasi-Identities

Open Problem: Quasi-Identities

Complexity of whether $S$ models

$$u_1(z_1, \ldots, z_m) \simeq v_1(z_1, \ldots, z_m) \Rightarrow u_2(z_1, \ldots, z_m) \simeq v_2(z_1, \ldots, z_m)?$$

Model($$z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u \approx v$$)

Input: $a_1, \ldots, a_k \in T_n$
Output: Whether $\langle a_1, \ldots, a_k \rangle$ models $z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u \approx v$
Quasi-Identities

Open Problem: Quasi-Identities

Complexity of whether $S$ models

$$u_1(z_1, \ldots, z_m) \approx v_1(z_1, \ldots, z_m) \Rightarrow u_2(z_1, \ldots, z_m) \approx v_2(z_1, \ldots, z_m)$$

Model($z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u \approx v$)

Input: $a_1, \ldots, a_k \in T_n$
Output: Whether $\langle a_1, \ldots, a_k \rangle$ models $z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u \approx v$

Idempotent Quasi-Identity Examples

1. idempotents are central: $z_1 \approx z_1^2 \Rightarrow z_1z_2 \approx z_2z_1$
2. idempotents commute: $z_1 \approx z_1^2, z_2 \approx z_2^2 \Rightarrow z_1z_2 \approx z_2z_1$
3. Clifford semigroup (completely regular and idempotents commute)
4. composition of idempotents are idempotent:
   $$z_1 \approx z_1^2, z_2 \approx z_2^2 \Rightarrow z_1z_2 \approx (z_1z_2)^2$$
Idempotent Quasi-Identity Problems are in P.

Theorem

\[
\text{Model}(z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u \approx v) \text{ is in } P.
\]
Idempotent Quasi-Identity Problems are in P.

**Theorem**

Model\( (z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u \approx v) \) is in P.

**Lemma**

Let \( W \) be the set of prefixes of \( u, v \in \{z_1, \ldots, z_m\}^* \), and \( S \subseteq T_n \). TFAE:

1. \( S \) models \( z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m) \).

2. \( \forall \alpha \in [n], \forall s_1, \ldots, s_m \in S : [\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2] \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m). \)
Idempotent Quasi-Identity Problems are in P.

**Theorem**

\[
\text{Model}(z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u \approx v) \text{ is in } P.
\]

**Lemma**

Let \( W \) be the set of prefixes of \( u, v \in \{z_1, \ldots, z_m\}^* \), and \( S \leq T_n \). TFAE:

1. \( S \) models \( z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m) \).

2. \( \forall x \in [n], \forall s_1, \ldots, s_m \in S : [\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2] \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m) \).

To obtain the Theorem from the Lemma, let
\( W' := W \cup \{wz_i^2 : wz_i \in W, 1 \leq i \leq \ell\} \). Enumerate \( E(W', S) \) and check if each \( f \in E(W', S) \) satisfies:
\[
[\forall i \in [\ell], \forall wz_i \in W : f(wz_i) = f(wz_i^2)] \Rightarrow f(u) = f(v).
\]
Sketch of Lemma Proof

Lemma

Let $W$ be the set of prefixes of $u, v \in \{z_1, \ldots, z_m\}^*$, and $S \leq T_n$. TFAE:

1. $S$ models $z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$.

2. $\forall x \in [n], \forall s_1, \ldots, s_m \in S : \forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2 \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m)$.

Proof Sketch: (2) $\Rightarrow$ (1)
Sketch of Lemma Proof

**Lemma**

Let $W$ be the set of prefixes of $u, v \in \{z_1, \ldots, z_m\}^*$, and $S \leq T_n$. TFAE:

1. $S$ models $z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$.

2. $\forall x \in [n], \forall s_1, \ldots, s_m \in S : [\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2] \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m)$.

**Proof Sketch: (2) $\Rightarrow$ (1)**

Let $s_1, \ldots, s_\ell$ be idempotent.
Lemma

Let $W$ be the set of prefixes of $u, v \in \{z_1, \ldots, z_m\}^*$, and $S \leq T_n$. TFAE:

1. $S$ models $z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$.

2. $\forall x \in [n], \forall s_1, \ldots, s_m \in S : [\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2] \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m)$.

Proof Sketch: (2) $\Rightarrow$ (1)

Let $s_1, \ldots, s_\ell$ be idempotent.

Then for each $x \in [n], i \in [\ell]$, and $wz_i \in W$:

$xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2$. 
Lemma

Let $W$ be the set of prefixes of $u, v \in \{z_1, \ldots, z_m\}^*$, and $S \subseteq T_n$. TFAE:

1. $S$ models $z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$.

2. $\forall x \in [n], \forall s_1, \ldots, s_m \in S : \forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2 \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m)$.

Proof Sketch: (2) $\Rightarrow$ (1)

Let $s_1, \ldots, s_\ell$ be idempotent.

Then for each $x \in [n]$, $i \in [\ell]$, and $wz_i \in W$:

$xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2$.

Thus, by (2), $xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m)$ for every $x \in [n]$.  

Sketch of Lemma Proof

Lemma

Let $W$ be the set of prefixes of $u, v \in \{z_1, \ldots, z_m\}^*$, and $S \leq T_n$. TFAE:

1. $S$ models $z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$.

2. $\forall x \in [n], \forall s_1, \ldots, s_m \in S : [\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2] \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m)$.

Proof Sketch: (1) $\Rightarrow$ (2)
Sketch of Lemma Proof

Lemma

Let $W$ be the set of prefixes of $u, v \in \{z_1, \ldots, z_m\}^*$, and $S \leq T_n$. TFAE:

1. $S$ models $z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$.

2. $\forall x \in [n], \forall s_1, \ldots, s_m \in S : [\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2] \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m)$.

Proof Sketch: (1) $\Rightarrow$ (2)

Pick any $x \in [n], s_1, \ldots, s_m \in S$ satisfying:

$\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2$. 
Sketch of Lemma Proof

Lemma

Let $W$ be the set of prefixes of $u, v \in \{z_1, \ldots, z_m\}^*$, and $S \subseteq T_n$. TFAE:

1. $S$ models $z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$.

2. $\forall x \in [n], \forall s_1, \ldots, s_m \in S : [\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2] \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m)$.

Proof Sketch: $(1) \Rightarrow (2)$

Pick any $x \in [n], s_1, \ldots, s_m \in S$ satisfying:

$\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2$.

Then $xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^{k_i}$ for each $wz_i \in W$ and $k_i \in \mathbb{N}$. 
Sketch of Lemma Proof

Lemma

Let $W$ be the set of prefixes of $u, v \in \{z_1, \ldots, z_m\}^*$, and $S \leq T_n$. TFAE:

1. $S$ models $z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$.

2. $\forall x \in [n], \forall s_1, \ldots, s_m \in S : [\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2] \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m)$.

Proof Sketch: (1) $\Rightarrow$ (2)

Pick any $x \in [n], s_1, \ldots, s_m \in S$ satisfying:

$\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2$.

Then $xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^{k_i}$ for each $wz_i \in W$ and $k_i \in \mathbb{N}$.

For each $i \in [\ell]$, let $k_i \in \mathbb{N}$ satisfy $s_i^{k_i} = (s_i^{k_i})^2$. By induction on the length of $u$: $xu(s_1, \ldots, s_m) = xu(s_1^{k_1}, \ldots, s_\ell^{k_\ell}, \ldots, s_m)$. 
Sketch of Lemma Proof

Lemma

Let $W$ be the set of prefixes of $u, v \in \{z_1, \ldots, z_m\}^*$, and $S \leq T_n$. TFAE:

1. $S$ models $z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m)$.

2. $\forall x \in [n], \forall s_1, \ldots, s_m \in S : [\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2] \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m)$.

Proof Sketch: (1) $\Rightarrow$ (2)

Pick any $x \in [n], s_1, \ldots, s_m \in S$ satisfying:

$\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2$.

Then $xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^{k_i}$ for each $wz_i \in W$ and $k_i \in \mathbb{N}$.

For each $i \in [\ell]$, let $k_i \in \mathbb{N}$ satisfy $s_i^{k_i} = (s_i^{k_i})^2$. By induction on the length of $u$: $xu(s_1, \ldots, s_m) = xu(s_1^{k_1}, \ldots, s_\ell^{k_\ell}, \ldots, s_m)$.

Similarly: $xv(s_1, \ldots, s_m) = xv(s_1^{k_1}, \ldots, s_\ell^{k_\ell}, \ldots, s_m)$.
Transformation Graphs

Sketch of Lemma Proof

Lemma

Let \( W \) be the set of prefixes of \( u, v \in \{ z_1, \ldots, z_m \}^* \), and \( S \leq T_n \). TFAE:

1. \( S \) models \( z_1 \approx z_1^2, \ldots, z_\ell \approx z_\ell^2 \Rightarrow u(z_1, \ldots, z_m) \approx v(z_1, \ldots, z_m) \).
2. \( \forall x \in [n], \forall s_1, \ldots, s_m \in S : [\forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2] \Rightarrow xu(s_1, \ldots, s_m) = xv(s_1, \ldots, s_m) \).

Proof Sketch: (1) \( \Rightarrow \) (2)

Pick any \( x \in [n], s_1, \ldots, s_m \in S \) satisfying:

\[ \forall i \in [\ell], \forall wz_i \in W : xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^2. \]

Then \( xw(s_1, \ldots, s_m)s_i = xw(s_1, \ldots, s_m)s_i^{k_i} \) for each \( wz_i \in W \) and \( k_i \in \mathbb{N} \).

For each \( i \in [\ell] \), let \( k_i \in \mathbb{N} \) satisfy \( s_i^{k_i} = (s_i^2)^{k_i} \). By induction on the length of \( u \):

\[ xu(s_1, \ldots, s_m) = xu(s_1^{k_1}, \ldots, s_\ell^{k_\ell}, \ldots, s_m). \]

Similarly:

\[ xv(s_1, \ldots, s_m) = xv(s_1^{k_1}, \ldots, s_\ell^{k_\ell}, \ldots, s_m). \]

By (1), \( xu(s_1^{k_1}, \ldots, s_\ell^{k_\ell}, \ldots, s_m) = xv(s_1^{k_1}, \ldots, s_\ell^{k_\ell}, \ldots, s_m) \).
Quantified Identities

Open Problem: Quantified Identities

Complexity of whether $S$ models

$$\exists z_1, \ldots, z_{\ell} \forall z_{\ell+1}, \ldots, z_m (u_1(z_1, \ldots, z_m) \approx v_1(z_1, \ldots, z_m))$$

Examples:

$$\exists z_1(z_1 z_2 \approx z_1) \text{ (left zero)} \text{ and } \exists z_1(z_2 z_1 \approx z_1) \text{ (right zero)}$$

Theorem

Determining if a transformation semigroup has a left zero is in $P$.

Theorem

Determining if a transformation semigroup has a right zero is in $P$. 
Quantified Identities

Open Problem: Quantified Identities

Complexity of whether $S$ models

$$\exists z_1, \ldots, z_\ell \forall z_{\ell+1}, \ldots, z_m (u_1(z_1, \ldots, z_m) \approx v_1(z_1, \ldots, z_m))$$

Examples: $\exists z_1(\left. z_1 z_2 \right. \approx z_1)$ (left zero) and $\exists z_1(\left. z_2 z_1 \right. \approx z_1)$ (right zero).
Quantified Identities

Open Problem: Quantified Identities
Complexity of whether $S$ models
$$\exists z_1, \ldots, z_\ell \forall z_{\ell+1}, \ldots, z_m (u_1(z_1, \ldots, z_m) \approx v_1(z_1, \ldots, z_m))?$$

Examples: $\exists z_1 (z_1 z_2 \approx z_1)$ (left zero) and $\exists z_1 (z_2 z_1 \approx z_1)$ (right zero).

Theorem
Determining if a transformation semigroup has a left zero is in P.
Quantified Identities

Open Problem: Quantified Identities

Complexity of whether $S$ models

$\exists z_1, \ldots, z_\ell \forall z_{\ell+1}, \ldots, z_m (u_1(z_1, \ldots, z_m) \approx v_1(z_1, \ldots, z_m))$?

Examples: $\exists z_1 (z_1 z_2 \approx z_1)$ (left zero) and $\exists z_1 (z_2 z_1 \approx z_1)$ (right zero).

Theorem

Determining if a transformation semigroup has a left zero is in P.

Theorem

Determining if a transformation semigroup has a right zero is in P.
Nilpotence

$0 \in S$ is called a **zero** if $s0 = 0 = 0s$ for all $s \in S$. A semigroup $S$ containing a zero is called **nilpotent** if $S^d = \{0\}$ for some $d \in \mathbb{N}$.

**Theorem**

Determining if $S = \langle a_1, \ldots, a_k \rangle \subseteq T_n$ is nilpotent is in P.
Nilpotence

0 ∈ S is called a **zero** if s0 = 0 = 0s for all s ∈ S. A semigroup S containing a zero is called **nilpotent** if S^d = {0} for some d ∈ N.

**Theorem**

Determining if S = ⟨a_1, ..., a_k⟩ ⊆ T_n is nilpotent is in P.

**Lemma**

S is nilpotent iff it has a zero element, 0, and the graph (V, E)

- V := [n] \ \text{Im}(0)
- E := \{(x, y) ∈ V^2 \mid x a_i = y \text{ for some } i ∈ [k]\}

is acyclic.
Open Problems

Open Problem: Semigroup Reguality
How hard is it to check that every element in $S$ is regular?
Open Problems

Open Problem: Semigroup Regularity
How hard is it to check that every element in $S$ is regular?

Open Problem: Quasi-Identities
Complexity of whether $S$ models

$u_1(z_1, ..., z_m) \approx v_1(z_1, ..., z_m) \Rightarrow u_2(z_1, ..., z_m) \approx v_2(z_1, ..., z_m)$?
Open Problems

Open Problem: Semigroup Regularity
How hard is it to check that every element in $S$ is regular?

Open Problem: Quasi-Identities
Complexity of whether $S$ models
$u_1(z_1, \ldots, z_m) \approx v_1(z_1, \ldots, z_m) \Rightarrow u_2(z_1, \ldots, z_m) \approx v_2(z_1, \ldots, z_m)$?

Open Problem: Quantified Identities
Complexity of whether $S$ models
$\exists z_1, \ldots, z_\ell \forall z_{\ell+1}, \ldots, z_m (u_1(z_1, \ldots, z_m) \approx v_1(z_1, \ldots, z_m))$?