Computational Complexity of Semigroup Properties

Trevor Jack

CU Boulder

Joint work with Peter Mayr

Mathematics
UNIVERSITY OF COLORADO BOULDER

Notation and Regularity Problem

Transformation Semigroups

- $[n] = \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S \leq T_n$

Notation and Regularity Problem

Transformation Semigroups

- $[n] = \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S \leq T_n$

Definition

$b \in T_n$ is **regular** in S if for some $s \in S$, $bsb = b$.

Notation and Regularity Problem

Transformation Semigroups

- $[n] = \{1, ..., n\}$
- T_n is the semigroup of all unary functions on $[n]$
- $S \leq T_n$

Definition

$b \in T_n$ is **regular** in S if for some $s \in S$, $bsb = b$.

RegularElement

Input: $a_1, ..., a_k, b \in T_n$
Output: Is b regular in $\langle a_1, ..., a_k \rangle$?

RegularElement Theorem and Proof

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 Σ, 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 Σ, 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 Σ
Output: Whether there is $w \in \Sigma^*$ accepted by each A_i.

Proof Sketch

Proof.

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

- Transformed Set: $Z = \bigsqcup_{i=1}^{\ell} Z_i$ along with new state 0.
- Generators: Σ 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 $A_1, \ldots, A_\ell$. 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. □

Regular Semigroup

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"

Identity Checking

Fix u, v semigroup terms in variables $z_1, \ldots, z_m$

Identity Checking

Fix u, v semigroup terms in variables $z_1, \ldots, z_m$

Model($u \approx v$)

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

Identity Checking

Fix u, v semigroup terms in variables $z_1, \ldots, z_m$

Model($u \approx v$)

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

Example: Band Identity

$z_1 z_1 = u \approx v = z_1$

Identity Checking

Fix u, v semigroup terms in 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

$z_1 z_1 = u \approx v = z_1$

Theorem

Model($u \approx v$) is in P.

Notation

Let W be the set of all initial segments of u and v including the empty word 1. For $x \in [n], s_1, \ldots, s_m \in S$ define evaluations,

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

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

Then S satisfies $u \approx v$ iff $f(u) = f(v)$ for all $f \in F$.

Notation

Let W be the set of all initial segments of u and v including the empty word 1. For $x \in [n], s_1, \ldots, s_m \in S$ define evaluations,

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

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

Then S satisfies $u \approx v$ iff $f(u) = f(v)$ for all $f \in F$.

Example: Band Identity

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

Lemmas

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.

Lemmas

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. Max of $n^d k$ edges.

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. Max of $n^d k$ edges.

Lemma

Let $f \in [n]^W$. Then $f \in F$ iff
$\forall i \in [m]\ \exists g \in fS\ \forall wz_i \in W : f(wz_i) = g(w)$.

Extensions of the above strategy

Back to that completely regular problem...

Lemma

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

We can check whether every element permutes its image by generating

$$F := \{(x, xs, xs^2, y, ys, ys^2) : x, y \in [n], s \in S\} \subseteq [n]^6$$

and checking that $f(2) \neq f(5) \Rightarrow f(3) \neq f(6)$ for each $f \in F$.

Unresolved Extensions

Open Problem: Quasi-Identities

Complexity of whether S models
$u_1(z_1, ..., z_m) \approx v_1(z_1, ..., z_m) \Rightarrow u_2(z_1, ..., z_m) \approx v_2(z_1, ..., z_m)$?

Unresolved Extensions

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: Quantifiers

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

An example of this last question is $\exists z_1(z_1 z_2 \approx z_1)$, the left zero problem.

Definitions and Problems

An element, $0 \in S$, is called a **left zero** if $0s = 0$ for all $s \in S$.

Theorem

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

Definitions and Problems

An element, $0 \in S$, is called a **left zero** if $0s = 0$ for all $s \in S$.

Theorem

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

An element, $0 \in S$, is called a **right zero** if $s0 = 0$ for all $s \in S$.

Theorem

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

Definitions and Problems

An element, $0 \in S$, is called a **left zero** if $0s = 0$ for all $s \in S$.

Theorem

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

An element, $0 \in S$, is called a **right zero** if $s0 = 0$ for all $s \in S$.

Theorem

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

An element, $0 \in S$, is called a **zero** if $s0 = 0 = 0s$ for all $s \in S$.

Theorem

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

Nilpotence

A semigroup S that has a zero element is called **nilpotent** if $S^d = \{0\}$ for some $d \in \mathbb{N}$.

Theorem

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

Nilpotence

A semigroup S that has a zero element is called **nilpotent** if $S^d = \{0\}$ for some $d \in \mathbb{N}$.

Theorem

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

Lemma

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

- $V := [n] \setminus \mathrm{Im}(0)$
- $E := \{(x, y) \in V^2 \mid xa_i = y \text{ for some } i \in [k])\}$

is acyclic.