Computational Complexity of Checking Semigroup Properties in Partial Bijection Semigroups and Inverse Semigroups

Trevor Jack

Illinois Wesleyan University

Finite Inverse Semigroup

Partial Bijection Semigroups

- $[n] := \{1, ..., n\}$
- I_n is the semigroup of all partial bijective functions on $[n]$
- $\mathrm{dom}(ab) := \{x \in \mathrm{dom}(a) : xa \in \mathrm{dom}(b)\}$
- $S = \langle a_1, \ldots, a_k \rangle \leq I_n$

Inverse Semigroups

- A semigroup S is *inverse* iff for each $s \in S$, there exists a unique s^{-1} such that $ss^{-1}s = s$ and $s^{-1}ss^{-1} = s^{-1}$.
- Every finite inverse semigroup can be embedded into some I_n.
- Unless otherwise stated, we presume S is a finite inverse semigroup.

Decision Problems

Generic Semigroup Problem

- Given: $a_1, \ldots, a_k \in I_n$
- Problem: Does $\langle a_1, \ldots, a_k \rangle$ satisfy a certain property?

Current Objective

Compare/contrast the computational complexity of checking for particular properties in partial bijection semigroups and inverse semigroups.

Note: checking for a property in an inverse semigroup is at most as difficult as checking for the same property in a partial bijection semigroup.

Computational Complexity Heirarchy

$$\mathrm{AC}^0 \subseteq \mathrm{L} \subseteq \mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}$$

Characterizing AC^0

Circuit Definition

Sets that are decidable by constant depth circuits of polynomial size consisting of unbounded fanin gates.

AC^0 Semigroup Problems

- AC^0 Semigroup Problems are properties that can be expressed as first-order formulas quantified over points and generators.
- Predicates: $xb_1 \cdots b_i = yc_1 \cdots c_j$ with points $x, y \in [n]$ and generators $b_1, \ldots, b_i, c_1, \ldots, c_j$.

Examples of AC^0 Semigroup Problems

- Commutative: $\forall x \in [n], \forall i, j \in [k](xa_i a_j = xa_j a_i)$.
- Semilattice: $\forall x \in [n], \forall i, j \in [k](xa_i a_j = xa_j a_i \wedge xa_i^2 = xa_i)$.
- Group: $\mathrm{dom}(a_i) = [n]a_j$.

NL-complete for Partial Bijection Semigroups

Definitions

- A semigroup S is said to be **nilpotent** if it has a zero element, $0 \in S$, satisfying $0S = S0 = \{0\}$ and there exists $d \in \mathbb{N}$ such that $S^d = \{0\}$.
- $a, b \in S$ are $\mathcal{R}$-related iff $aS = bS$. S is $\mathcal{R}$-trivial if $a \mathcal{R} b$ implies $a = b$.

Theorem (TJ 2022)

Each of the following three problems are NL-complete. Given generators for a partial bijection semigroup S, checking if: (1) S is nilpotent; (2) S is $\mathcal{R}$-trivial; or (3) all of the idempotents in S are central.

Proof Sketch

Each of these problems are NL-complete for transformation semigroups (Fleischer, TJ, 2022), so we need only show hardness. We reduce from the NL-complete problem of checking if a directed graph $G = (V, E)$ is acyclic.

For each edge $(u, v) \in E$, define a generator $a_{uv} \in I_V$ such that $\mathrm{dom}(a_{uv}) = \{u\}$ and $ua_{uv} = v$. Let S be the generated semigroup.

If G is acyclic, $\mathrm{dom}(s^2) = \emptyset$ for every $s \in S$. Since S is finite, it must be nilpotent and, hence, $\mathcal{R}$-trivial. Its only idempotent is the zero element, which is central.

If G has a cycle $(u_1, \ldots, u_n, u_1)$, then $s = a_{u_1 u_2} \cdots a_{u_n u_1}$ is an idempotent that fixes only u_1. Note, $sa_{u_1 u_2} \neq a_{u_1 u_2} s$ and $s \mathrel{\mathcal{R}} sa_{u_1 u_2}$.

AC^0 for Inverse Semigroups

Note: $\{0\}$ is the only nilpotent inverse semigroup.

Proposition (TJ 2022)

Each of the following two problems are in AC^0. Given generators of an inverse semigroup S, checking if (1) S is $\mathcal{R}$-trivial or (2) all of the idempotents in S are central.

Proof Sketch

Note that idempotents in inverse semigroups commute and that $a \mathcal{R} aa^{-1}$, so an inverse semigroup is $\mathcal{R}$-trivial iff it is a semilattice. This can be checked in AC^0 even for transformation semigroups (Fleischer, TJ, 2019). Suppose every idempotent is central. Then $sss^{-1} = ss^{-1}s = s$ and thus every element permutes its image. Suppose every element generates a subgroup. Equivalently, $\mathrm{dom}(ab) = \mathrm{dom}(a) \cap \mathrm{dom}(b)$ for every $a, b \in S$ (TJ 2022). Then for any idempotent e, and any $s \in S$, $\mathrm{dom}(es) = \mathrm{dom}(se)$ and thus $es = se$.

Zero Membership

Theorem (TJ 2022)

Given generators for a partial bijection semigroup S, determining if S has a zero is a L-complete problem.

Definition

For $A = \{a_1, \ldots, a_k\} \subset I_n$, define the *transformation graph* $\Gamma(A, [n+1])$ to have vertices [n+1] and the following undirected edges:

- $(p, q) \in [n]^2$ if either $pa_i = q$ or $qa_i = p$ for some $i \in [k]$ and
- $(p, n+1)$ if $p \in [n] \setminus \mathrm{dom}(a_i)$ for some $i \in [k]$.

Lemma (TJ 2022)

Let $A = \{a_1, \ldots, a_k\} \subset I_n$ and let S be the partial bijection semigroup generated by the elements of A. Then S has a zero iff the only connected component of $\Gamma(A, [n+1])$ containing more than one vertex is the component containing $n+1$.

Sketch for Proof of Lemma

$\Rightarrow$: Suppose $0 = a_{i_1} \cdots a_{i_m}$.

Pick any $(p, q) \in [n]^2$ in the graph $\Gamma(A, [n])$ such that $p \neq q$.

WLOG, let $a \in A$ satisfy $pa = q$. If $q \in \mathrm{dom}(0)$, then $q0 = pa0 = p0$, contradicting that 0 is a partial bijection.

Then there exists $\ell \in [m]$ such that $qa_{i_1} \cdots a_{i_{\ell-1}} \notin \mathrm{dom}(a_{i_\ell})$.

Hence, q is connected to $n + 1$.

$\Leftarrow$: Let $X \subset [n+1]$ be the connected component containing $n + 1$.

For every $x \in X$, there exists $s \in S$ such that $x \notin \mathrm{dom}(s)$

The element $s \in S$ that minimizes $|X \cap \mathrm{dom}(s)|$ will be the zero element, for which $|X \cap \mathrm{dom}(0)| = 0$.

Sketch for Proof of Theorem

By the Lemma, we need only check that the only connected component of $\Gamma(A, [n+1])$ with more than one vertex also contains $n+1$. Equivalently, for each edge (a, b) with $a \neq b$, check that a is connected to $n+1$.

Reingold's algorithm checks connectedness in undirected graphs in deterministic logspace.

For hardness, we reduce from the L-complete problem of checking if a given permutation that fixes no points consists of a single cycle.

Given a permutation $\sigma \in S_n$, embed it into I_n and define $e \in I_n$ to be the idempotent with $\mathrm{dom}(e) = \{2, \ldots, n\}$.

Then $\langle \sigma, e \rangle$ has a zero element iff σ consists of a single cycle.

Identity Membership

Definition

A semigroup element $1 \in S$ is a *left (resp. right) identity* iff $1s = s$ (resp. $s1 = s$) for each $s \in S$. An element that is both a left and right identity is the unique *identity* of the semigroup.

T_n is the semigroup of transformations $s : [n] \to [n]$.

Theorem (TJ 2022)

Given generators $a_1, \ldots, a_k \in T_n$, enumerating the identities of the generated semigroup is in L.

Note: left and right identities of transformation semigroups must be idempotent powers of generators (Fleischer, TJ, 2019).

Identity Membership

Lemma (TJ 2022)

Let $S := \langle a_1, \ldots, a_k \rangle \leq T_n$.
The idempotent power of a_i is a left identity iff:

$$\forall j \in [k] \forall x, y \in [n] : (xa_i = ya_i \to xa_j = ya_j) \wedge (xa_i^2 = ya_i^2 \to xa_i = ya_i)$$

The idempotent power of a_i is a right identity iff:

$$\forall j, \ell \in [k] \forall x, y \in [n] : (xa_j a_i = ya_\ell a_i \to xa_j = ya_\ell)$$

Sketch of Proof of Theorem: If a_i^ω is a left or right identity, the Lemma guarantees that $xa_i^{\omega+1} = ya_i^2$ implies $xa_i^\omega = ya_i$.

For each $x \in [n]$, find $y \in [n]$ such that $xa_i = ya_i^2$. Then $xa_i^\omega = ya_i$.

Idempotent Membership

Theorem (TJ 2022)

Given generators $a_1, \ldots, a_k \in I_n$ and an idempotent $e \in I_n$, checking if e is in the generated inverse semigroup is a PSPACE-complete problem.

We can guess generators and store the generated element using at most polynomial space. To prove hardness, we will reduce from the following PSPACE-complete problem (Birget, et al., 2000).

Inverse DFA Intersection

Given: DFAs over a shared alphabet Σ, each with unique sets of states, a start state, a final state, and transitions satisfying the following conditions for any states a, b and any word $w \in \Sigma^*$: (1) $pw = qw$ implies $p = q$ and (2) there exists $w^{-1} \in \Sigma^*$ such that $pww^{-1} = pw^{-1}w = p$.

Problem: Is there a word $w \in \Sigma^*$ that sends each start state to its corresponding final state?

Proof Sketch

Let $Q_1, \ldots, Q_k$ be the disjoint sets of states for the given DFAs. Let $p_1, \ldots, p_k$ and $q_1, \ldots, q_k$ be their start and final states, respectively. Let $\Sigma = \{a_1, \ldots, a_m\}$.

Let $Q := \{0\} \cup \bigcup_{i \in [k]} Q_i$.
Extend each a_i to act on Q by fixing the additional state 0.

Define idempotents e and r whose domains are $\{p_1, \ldots, p_k\}$ and $\{q_1, \ldots, q_k\}$, respectively. We claim $f \in \langle a_1, \ldots, a_m, e \rangle$ iff there exists $w \in \Sigma^*$ such that $p_i w = q_i$ for each $i \in [k]$.

$\Leftarrow$: Suppose such a w exists. Then $f = w^{-1} e w$.

$\Rightarrow$: Since $0 \notin \mathrm{dom}(f)$, $f = f_1 e f_2$ with $f_1 \in \langle a_1, \ldots, a_m \rangle$ and $f_2 \in \langle a_1, \ldots, a_m, e \rangle$.

Then $p_i f_1 = q_i$ for every $i \in [k]$.

Thank You!