The Subpower Intersection Problem for Semigroups

Sangman Lee

BLAST, May 20, 2025

Mathematics
UNIVERSITY OF COLORADO BOULDER

The Subpower Membership Problem (SMP)

In connection with the universal algebraic approach to CSPs[1], Idziak et al. introduced the subpower membership problem in 2007.

Let S be a fixed finite algebra.

$\mathrm{SMP}(S)$

Input:	$A \subseteq S^n, b \in S^n$
Problem:	Is $b \in \langle A \rangle$?

[1] Idziak, P., Marković, P., McKenzie, R., Valeriote, M., and Willard, R., Tractability and learnability arising from algebras with few subpowers, SIAM J. Comput. **39** (2010), no. 7, 3023–3037; MR2678065

Known Results on SMP

Vector spaces, Groups	In P [1]
General algebras	In EXPTIME [2]
Malcev algebras	In NP [3]
Semigroups	In PSPACE [4]
Full transformation semigroup T_2	In P [4]
Full transformation semigroup T_3	PSPACE-complete [4]
Clifford semigroups	In P [4]
Commutative semigroups	P/NP-complete dichotomy [4]
Bands	P/NP-complete dichotomy [5]
Rees matrix semigroups	in P [5]
Combin. Rees matrix semigroups	P/NP-complete dichotomy [5]
(With adjoined identity)	P/NP-c./PSPACE-c. trichotomy [5]

[1] Talk at Nashville by Willard (June 2007)

[2] Kozik constructed some EXPTIME-complete examples (Kozik, 2008)

[3] Mayr (2012)

[4] Bulatov, Kozik, Mayr, and Steindl (2016)

[5] Steindl (2017, 2015, 2019, 2019)

The Subpower Intersection Problem (SIP)

Let S be a fixed finite algebra.

$\mathrm{SIP}(S)$

Input:	$A, B \subseteq S^n$
Problem:	Is $\langle A \rangle \cap \langle B \rangle \neq \emptyset$?

For monoids: Trivial

For semigroups: ?

We are interested in the complexity of the SIP for semigroups.

Difference Between $\mathrm{SMP}(S)$ and $\mathrm{SIP}(S)$

Let S be a finite semigroup.

$\mathrm{SIP}(S)$

Input:	$A, B \subseteq S^n$
Problem:	Is $\langle A \rangle \cap \langle B \rangle \neq \emptyset$?

Although some proof techniques from Bulatov et al.[1] for $\mathrm{SMP}(S)$ extend to $\mathrm{SIP}(S)$, the absence of a specific target element often requires us to consider numerous potential candidates for common elements in $\langle A \rangle$ and $\langle B \rangle$.

This makes it more difficult to apply the bounding/approximation techniques used for $\mathrm{SMP}(S)$.

[1] Bulatov, A., Kozik, M., Mayr, P., and Steindl, M., The subpower membership problem for semigroups (2016)

Complexity Results for $\mathrm{SMP}(S)$ and $\mathrm{SIP}(S)$

Class	$\mathrm{SMP}(S)$	$\mathrm{SIP}(S)$
Semigroups	In PSPACE[1]	In PSPACE[3]
T_2	In P[1]	?
T_3	PSPACE-complete[1]	PSPACE-complete[3]
Clifford	In P[1]	In P[3]
Commutative	P/NP-complete[1]	In P[3]
Bands	P/NP-complete[2]	In P (normal) / In NP [3]
Rees matrix s.	in P[2]	In P[3]

[1] Bulatov, Kozik, Mayr, and Steindl (2016)
[2] Steindl (2017, 2015)
[3] Sangman Lee (2025)

The SIP for Finite Semigroups

Theorem (SL, 2025)

The SIP for any finite semigroup is in PSPACE.

We use the same argument as in the proof of SMP for any finite semigroup by Bulatov et al. (2016) to show that $\mathrm{SIP}(S)$ is in nondeterministic linear space.

Definition

Let S be a semigroup. The set of all idempotent elements in S, denoted by $E(S)$, is defined as

$$E(S) := \{e \in S : e^2 = e\}.$$

Proposition

$\mathrm{SMP}(S)$ restricted to instances where $b \in E(S^n)$ reduces to $\mathrm{SIP}(S)$ in polynomial time.

Definition

T_n is the semigroup of all functions on $\{1, 2, \ldots, n\}$.

The SIP for T_3

Kozen (1977) showed that the following decision problem is PSPACE-complete:

Kozen's composition problem

Input:	n and functions $f, f_1, \dots, f_m : [n] \to [n]$
Problem:	Is f a composition of $f_1, \dots, f_m$?

Theorem (SL, 2025)

$\mathrm{SIP}(T_3)$ is PSPACE-complete.

- Bulatov et al. (2016) showed that Kozen's composition problem reduces to $\mathrm{SMP}(T_3)$ restricted to instances where $b \in E(T_3^n)$ in polynomial time.
- Hence, $\mathrm{SIP}(T_3)$ is PSPACE-complete.

The SIP for Bands

Lemma (Steindl, 2017)

Let S be a finite band. Then there is a polynomial p such that every k-ary term function on S is induced by a word of length at most $p(k)$.

Theorem (SL, 2025)

The SIP for any finite band is in NP.

- Use the above lemma to show that SIP for bands is in NP.

Green's Relations for Semigroups

Definition

For $a, b \in S$ let

$$a \leq_{\mathcal{L}} b \text{ if } S^1 a \subseteq S^1 b,$$
$$a \leq_{\mathcal{R}} b \text{ if } aS^1 \subseteq bS^1,$$
$$a \leq_{\mathcal{J}} b \text{ if } S^1 a S^1 \subseteq S^1 b S^1.$$

$\leq_{\mathcal{L}}, \leq_{\mathcal{R}}, \leq_{\mathcal{J}}$ are preorders on S.

The SIP for Normal Bands

Definition

A *normal band* is a band (idempotent semigroup) S satisfying

$$axyb = ayxb \text{ for all } a, b, x, y \in S.$$

Corollary (SL, 2025)

Let S be a normal band. Let $\leq$ be one of the preorders $\leq_L, \leq_R, \leq_J$. Then for $x, y, z \in S$,

$$x \leq y, z \Rightarrow x \leq yz, zy.$$

Moreover, for $a, b, x, y \in S$ with $x \mathcal{J} y$,

$$axyb = axb = ayb.$$

The SIP for Normal Bands

Theorem (SL,2025)

The SIP for any finite normal band is in P.

- Our algorithm iterates through tuples $(\alpha, \beta, \gamma, \delta) \in A \times A \times B \times B$ checking if there exist $x \in \langle A \rangle$, $y \in \langle B \rangle$ where

$$\alpha x \beta = \gamma y \delta.$$

- Finding such (x, y) shows

$$\alpha x \beta = \gamma y \delta \in \langle A \rangle \cap \langle B \rangle \neq \emptyset.$$

- Otherwise, $\langle A \rangle \cap \langle B \rangle = \emptyset$.

SIP for Normal Bands

ExistIntermediateProducts(A, B, α, β, γ, δ):

Inputs: $A, B \subseteq S^n$, $\alpha, \beta, \gamma, \delta \in S^n$

Output: Are there $x \in \langle A \rangle$ and $y \in \langle B \rangle$ such that $\alpha x \beta = \gamma y \delta$?

1: Check if A and B are non-empty

2: Compute $p_A := \prod_{a \in A} a$ and $p_B := \prod_{b \in B} b$

3: Check if $\alpha p_A \beta \leq_{\mathcal{J}} \gamma$ and $\gamma p_B \delta \leq_{\mathcal{J}} \beta$

4: Check if $\alpha p_A \beta \leq_{\mathcal{L}} \delta$ and $\gamma p_B \delta \leq_{\mathcal{R}} \alpha$

5: Refine $A_{new} := \{a \in A \mid \gamma p_B \delta \leq_{\mathcal{J}} a\}$

6: Refine $B_{new} := \{b \in B \mid \alpha p_A \beta \leq_{\mathcal{J}} b\}$

7: If $A_{new} = A$ and $B_{new} = B$, return True

8: Otherwise, return **ExistIntermediateProducts(A_{new}, B_{new}, α, β, γ, δ)**

An observation

Proposition (SL, 2025)

Let S be a finite semigroup and $A, B \subseteq S$. Then

$$\langle A \rangle \cap \langle B \rangle \neq \emptyset \iff E(\langle A \rangle) \cap E(\langle B \rangle) \neq \emptyset$$

Q: Can we have a canonical form of $E(S)$?

Definition

A semigroup S is called an *E-semigroup* if $E(S)$ is a subsemigroup of S.

Lemma (SL, 2025)

Let S be a finite E-semigroup with idempotent separating congruence $\sim$ such that $S/\sim$ is commutative. Let A be a generating set for S. Then

$$E(S) = \langle \{a^{\omega} : a \in A\} \rangle.$$

- $\pi : S \to S/\sim$ restricted to $E(S)$ is an injective homomorphism.
- So, $E(S)$ is a commutative semigroup.
- Any product of idempotent powers is an idempotent.
- Conversely, any idempotent is a product of idempotent powers using the idempotent separateness of $\sim$ and the commutativity of $S/\sim$.

Theorem (SL, 2025)

Let S be a finite E-semigroup with idempotent separating congruence $\sim$ such that $S/\sim$ is commutative. Then the $\mathrm{SIP}(S)$ is in P.

Proof.

Recall for $\mathrm{SIP}(S)$ with an instance $A, B \subseteq S^n$,

$$\langle A \rangle \cap \langle B \rangle \neq \emptyset \iff E(\langle A \rangle) \cap E(\langle B \rangle) \neq \emptyset.$$

By the previous lemma,

$$\langle A \rangle \cap \langle B \rangle \neq \emptyset \iff \langle \{a^\omega : a \in A\} \rangle \cap \langle \{b^\omega : b \in B\} \rangle \neq \emptyset.$$

So, $\mathrm{SIP}(S)$ with an instance $A, B \subseteq S^n$ reduces to $\mathrm{SIP}(E(S))$ with an instance $\{a^\omega : a \in A\}, \{b^\omega : b \in B\} \subseteq E(S)^n$ in polynomial time. Finally, $\mathrm{SIP}(E(S))$ is in P because $E(S)$ is a commutative semigroup and SIP for normal bands is in P. So $\mathrm{SIP}(S)$ is in P. $\square$

SIP for Commutative/Clifford Semigroups is in P

Corollary (SL, 2025)

The SIP for any finite commutative semigroup or finite Clifford semigroup is in P.

- Commutative semigroup: use $=$ in previous theorem
- Clifford semigroup: use Green's $\mathcal{H}$-relation in previous theorem (Note that idempotents are central in Clifford semigroups and $S/\mathcal{H}$ is a semilattice.)

One Notable Reduction

- $\mathrm{SIP}(S) \leq_p \mathrm{SIP}(S/\sim)$ if $\sim$ is an idempotent separating congruence for any finite semigroup S.
- With the above reduction, we have an alternative proof that SIP for Clifford semigroups is in P. (But this reduction is not really helpful for commutative semigroups.)
- We can also show that SIP for Rees matrix semigroups over a group is in P using this reduction.

Open Problems

1. Is $\mathrm{SIP}(T_2)$ in P?
2. Is $\mathrm{SIP}(E(T_2))$ in P?
3. Is SIP NP-complete for all non-normal bands?

Thank you!