J. Aust. Math. Soc. **106** (2019), 127–142
doi:10.1017/S1446788718000010

ON SEMIGROUPS WITH PSPACE-COMPLETE SUBPOWER MEMBERSHIP PROBLEM

MARKUS STEINDL

(Received 11 May 2016; accepted 19 November 2017; first published online 30 May 2018)

Communicated by M. Jackson

Abstract

Fix a finite semigroup S and let $a_1, \dots, a_k, b$ be tuples in a direct power S^n. The subpower membership problem (SMP) for S asks whether b can be generated by $a_1, \dots, a_k$. For combinatorial Rees matrix semigroups we establish a dichotomy result: if the corresponding matrix is of a certain form, then the SMP is in P; otherwise it is NP-complete. For combinatorial Rees matrix semigroups with adjoined identity, we obtain a trichotomy: the SMP is either in P, NP-complete, or PSPACE-complete. This result yields various semigroups with PSPACE-complete SMP including the six-element Brandt monoid, the full transformation semigroup on three or more letters, and semigroups of all n by n matrices over a field for $n \geq 2$.

2010 *Mathematics subject classification*: primary 20M99; secondary 68Q25.

Keywords and phrases: subalgebras of powers, membership test, computational complexity, PSPACE-complete, NP-complete.

1. Introduction

In this paper we continue the investigation of the subpower membership problem (SMP) for semigroups started in [1] and [11]. At the *C*onference on Order, Algebra, and Logics in Nashville, 2007, Ross Willard proposed the SMP as follows [12]: fix a finite algebraic structure S with finitely many basic operations. Then the *subpower membership problem* for S is the following decision problem:

SMP(S)
Input: $\{a_1, \dots, a_k\} \subseteq S^n, b \in S^n$
Problem: Is b in the subalgebra of S^n generated by $a_1, \dots, a_k$?

The SMP occurs in connection with the constraint satisfaction problem (CSP) [5]. In the algebraic approach to the CSP, each constraint relation is considered to be a subalgebra of a power (*subpower*) of a certain finite algebra whose operations are

The author was supported by the Austrian Science Fund (FWF): P24285.

the polymorphisms of the constraint language. Instead of storing all elements of a constraint relation, we can store a set of generators. Checking whether a given tuple belongs to a constraint relation represented by its generators is precisely the SMP for the polymorphism algebra.

The input size of SMP(S) is essentially $(k+1)n$. Since the size of the subalgebra generated by $a_1, \dots, a_k$ is limited by $|S|^n$, one can enumerate all elements in time exponential in n using a straightforward closure algorithm. Thus SMP(S) is in EXPTIME for every algebra S. However, the following questions arise.

- How does the algebra S affect the computational complexity of SMP(S)?
- For which algebras S can SMP(S) be solved in time polynomial in k and n?
- When is the problem complete in NP, PSPACE, or EXPTIME? Can it also be complete in a class other than these?

Mayr [8] proved that the SMP for Mal'cev algebras is in NP. He also showed that for certain generalizations of groups and quasigroups the SMP is in Kozik [7] constructed a finite algebra with EXPTIME-complete SMP.

For semigroups the SMP is in PSPACE. This was shown in [1] by Bulatov, Kozik, Mayr, and the author of the present paper. We also proved that the SMP of the full transformation semigroup on three letters is PSPACE-complete. It was the first algebra known to have a PSPACE-complete SMP. In the same paper a dichotomy result for commutative semigroups was established: if a commutative semigroup S embeds into a direct product of a Clifford semigroup and a nilpotent semigroup, then SMP(S) is in P; otherwise it is NP-complete.

Another dichotomy for idempotent semigroups was established in [11]: if an idempotent semigroup S satisfies a certain pair of quasiidentities, then SMP(S) is in P; otherwise it is NP-complete.

The first result of the current work is a condition for semigroups S under which SMP(S) is NP-hard.

THEOREM 1.1. *Let r, s, t be elements of a finite semigroup S such that s does not generate a group and $rs = st = s$. Then* SMP(S) *is* NP*-hard.*

We will prove this result in Section 2 by reducing the Boolean satisfiability problem SAT to SMP(S).

A semigroup is called *combinatorial* if every subgroup has one element. Combinatorial *Rees matrix semigroups* are of the form $\mathcal{M}^0(\{1\}, I, \Lambda, P)$ (see [4, Theorem 3.2.3]). We give the following alternative notation: for nonempty sets I, Λ and a matrix $P \in \{0,1\}^{\Lambda \times I}$ we let $S_P := (I \times \Lambda) \cup \{0\}$ and define a multiplication on S_P by

$$[i,\lambda] \cdot [j,\mu] := \begin{cases} [i,\mu] & \text{if } P(\lambda, j) = 1, \\ 0 & \text{if } P(\lambda, j) = 0, \end{cases}$$
$$0 \cdot [i,\lambda] := [i,\lambda] \cdot 0 := 0 \cdot 0 := 0.$$

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

In this paper we allow the matrix P to have zero rows and zero columns. It is easy to see that S_P is indeed a combinatorial semigroup. We say the matrix $P \in \{0,1\}^{\Lambda \times I}$ has *one block* if there exist $J \subseteq I$, $\Delta \subseteq \Lambda$ such that for $i \in I$, $\lambda \in \Lambda$,

$$P(\lambda, i) = 1 \quad \text{if and only if } (\lambda, i) \in \Delta \times J.$$

For $P = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ we call $B_2 := S_P$ the *Brandt semigroup*, and for $P = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ we denote S_P by A_2.

In Section 3 we establish the following two results.

THEOREM 1.2. *Let S_P be a finite combinatorial Rees matrix semigroup. If the matrix P has one block, then* SMP(S_P) *is in* P. *Otherwise* SMP(S_P) *is* NP*-complete.*

COROLLARY 1.3. *The* SMP *for the Brandt semigroup B_2 and for the semigroup A_2 is* NP*-complete.*

In Section 4 we state a condition for semigroups S under which SMP(S) is PSPACE-complete.

THEOREM 1.4. *Let S be a finite semigroup and $s, t, u \in S$ such that:*

(a) $sts = s$;
(b) *s does not generate a group;*
(c) $su = s$ *and* $tu = t$.

Then SMP(S) *is* PSPACE*-complete.*

In the proof we will reduce a PSPACE-complete function composition problem to SMP(S). It follows that adjoining an identity to B_2 or A_2 already results in a PSPACE-complete SMP.

THEOREM 1.5. *The* SMP *for the Brandt monoid B_2^1 and for the monoid A_2^1 is* PSPACE*-complete.*

This result is part of Corollary 4.3. Both B_2^1 and A_2^1 embed into T_3, the full transformation semigroup on three letters. So Theorem 1.5 generalizes the result from [1] that SMP(T_3) is PSPACE-complete. In addition, B_2 and A_2 are the first groupoids known to have an NP-complete SMP where adjoining an identity yields a groupoid with PSPACE-complete SMP. Further examples of semigroups with PSPACE-complete SMP are listed in Section 4.

In Section 5 we will consider Rees matrix semigroups with adjoined identity and prove the following trichotomy result.

THEOREM 1.6. *Let S_P be a finite combinatorial Rees matrix semigroup.*

(a) *If all entries of the matrix P are* 1, *then* SMP(S_P^1) *is in* P.
(b) *If P has one block and some entries are* 0, *then* SMP(S_P^1) *is* NP*-complete.*
(c) *Otherwise* SMP(S_P^1) *is* PSPACE*-complete.*

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

2. Semigroups with NP-hard SMP

In this section we will prove Theorem 1.1 by reducing the Boolean satisfiability problem SAT to SMP(S). It follows that the SMP for a semigroup S is already NP-hard if S has a $\mathcal{J}$-class that contains both group and nongroup $\mathcal{H}$-classes. Here $\mathcal{J}$ and $\mathcal{H}$ denote two of Green's equivalences. We give the following definitions. For a semigroup S let

$$S^1 := \begin{cases} S \cup \{1\} & \text{if } S \text{ has no identity,} \\ S & \text{otherwise.} \end{cases}$$

For $a, b \in S$ let

$$\begin{aligned} a \,\mathcal{J}\, b &\quad \text{if } S^1aS^1 = S^1bS^1, \\ a \leq_{\mathcal{J}} b &\quad \text{if } S^1aS^1 \subseteq S^1bS^1, \\ a <_{\mathcal{J}} b &\quad \text{if } S^1aS^1 \subset S^1bS^1, \\ a \,\mathcal{H}\, b &\quad \text{if } S^1a = S^1b \text{ and } aS^1 = bS^1. \end{aligned}$$

Note that $S^1aS^1 = SaS \cup Sa \cup aS \cup \{a\}$. The equivalence classes of a with respect to $\mathcal{J}$ and $\mathcal{H}$ are denoted by J_a and H_a, respectively.

We write $[n] := \{1, \ldots, n\}$ for $n \in \mathbb{N}$ and set $[0] := \emptyset$. We consider a tuple b in a direct power S^n to be a function $b\colon [n] \to S$. This means the ith coordinate of b is denoted by $b(i)$ rather than b_i. The subsemigroup generated by a set $A = \{a_1, \ldots, a_k\}$ is denoted by $\langle A \rangle$ or $\langle a_1, \ldots, a_k \rangle$.

Lemma 2.1. *Let s belong to a finite semigroup S. Then s generates a group if and only if $s^2 \,\mathcal{J}\, s$.*

Proof. If s generates a group, then $s^k = s$ for some $k \geq 2$. Thus $s^2 \,\mathcal{J}\, s$.

For the converse let $s^2 \,\mathcal{J}\, s$. First assume the $\mathcal{J}$-class J_s is the minimal ideal of S. Then J_s is a finite simple semigroup by [4, Proposition 3.1.4]. Thus J_s^0 is a finite 0-simple semigroup. By [2, Theorem 2.52(i)] s generates a group.

Now assume J_s is not the minimal ideal of S. Let

$$J(s) := \{r \in S \mid r \leq_{\mathcal{J}} s\}, \quad I(s) := \{r \in S \mid r <_{\mathcal{J}} s\}.$$

By [4, Proposition 3.1.4] the *principal factor* $J(s)/I(s)$ is either null or 0-simple. Since $s^2 \,\mathcal{J}\, s$, the second case applies. By [2, Theorem 2.52(i)] s generates a group. □

Lemma 2.2. *Let r, s, t be elements of a finite semigroup S such that s does not generate a group and $rs = st = s$. Then there are idempotents $e, f \in S$ such that $es = sf = s$ and every product $a_1 \cdots a_k$ in s, e, f in which s occurs at least twice does not yield s.*

Proof. First assume s is regular, that is, $sus = s$ for some $u \in S$. Let e and f be the idempotent powers of su and us respectively. Clearly $es = sf = s$. Let $a_1 \cdots a_k$ be a product in s, e, f, and $i < j$ such that $a_i = a_j = s$. Let $\ell \in \{i+1, \ldots, j\}$ be maximal such that $a_{i+1} = \ldots = a_{\ell-1} = f$. Then $a_i \cdots a_{\ell-1} = s$, and thus $a_i \cdots a_\ell \in \{s^2, se\}$. Note that

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

$se = s(su)^m$ for some $m \in \mathbb{N}$. Now a factor s^2 occurs in the product $a_i \cdots a_\ell$. Since s does not generate a group, Lemma 2.1 implies that $s^2 <_{\mathcal{J}} s$. Thus $a_1 \cdots a_\ell <_{\mathcal{J}} s$, and the result follows.

Now assume s is not regular. By [4, Theorem 3.1.6] the principal factor $J(s)/I(s)$ is null. Let e and f be the idempotent powers of r and t respectively. Let $a_1 \cdots a_k$ be a product in s, e, f, and let $i < j$ such that $a_i = a_j = s$. Then $a_1 \cdots a_i \leq_{\mathcal{J}} s$ and $a_{i+1} \cdots a_k \leq_{\mathcal{J}} s$. Since $J(s)/I(s)$ is null, it follows that $a_1 \cdots a_k <_{\mathcal{J}} s$. □

Proof of Theorem 1.1. Let S satisfy the assumptions. We reduce the Boolean satisfiability problem SAT to SMP(S). SAT is NP-complete [3], and we give the following definition:

SAT
Input: Clauses $C_1, \ldots, C_m \subseteq \{x_1, \ldots, x_k, \neg x_1, \ldots, \neg x_k\}$.
Problem: Do truth values for $x_1, \ldots, x_k$ exist for which the Boolean formula $\Phi(x_1, \ldots, x_k) := (\bigvee C_1) \wedge \ldots \wedge (\bigvee C_m)$ is true?

For all $j \in [k]$ we may assume that x_j or $\neg x_j$ occurs in some clause C_i. We define an SMP(S) instance

$$A := \{a_1^0, \ldots, a_k^0, a_1^1, \ldots, a_k^1\} \subseteq S^{k+m},\ b \in S^{k+m}.$$

Let $e, f \in S$ be idempotents with the properties from Lemma 2.2. Let g be the idempotent power of se. Observe that e and g form a two-element semilattice with $g < e$.

Let $j \in [k]$ and $z \in \{0, 1\}$. For $i \in [k]$ let

$$a_j^z(i) := \begin{cases} f & \text{if } i < j, \\ s & \text{if } i = j, \\ e & \text{if } i > j, \end{cases}$$

and for $i \in [m]$ let

$$a_j^0(k+i) := \begin{cases} g & \text{if } \neg x_j \in C_i, \\ e & \text{otherwise,} \end{cases}$$

$$a_j^1(k+i) := \begin{cases} g & \text{if } x_j \in C_i, \\ e & \text{otherwise.} \end{cases}$$

Let

$$b(i) := s \quad \text{for } i \in [k],$$
$$b(k+i) := g \quad \text{for } i \in [m].$$

We claim that

$$\text{the Boolean formula } \Phi \text{ is satisfiable if and only if } b \in \langle A \rangle. \tag{2.1}$$

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

For the ($\Rightarrow$) direction let $z_1, \dots, z_k \in \{0,1\}$ such that $\Phi(z_1, \dots, z_k) = 1$. We show that

$$b = a_1^{z_1} \cdots a_k^{z_k}. \tag{2.2}$$

For $i \in [k]$ we have $a_1^{z_1} \cdots a_k^{z_k}(i) = e^{i-1} s f^{k-i} = s = b(i)$. For $i \in [m]$ the clause $\bigvee C_i$ is satisfied under the assignment $x_1 \mapsto z_1, \dots, x_k \mapsto z_k$. Thus there is a $j \in [k]$ such that $x_j \in C_i$ and $z_j = 1$, or $\neg x_j \in C_i$ and $z_j = 0$. In both cases $a_j^{z_j}(k+i) = g$, and thus $a_1^{z_1} \cdots a_k^{z_k}(k+i) = g = b(k+i)$. This proves (2.2) and the ($\Rightarrow$) direction of (2.1).

For the ($\Leftarrow$) direction of (2.1) assume $b = a_{j_1}^{z_1} \cdots a_{j_\ell}^{z_\ell}$ for some $\ell \in \mathbb{N}$, $j_1, \dots, j_\ell \in [k]$, and $z_1, \dots, z_\ell \in \{0,1\}$. We show that $j_1, \dots, j_\ell$ are distinct. Suppose $j_p = j_q$ for $p < q$. The factors of the product $a_{j_1}^{z_1} \cdots a_{j_\ell}^{z_\ell}(j_p)$ are given by s, e, f. The factor s occurs at least twice since $a_{j_p}(j_p) = a_{j_q}(j_p) = s$. By Lemma 2.2 this product does not yield s, contradicting our assumption. We define an assignment

$$\begin{aligned} \theta\colon\ & x_{j_1} \mapsto z_1, \dots, x_{j_\ell} \mapsto z_\ell, \\ & x_j \mapsto 0 \quad \text{for } j \in [k] \backslash \{j_1, \dots, j_\ell\}, \end{aligned}$$

and show that θ satisfies the formula Φ. Let $i \in [m]$. Since $a_{j_1}^{z_1} \dots a_{j_\ell}^{z_\ell}(k+i)$ is a product in e, g that yields g, some factor $a_{j_p}^{z_p}(k+i)$ must be g. From the definition of $a_{j_p}^{z_p}$ we see that either $z_p = 0$ and $\neg x_{j_p} \in C_i$, or $z_p = 1$ and $x_{j_p} \in C_i$. This means the formula $\bigvee C_i$ is satisfied under the assignment θ. Since i was arbitrary, Φ is also satisfied. The equivalence (2.1) and the theorem are proved. □

Corollary 2.3. *If a $\mathcal{J}$-class of a finite semigroup S contains both group and nongroup $\mathcal{H}$-classes, then* SMP(S) *is* NP*-hard.*

Proof. Let $s \in S$ such that H_s is not a group and J_s contains group $\mathcal{H}$-classes. From Green's theorem [4, Theorem 2.2.5] we know that s does not generate a group. Since S is finite and J_s contains an idempotent, the element s is regular by [4, Proposition 2.3.1]. That is, there is a $u \in S$ such that $sus = s$. Now su, s, and us fulfill the hypothesis of Theorem 1.1. □

3. Combinatorial Rees matrix semigroups

In this section we will establish a P/NP-complete dichotomy for the SMP for combinatorial Rees matrix semigroups by proving Theorem 1.2. After that we apply this result to combinatorial 0-simple semigroups.

Combinatorial Rees matrix semigroups have the following property.

Lemma 3.1 (see [10, Lemma 2.2]). *Let $k \geq 2$ and $a_1, \dots, a_k$ be elements of a combinatorial Rees matrix semigroup S_P.*

(a) *We have $a_1 \cdots a_k = 0$ if and only if $a_j a_{j+1} = 0$ for some $j \in [k-1]$.*
(b) *If $a_1 \cdots a_k \neq 0$, then there are $i, j \in I$ and $\lambda, \mu \in \Lambda$ such that $a_1 = [i, \lambda]$, $a_k = [j, \mu]$, and $a_1 \cdots a_k = [i, \mu]$.*

Proof. Straightforward. □

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

The next two results will allow us to show that the SMP for a combinatorial Rees matrix semigroup is in NP. Both lemmas have a digraph-theoretic interpretation. For a word w over an alphabet X one can associate a digraph Γ_w with vertex set X and directed edges $a \to b$ for every two-letter subword ab of w. The word w then corresponds to a directed path which starts at the first letter of w, ends at the last letter of w, and traverses every edge of Γ_w at least once. In this interpretation, Lemma 3.3 states that there is a short version of such a path. Finding the shortest path is referred to as the *Chinese postman problem*.

Let v, w be words over variables $x_1, \dots, x_k$. For a semigroup S, w^S denotes the k-ary *term function* induced by w. An expression of the form $v \approx w$ is called an *identity* over $x_1, \dots, x_k$. A semigroup S *satisfies* the identity $v \approx w$ if $v^S = w^S$.

Lemma 3.2 (see [10, Theorem 4.3]). *Let $f := y_1 \cdots y_k$ and $g := z_1 \cdots z_\ell$ be words over an alphabet X such that:*

(a) $\{y_i y_{i+1} \mid i \in [k-1]\} = \{z_j z_{j+1} \mid j \in [\ell - 1]\}$;
(b) $y_1 = z_1$ *and* $y_k = z_\ell$.

Then every combinatorial Rees matrix semigroup S_P satisfies $f \approx g$.

Proof. Let S_P be a combinatorial Rees matrix semigroup, and let $\alpha\colon X^+ \to S_P$ be a homomorphism from the free semigroup over X to S_P. By item (a) we have $\{y_1, \dots, y_k\} = \{z_1, \dots, z_\ell\}$. We claim that

$$\alpha(y_1 \cdots y_k) = 0 \quad \text{if and only if } \alpha(z_1 \cdots z_\ell) = 0. \tag{3.1}$$

Assume $\alpha(y_1 \cdots y_k) = 0$. Then $\alpha(y_i)\alpha(y_{i+1}) = 0$ for some $i \in [k-1]$ by Lemma 3.1(a). By item (a) $y_i y_{i+1} = z_j z_{j+1}$ for some $j \in [\ell - 1]$. Thus $\alpha(z_j)\alpha(z_{j+1}) = 0$, and hence $\alpha(z_1 \cdots z_\ell) = 0$. This proves (3.1).

If $\alpha(y_1 \cdots y_k) = 0$, then $\alpha(y_1 \cdots y_k) = \alpha(z_1 \cdots z_\ell)$ by (3.1). Assume $\alpha(y_1 \cdots y_k) \neq 0$. Then also $\alpha(z_1 \cdots z_\ell) \neq 0$, and Lemma 3.1(b) implies

$$\alpha(y_1) \cdots \alpha(y_k) = \alpha(z_1) \cdots \alpha(z_\ell).$$

This proves the lemma. □

Lemma 3.3. *Let f be a word over $x_1, \dots, x_k$. Then there is a word g such that:*

(a) *the length of g is at most $k(k^2 + 1)$;*
(b) *every combinatorial Rees matrix semigroup satisfies $f \approx g$.*

Proof. Let $f = y_1 \cdots y_\ell$ for $y_1, \dots, y_\ell \in \{x_1, \dots, x_k\}$. We show that there is a word g such that item (b) holds and in which each variable x_i occurs at most $k^2 + 1$ times. Fix $i \in [k]$. Let $j_1, \dots, j_m \in [\ell]$ be the positions of x_i in $y_1 \cdots y_\ell$. Let

$$\begin{aligned} v_1 &:= y_1 \cdots y_{j_1}, \\ v_r &:= y_{j_{r-1}+1} \cdots y_{j_r} \quad \text{for } r \in \{2, \dots, m\}, \\ v_{m+1} &:= y_{j_m+1} \cdots y_\ell. \end{aligned}$$

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

Note that $f = v_1 \cdots v_{m+1}$. Now for every word $h := z_1 \cdots z_n$ over $x_1, \ldots, x_k$ let

$$E(h) := \{z_j z_{j+1} \mid j \in [n-1]\}.$$

It is not hard to see that

$$E(v_1 \cdots v_r) = E(v_1) \cup E(x_i v_2) \cup \ldots \cup E(x_i v_r) \quad \text{for } r \in \{2, \ldots, m+1\}.$$

We define

$$R := \{r \in \{2, \ldots, m\} \mid E(x_i v_r) \not\subseteq E(v_1 \cdots v_{r-1})\}$$

and let

$$g := v_1 \Big(\prod_{r \in R} v_r \Big) v_{m+1}.$$

Clearly g is a concatenation of subwords of f, and f and g start with the same letter. We show that

$$f \text{ and } g \text{ also end with the same letter.} \tag{3.2}$$

If v_{m+1} is nonempty, then (3.2) is clear. If v_{m+1} is empty, then $y_\ell = x_i$, and g ends with a subword v_r for some $r \in [m]$. Since v_r and f both end with x_i, (3.2) is proved. We have

$$\begin{aligned} E(f) = E(v_1 \cdots v_{m+1}) &= E(v_1) \cup \bigcup_{r=2}^{m} E(x_i v_r) \cup E(x_i v_{m+1}) \\ &= E(v_1) \cup \bigcup_{r \in R} E(x_i v_r) \cup E(x_i v_{m+1}) = E(g). \end{aligned}$$

Now Lemma 3.2 implies item (b).

Next observe that $|R| \leq k^2$ by the definitions of R and E. This means x_i occurs at most $k^2 + 1$ times in g. Since x_i was arbitrary, we can reduce the number of occurrences of each variable in f to at most $k^2 + 1$. Item (a) is proved. □

Lemma 3.4. *The* SMP *for a finite combinatorial Rees matrix semigroup is in* NP.

Proof. Let S be such a semigroup, and let $\{a_1, \ldots, a_k\} \subseteq S^n$, $b \in S^n$ be an instance of SMP(S). If $b \in \langle a_1, \ldots, a_k \rangle$, then there is a term function f such that $f(a_1, \ldots, a_k) = b$. By Lemma 3.3 there is a word g which induces f and whose length is polynomial in k. Now g witnesses the positive answer. □

For the following lemma note that the all-0 matrix has one block. We may assume that the first m positions of the input tuple b of Algorithm 1 are the nonzero ones.

Lemma 3.5. *Let S_P be a finite combinatorial Rees matrix semigroup such that $P \in \{0,1\}^{\Lambda \times I}$ has one block. Then Algorithm 1 decides* SMP(S_P) *in polynomial time.*

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

Algorithm 1 Decides SMP(S_P) in polynomial time if P has one block.

Input: $A \subseteq {S_P}^n$, $b \in {S_P}^n$,
$m \in \{0, \dots, n\}$ such that $b(i) \neq 0$ if and only if $i \in [m]$,
$J \subseteq I$, $\Delta \subseteq \Lambda$ such that $P(\lambda, i) = 1$ if and only if $(\lambda, i) \in \Delta \times J$ for $i \in I$, $\lambda \in \Lambda$.
Output: true if $b \in \langle A \rangle$, false otherwise.

1: **if** $b \in A$ **then**
2: **return** true
3: **end if**
4: $d := \prod\{a \in A \mid a([m]) \subseteq J \times \Delta\}$ (some order)
5: **return** $\exists a_1, a_2 \in A \colon a_1 d a_2 = b$

Proof. *Correctness of Algorithm 1.* Fix $A \subseteq {S_P}^n$, $b \in {S_P}^n$. If Algorithm 1 returns true, then clearly $b \in \langle A \rangle$. Conversely assume $b \in \langle A \rangle$. We show that true is returned. Let $g_1, \dots, g_k \in A$ such that $b = g_1 \cdots g_k$. If $k = 1$ then true is returned in line 2. Assume $k \geq 2$. We have

$$\begin{gathered} g_1(i) \in I \times \Delta, \quad g_k(i) \in J \times \Lambda, \text{ and} \\ g_2(i), \dots, g_{k-1}(i) \in J \times \Delta \text{ for all } i \in [m]; \end{gathered} \tag{3.3}$$

otherwise we obtain the contradiction $g_1 \cdots g_k(i) = 0$ for some $i \in [m]$. Let d have a value assigned by line 4. We claim that

$$g_1 d g_k = b. \tag{3.4}$$

For $i \in [m]$ we have $d(i) \in J \times \Delta$. The multiplication rule and (3.3) imply

$$b(i) = g_1 \cdots g_k(i) = g_1 d g_k(i).$$

Now let $i \in \{m+1, \dots, n\}$. Since $b(i) = 0$, there are three cases: $g_1(i) \notin I \times \Delta$, $g_k(i) \notin J \times \Lambda$, or $g_j(i) \notin J \times \Delta$ for some $j \in \{2, \dots, k-1\}$. In the first two cases $g_1 d g_k(i) = 0 = b(i)$ holds. In the third case $a := g_j$ occurs as a factor in line 4. Thus $d(i) \notin J \times \Delta$, and hence $g_1 d g_k(i) = 0$. This proves (3.4). So the algorithm returns true in line 5.

Complexity of Algorithm 1. The product in line 4 can be computed in $O(|A|n)$ time. Checking the condition in line 5 requires $O(|A|^2 n)$ time. Altogether Algorithm 1 runs in $O(|A|^2 n)$ time. □

Now we prove Theorem 1.2 and Corollary 1.3.

Proof of Theorem 1.2. Assume $P \in \{0,1\}^{\Lambda \times I}$. If P has one block, then SMP(S_P) is in P by Lemma 3.5. Assume P does not have one block. Then there are $i, j \in I$ and $\lambda, \mu \in \Lambda$ such that

$$P(\lambda, i) = P(\mu, j) = 1 \quad \text{and} \quad P(\mu, i) = 0.$$

Let $r := [i, \lambda]$, $s := [i, \mu]$, and $t := [j, \mu]$. Then $rs = st = s$, and s does not generate a group. By Theorem 1.1 SMP(S_P) is NP-hard. NP-easiness follows from Lemma 3.4. □

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

Proof of Corollary 1.3. The result is immediate from Theorem 1.2. □

Next we restate the Rees theorem (see [4, Theorem 3.2.3]) for the case of finite combinatorial 0-simple semigroups.

Theorem 3.6 (Rees theorem). *Let P be a finite* 0-1 *matrix such that each row and each column has at least one 1. Then S_P is a finite combinatorial* 0*-simple semigroup.*

Conversely, every finite combinatorial 0*-simple semigroup is isomorphic to one constructed in this way.*

Proof. See [4]. □

A semigroup S is said to have no *zero divisors* if for $s, t \in S$, $st = 0$ implies that $s = 0$ or $t = 0$.

Lemma 3.7. *Let S_P be a finite combinatorial* 0*-simple semigroup. Then the matrix P has one block if and only if S_P has no zero divisors.*

Proof. Assume $P \in \{0, 1\}^{\Lambda \times I}$. If P has one block, then all entries of P are 1. Thus S_P has no zero divisors. If P does not have one block, then $P(\lambda, i) = 0$ for some $\lambda \in \Lambda$, $i \in I$. Now $[i, \lambda]$ is a zero divisor since $[i, \lambda]^2 = 0$. □

Corollary 3.8. *If a finite combinatorial* 0*-simple semigroup S has no zero divisors, then* SMP(S) *is in* P. *Otherwise* SMP(S) *is* NP*-complete.*

Proof. The result is immediate from Theorem 1.2 and Lemma 3.7. □

4. Semigroups with PSPACE-complete SMP

There is an upper bound on the complexity of the SMP for semigroups.

Theorem 4.1 [1, Theorem 2.1]. *The* SMP *for a finite semigroup is in* PSPACE.

In [1] it has been shown that the SMP for T_3, the full transformation semigroup on three letters, is PSPACE-complete by reducing Kozen's function composition problem [6] to SMP(T_3). We adapt this proof to show that under the following conditions the SMP for a semigroup is PSPACE-complete.

Lemma 4.2. *Let S be a finite semigroup and $s, t, u \in S$ such that:*

(a) $sts = s$, $tst = t$;
(b) $s^2, t^2 <_{\mathcal{J}} s$;
(c) $su = s$ *and* $tu = t$.

Then SMP(S) *is* PSPACE*-complete.*

Proof. Kozen [6] showed that the following decision problem is PSPACE-complete: given $n \geq 1$ and functions $f_1, \ldots, f_m, g : [n] \to [n]$, we have to decide whether g can be obtained by composing the f_i's. The input size for this problem is $(m + 1)n \log n$. We will assume that the identity function can be obtained even from an empty set of functions. This does not change the complexity of the problem.

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

We encode Kozen's composition problem into SMP(S). By (a) s, t, st, ts are in the same $\mathcal{J}$-class. Observe that $s \neq st$; otherwise $s^2 = sts = s$, which is impossible. By similar arguments we obtain that u, s, t, st, ts are distinct. Also note that st and ts are idempotent while s and t are not.

We rename the following elements:

$$0 := s, \quad 1 := st, \quad 0 \to 0 := ts, \quad 0 \to 1 := t, \quad 1 \to 0 := s.$$

We regard 0 and 1 as states and let $u, 0 \to 0, 0 \to 1, 1 \to 0$ act on these states by right multiplication. This yields the partial multiplication table

S	u	$0 \to 0$	$0 \to 1$	$1 \to 0$
0	0	0	1	bad
1	1	bad	bad	0

(4.1)

where *bad* means an element $<_{\mathcal{J}} 0$ (or equivalently, $<_{\mathcal{J}} 1$). Note that if $x, y \in S$ and x is bad, then xy is also bad by the definition of $<_{\mathcal{J}}$. We say a tuple is *bad* if it contains a bad element.

Let n and $f_1, \ldots, f_m, g$ be an input to Kozen's composition problem. We will encode it as SMP on $n^2 + mn + 1$ positions. For $i \in [n]$ and $h\colon [n] \to [n]$ we write i^h instead of $h(i)$. We encode h by a *mapping tuple* $m_h \in S^{n^2+mn+1}$ as follows:

$$m_h(x) := \begin{cases} 1 & \text{if } x \in \{1^h, n + 2^h, \ldots, (n-1)n + n^h\}, \\ 0 & \text{otherwise.} \end{cases}$$

Hence the first n positions encode the image of 1, the next n positions the image of 2, and so on. The final $mn + 1$ positions are used to distinguish mapping tuples from other tuples that we will define shortly.

We introduce the generators of the subalgebra of S^{n^2+mn+1} gradually. The first generator is the mapping tuple m_1 for the identity on $[n]$.

Next, for each f_i we add the *choice tuple* c_i defined as

$$c_i(x) := \begin{cases} u & \text{if } x \in [n^2], \\ 0 \to 1 & \text{if } x \in \{n^2 + (i-1)n + 1, \ldots, n^2 + (i-1)n + n\}, \\ 0 \to 0 & \text{otherwise.} \end{cases}$$

Multiplying the mapping tuple for some h on the right by the choice tuple for f_i corresponds to deciding that h will be composed with f_i.

Finally, for each f_i and $j, k \in [n]$ we add the *application tuple* a_{ijk} with the semantics

$$\text{apply } f_i \text{ on coordinate } j \text{ to } k,$$

that is, in a mapping tuple m_h with $h(j) = k$ the encoded k is replaced by $f_i(k)$. If $k \neq k^{f_i}$, then

$$a_{ijk}(x) := \begin{cases} 1 \to 0 & \text{if } x \in \{(j-1)n + k, n^2 + (i-1)n + j\}, \\ 0 \to 1 & \text{if } x = (j-1)n + k^{f_i}, \\ 0 \to 0 & \text{if } x = mn + 1, \\ u & \text{otherwise.} \end{cases}$$

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

If $k = k^{f_i}$, then

$$a_{ijk}(x) := \begin{cases} 1 \to 0 & \text{if } x = n^2 + (i-1)n + j, \\ 0 \to 0 & \text{if } x = mn + 1, \\ u & \text{otherwise.} \end{cases}$$

Multiplication by the application tuples computes the composition decided by the choice tuples. More precisely, for any $h\colon [n] \to [n]$ and f_i,

$$m_{hf_i} = m_h c_i a_{i1 1^h} \cdots a_{inn^h}. \tag{4.2}$$

We refer to positions $n^2 + 1, \ldots, n^2 + mn$ as the *middle mn positions*. Multiplying m_h by c_i turns the ith block of n positions among the middle mn positions of m_h to 1. The following multiplication with $a_{i1 1^h} \cdots a_{inn^h}$ resets these n positions to 0. At the same time, in the first n positions of $m_h c_i$ the 1 gets moved from position 1^h to $(1^h)^{f_i}$, in the next n positions the 1 gets moved from $n + 2^h$ to $n + (2^h)^{f_i}$, and so on. The last position remains 0. Hence we obtain the mapping tuple of hf_i, and (4.2) is proved.

It remains to choose an element which will be generated by all these tuples if and only if g is a composition of f_i's. This final element is the mapping tuple for g. We claim

$$g \in \langle f_1, \ldots, f_m \rangle \quad \text{if and only if } m_g \in \langle m_1, c_1, \ldots, c_m, a_{111}, \ldots, a_{mnn} \rangle. \tag{4.3}$$

The implication from left to right is immediate from our observation (4.2). For the converse we fix a product of generator tuples which yields m_g and show that it essentially follows the pattern from (4.2).

The last position of every mapping tuple is $0 = s$, whereas the last position of the choice and application tuples is $0 \to 0 = ts$. By (a) and (b) the only products of s and ts that are equal to s are those of the form $s \cdot ts \cdots ts$. This means in the product yielding m_g, the generator m_1 must occur at the beginning and nowhere else.

The second element from the left cannot be an application tuple as the $1 \to 0$ in one of the middle mn positions would turn the result bad by (4.1). Thus the only option is the choice tuple for some function f_i. Multiplying m_1 by c_i turns n positions (among the middle mn positions) of m_1 to 1.

The third element from the left cannot be a choice tuple: since n of the middle mn positions are 1's, a multiplication by another choice tuple would produce a bad result. So before any more choice tuples can occur in our product, all n 1's in the middle mn positions have to be reset to 0. This can only be achieved by multiplying with n application tuples of the form a_{ijk_j} for $j \in [n]$. Focusing on the first n^2 positions of $m_1 c_i$, we see that necessarily $k_j = j$ for all j. Hence the first $n + 2$ factors of our product are

$$m_1 c_i a_{i11} \cdots a_{inn} = m_{f_i}.$$

Note that the order of the application tuples does not matter.

Continuing this reasoning with the mapping tuple for f_i (instead of the identity), we see that the next $n + 1$ factors of our product are some c_j followed by n application

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

tuples $a_{j11^{f_i}}, \ldots, a_{jmn^{f_i}}$. Invoking (4.2) we then get the mapping tuple for $f_i f_j$. In the end we get a mapping tuple for g if and only if g can be obtained as a composition of the f_i's and the identity. This proves (4.3).

The number of tuples we input into SMP is $mn^2 + m + 2$, so the total size of the input is $O((mn^2 + m + 2)(n^2 + mn + 1))$, that is, polynomial with respect to the size of the input of the original problem. Thus Kozen's composition problem has a polynomial time reduction to SMP(S) and the latter is PSPACE-hard as well. Together with Theorem 4.1 this yields the result. □

Proof of Theorem 1.4. Let $s' := (s, tst)$, $t' := (tst, s)$, and $u' := (u, u)$ be elements of $S^2 := S \times S$. Clearly $s't's' = s'$ and $t's't' = t'$. Both s' and t' do not generate groups. By Lemma 2.1 $s'^2 <_{\mathcal{J}} s'$ and $t'^2 <_{\mathcal{J}} t'$. Since $t' \mathcal{J} s'$, we have $t'^2 <_{\mathcal{J}} s'$. Now s', t', u' fulfill the hypothesis of Lemma 4.2. Thus SMP(S^2) is PSPACE-complete. As SMP(S^2) reduces to SMP(S) and vice versa, the result follows. □

Now we are able to list several 'naturally occuring' semigroups (with semigroup signature) that have a PSPACE-complete SMP.

Corollary 4.3. *The* SMP *for the following semigroups is* PSPACE*-complete:*

(a) *the* Brandt monoid B_2^1 *and the monoid* A_2^1*;*
(b) *for* $n \geq 2$ *and a finite ring* R *with identity* $1 \neq 0$*, the semigroup of all* $n \times n$ *matrices over* R*;*
(c) *the full transformation semigroup* T_n *on* $n \geq 3$ *letters;*
(d) *the symmetric inverse semigroup* I_n *on* $n \geq 2$ *letters.*

Proof. We apply Theorem 1.4.

(a) For B_2^1 let $s := [1, 2]$ and $t := [2, 1]$. For A_2^1 let $s := [2, 2]$ and $t := [1, 1]$.

(b) Define $n \times n$ matrices s, t over R by

$$s_{ij} := \begin{cases} 1 & \text{if } (i, j) = (1, 2), \\ 0 & \text{otherwise,} \end{cases} \qquad t_{ij} := \begin{cases} 1 & \text{if } (i, j) = (2, 1), \\ 0 & \text{otherwise} \end{cases}$$

for $i, j \in [n]$. Let u be the identity matrix.

(c) Let u be the identity mapping on $[n]$, and $s, t \colon [n] \to [n]$,

$$s(x) := \begin{cases} 2 & \text{if } x = 1, \\ 3 & \text{otherwise,} \end{cases} \qquad t(x) := \begin{cases} 1 & \text{if } x = 2, \\ 3 & \text{otherwise.} \end{cases}$$

(d) Let u be the identity mapping, $s \colon 1 \mapsto 2$, and $t \colon 2 \mapsto 1$. □

In [9] Schützenberger introduced the pseudovariety DS which comprises all finite monoids each of whose regular $\mathcal{J}$-classes is a subsemigroup. Besides studying the structure of these monoids, he determined the languages recognized by various subpseudovarieties of DS. We can now generalize Corollary 2.3 for the case of monoids.

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

COROLLARY 4.4. *If a finite monoid is not in* DS*, then its* SMP *is* PSPACE*-complete.*

PROOF. Let S be a monoid which does not belong to DS. Then S has a $\mathcal{J}$-class which contains both group and nongroup $\mathcal{H}$-classes. Similar to the proof of Corollary 2.3, there is a $t \in S$ such that $sts = s$. Now s, t, and the identity fulfill the hypothesis of Theorem 1.4. □

5. Proof of Theorem 1.6

LEMMA 5.1. *If the* 0-1 *matrix P of a finite combinatorial Rees matrix semigroup S_P has one block, then* SMP(S_P^1) *is in* NP.

PROOF. Assume $P \in \{0,1\}^{\Lambda \times I}$, and let $J \subseteq I$ and $\Delta \subseteq \Lambda$ such that $P(\lambda, i) = 1$ if and only if $(\lambda, i) \in \Delta \times J$ for $i \in I$, $\lambda \in \Lambda$. Let $T := S_P^1$ and $A \subseteq T^n$, $b \in T^n$ be an instance of SMP(T) such that $b \in \langle A \rangle$. Let $a_1, \ldots, a_k \in A$ such that $b = a_1 \cdots a_k$. If $b = (1, \ldots, 1)$ or $k = 1$, then clearly $b \in A$. In this case the position of b in the list A is a witness. Assume $b \neq (1, \ldots, 1)$ and $k \geq 2$.

We claim that for $i \in [n]$ with $b(i) = 0$ there are $\ell_i, r_i \in [k]$, $\ell_i < r_i$ such that

$$a_{\ell_i} a_{r_i}(i) = 0 \quad \text{and} \quad a_{\ell_i+1}(i) = \ldots = a_{r_i-1}(i) = 1. \tag{5.1}$$

This follows from Lemma 3.1(a). For $i \in [n]$ with $b(i) \in I \times \Lambda$ let

$$\ell_i := \min\{j \in [k] \mid a_j(i) \neq 1\},$$
$$r_i := \max\{j \in [k] \mid a_j(i) \neq 1\}.$$

Now define an index set $N \subseteq [k]$ by

$$N := \{\ell_i \mid i \in [n],\ b(i) \neq 1\} \cup \{r_i \mid i \in [n],\ b(i) \neq 1\}.$$

Note that $N \neq \emptyset$; otherwise $b = (1, \ldots, 1)$ which contradicts our assumption.

For $i \in [n]$ we claim that

$$\prod_{j \in N} a_j(i) = b(i), \tag{5.2}$$

where the indexes j of the factors are in ascending order. If $b(i) = 1$, then $a_j(i) = 1$ for all $j \in [k]$, and (5.2) follows. Assume $b(i) = 0$. We have $\ell_i, r_i \in N$. By (5.1) all factors in (5.2) between $a_{\ell_i}(i)$ and $a_{r_i}(i)$ are equal to 1. This and (5.1) imply (5.2). Finally assume $b(i) \in I \times \Lambda$. For $\ell_i < j < r_i$ we have $a_j(i) \in \{1\} \cup (J \times \Delta)$; otherwise we obtain the contradiction $b(i) = 0$. Thus

$$\prod_{\substack{j \in N \\ \ell_i \leq j \leq r_i}} a_j(i) = \prod_{\ell_i \leq j \leq r_i} a_j(i).$$

Since $a_j(i) = 1$ for $j < \ell_i$ and $j > r_i$, (5.2) follows.

The length of the product in (5.2) is $|N|$ and thus at most $2n$. Thus this product is a valid witness for $b \in \langle A \rangle$, and the lemma is proved. □

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

Proof of Theorem 1.6. Assume $P \in \{0,1\}^{\Lambda \times I}$.

(a) If P is the all-1 matrix, then S_P^1 is a band (idempotent semigroup) with $\mathcal{J}$-classes $\{0\}$, $I \times \Lambda$, and $\{1\}$. We show that S_P^1 is a *regular band*, that is, S_P^1 satisfies the identity

$$xyxzx \approx xyzx. \tag{5.3}$$

Let $x, y, z \in S_P^1$. If one of the variables is 0 or 1, then (5.3) clearly holds. If $x, y, z \in I \times \Lambda$, then $xyxzx = x = xyzx$ by the definition of the multiplication. Thus S_P^1 is a regular band. By [11, Corollary 1.7] the SMP for every regular band is in P.

(b) Assume P has one block and some entries are 0. Let $i \in I$ and $\lambda \in \Lambda$ such that $P(\lambda, i) = 0$. Let $s := [i, \lambda]$ and $r := t := 1$. Since s does not generate a group, SMP(S_P^1) is NP-hard by Theorem 1.1. NP-easiness follows from Lemma 5.1.

(c) In this case P does not have one block. Thus there are $i, j \in I$ and $\lambda, \mu \in \Lambda$ such that

$$P(\lambda, i) = P(\mu, j) = 1 \quad \text{and} \quad P(\lambda, j) = 0.$$

Let $s := [j, \lambda]$ and $t := [i, \mu]$. Then s does not generate a group, $sts = s$, $s1 = s$, and $t1 = t$. By Theorem 1.4 SMP(S) is PSPACE-complete. □

References

[1] A. Bulatov, M. Kozik, P. Mayr and M. Steindl, 'The subpower membership problem for semigroups', *Internat. J. Algebra Comput.* **26**(07) (2016), 1435–1451.

[2] A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups.* Vol. I, Mathematical Surveys, 7 (American Mathematical Society, Providence, RI, 1961).

[3] S. A. Cook., 'Characterizations of pushdown machines in terms of time-bounded computers', *J. Assoc. Comput. Mach.* **18** (1971), 4–18.

[4] J. M. Howie, *Fundamentals of Semigroup Theory*, London Mathematical Society Monographs. New Series, 12 (The Clarendon Press, Oxford University Press, New York, Oxford Science Publications, 1995).

[5] P. Idziak, P. Marković, R. McKenzie, M. Valeriote and R. Willard, 'Tractability and learnability arising from algebras with few subpowers', *SIAM J. Comput.* **39**(7) (2010), 3023–3037.

[6] D. Kozen, 'Complexity of finitely presented algebras', in: *Conference Record of the Ninth Annual ACM Symposium on Theory of Computing (Boulder, CO, 1977)* (Association for Computing Machinery, 1977), 164–177.

[7] M. Kozik., 'A finite set of functions with an EXPTIME-complete composition problem', *Theoret. Comput. Sci.* **407**(1–3) (2008), 330–341.

[8] P. Mayr, 'The subpower membership problem for Mal'cev algebras', *Internat. J. Algebra Comput.* **22**(7) (2012), 1250075, 23.

[9] M. P. Schützenberger, 'Sur le produit de concaténation non ambigu', *Semigroup Forum* **13**(1) (1976/77), 47–75.

[10] S. Seif and C. Szabó, 'Computational complexity of checking identities in 0-simple semigroups and matrix semigroups over finite fields', *Semigroup Forum* **72**(2) (2006), 207–222.

[11] M. Steindl, 'The subpower membership problem for bands', *J. Algebra* **489**(Supplement C) (2017), 529–551.

[12] R. Willard, 'Four unsolved problems in congruence permutable varieties'. *Talk at International Conference on Order, Algebra, and Logics, Vanderbilt University, Nashville, June 12–16, 2007.*

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press

MARKUS STEINDL, Institute for Algebra, Johannes Kepler University Linz,
Altenberger St 69, 4040 Linz, Austria
and
Department of Mathematics, University of Colorado Boulder,
Campus Box 395, Boulder, CO 80309-0395, USA
e-mail: markus.steindl@colorado.edu

https://doi.org/10.1017/S1446788718000010 Published online by Cambridge University Press