On the Complexity of the Cayley Semigroup Membership Problem

Lukas Fleischer[1]
FMI, University of Stuttgart
Universitätsstraße 38, 70569 Stuttgart, Germany
fleischer@fmi.uni-stuttgart.de

Abstract

We investigate the complexity of deciding, given a multiplication table representing a semigroup S, a subset X of S and an element t of S, whether t can be expressed as a product of elements of X. It is well-known that this problem is NL-complete and that the more general *Cayley groupoid membership problem*, where the multiplication table is not required to be associative, is P-complete. For groups, the problem can be solved in deterministic log-space which raised the question of determining the exact complexity of this variant. Barrington, Kadau, Lange and McKenzie showed that for Abelian groups and for certain solvable groups, the problem is contained in the complexity class FOLL and they concluded that these variants are not hard for any complexity class containing Parity. The more general case of arbitrary groups remained open. In this work, we show that for both groups and for commutative semigroups, the problem is solvable in qAC^0 (quasi-polynomial size circuits of constant depth with unbounded fan-in) and conclude that these variants are also not hard for any class containing Parity. Moreover, we prove that NL-completeness already holds for the classes of 0-simple semigroups and nilpotent semigroups. Together with our results on groups and commutative semigroups, we prove the existence of a natural class of finite semigroups which generates a variety of finite semigroups with NL-complete Cayley semigroup membership, while the Cayley semigroup membership problem for the class itself is not NL-hard. We also discuss applications of our technique to FOLL.

2012 ACM Subject Classification Theory of computation → Problems, reductions and completeness, Theory of computation → Circuit complexity

Keywords and phrases subsemigroup, multiplication table, generators, completeness, quasi-polynomial-size circuits, FOLL

Digital Object Identifier 10.4230/LIPIcs.CCC.2018.25

Acknowledgements I would like to thank Armin Weiß for several interesting and inspiring discussions, and for pointing out that qAC^0 is not contained within P/poly. I would also like to thank Samuel Schlesinger for comments which led to an improved presentation of the proof of Proposition 3 and for pointing out that results on the average sensitivity of bounded-depth circuits can be used to show that FOLL is not contained within qAC^0. Moreover, I am grateful to the anonymous referees for providing helpful comments that improved the paper.

1 Introduction

The *Cayley groupoid membership problem* (sometimes also called the *generation problem*) asks, given a multiplication table representing a groupoid G, a subset X of G and an element t of G, whether t can be expressed as a product of elements of X. In 1976, Jones and Laaser

[1] This work was supported by the DFG grant DI 435/5–2.

33rd Computational Complexity Conference (CCC 2018).
Editor: Rocco A. Servedio; Article No. 25; pp. 25:1–25:12
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

showed that this problem is P-complete [20]. Barrington and McKenzie later studied natural subproblems and connected them to standard subclasses of P [10].

When restricting the set of valid inputs to inputs with an associative multiplication table, the problem becomes NL-complete [21]. We will call this variant of the problem the *Cayley semigroup membership problem* and analyze its complexity when further restricting the semigroups encoded by the input. For a class of finite semigroups $\mathbf{V}$, the *Cayley semigroup membership problem for* $\mathbf{V}$ is formally defined as follows.

CSM($\mathbf{V}$)	
Input:	The Cayley table of a semigroup $S \in \mathbf{V}$, a set $X \subseteq S$ and an element $t \in S$
Question:	Is t in the subsemigroup of S generated by X?

The motivation for investigating this problem is two-fold. Firstly, there is a direct connection between the Cayley semigroup membership problem and decision problems for regular languages: a language $L \subseteq \Sigma^+$ is regular if and only if there exist a finite semigroup S, a morphism $\varphi\colon \Sigma^+ \to S$ and a set $P \subseteq S$ such that $L = \varphi^{-1}(P)$. Thus, morphisms to finite semigroups can be seen as a way of encoding regular languages. For encoding such a semigroup, specifying the multiplication table is a natural choice. Deciding emptiness of a regular language represented by a morphism $\varphi\colon \Sigma^+ \to S$ to a finite semigroup S and a set $P \subseteq S$ boils down to checking whether any of the elements from the set P is contained in the subsemigroup of S generated by the images of the letters of Σ under φ. Conversely, the Cayley semigroup membership problem is a special case of the emptiness problem for regular languages: an element $t \in S$ is contained in the subsemigroup generated by a set $X \subseteq S$ if and only if the language $\varphi^{-1}(P)$ with $\varphi\colon X^+ \to S, x \mapsto x$ and $P = \{t\}$ is non-empty.

Secondly, we hope to get a better understanding of the connection between algebra and low-level complexity classes included in NL in a fashion similar to the results of [10]. In the past, several intriguing links between so-called *varieties of finite semigroups* and the computational complexity of algebraic problems for such varieties were made. For example, the fixed membership problem for a regular language was shown to be in AC^0 if its syntactic monoid is aperiodic, in ACC^0 if the syntactic monoid is solvable and NC^1-complete otherwise [8, 11]. It is remarkable that in most results of this type, both the involved complexity classes and the algebraic varieties are natural. On a language-theoretical level, varieties of finite semigroups correspond to subclasses of the regular languages closed under Boolean operations, quotients and inverse morphisms.

Related Work. We already mentioned the work of Jones and Laaser on the Cayley groupoid membership problem [20], the work of Jones, Lien and Laaser on the Cayley semigroup membership problem [21] and the work of Barrington and McKenzie on subproblems thereof [10]. The semigroup membership problem and its restrictions to varieties of finite semigroups was also studied for other encodings of the input, such as matrix semigroups [2, 4, 7] or transformation semigroups [5, 6, 12, 13, 14, 15, 18].

The group version of the Cayley semigroup membership problem (CSM($\mathbf{G}$), using our notation) was first investigated by Barrington and McKenzie in 1991 [10]. They observed that the problem is in symmetric log-space, which has been shown to be the same as deterministic log-space by Reingold in 2008 [23], and suggested it might be complete for deterministic log-space. However, all attempts to obtain a hardness proof failed (in fact, their conjecture is shown to be false in this work). There was no progress in a long time until Barrington, Kadau, Lange and McKenzie showed that for Abelian groups and certain solvable groups, the problem lies in the complexity class FOLL and thus, cannot be hard for any complexity class containing Parity in 2001 [9]. The case of arbitrary groups remained open.

Our Contributions. We generalize previous results on Abelian groups to arbitrary commutative semigroups. Then, using novel techniques, we show that the Cayley semigroup membership problem for the variety of finite groups **G** is contained in qAC^0 and thus, cannot be hard for any class containing Parity. Our approach relies on the existence of succinct representations of group elements by algebraic circuits. More precisely, it uses the fact that every element of a group G can be computed by an algebraic circuit of size $\mathcal{O}(\log^3 |G|)$ over any set of generators. Since in the Cayley semigroup membership problem, the algebraic structure is not fixed, we introduce so-called Cayley circuits, which are similar to regular algebraic circuits but expect the finite semigroup to be given as part of the input. We prove that these Cayley circuits can be simulated by sufficiently small unbounded fan-in Boolean circuits. We then use this kind of simulation to evaluate all Cayley circuits, up to a certain size, in parallel.

By means of a closer analysis and an extension of the technique used by Jones, Lien and Laaser in [21], we also show that the Cayley semigroup membership problem remains NL-complete when restricting the input to 0-simple semigroups or to nilpotent semigroups.

Combining our results, we obtain that the Cayley semigroup membership problem for the class $\mathbf{G} \cup \mathbf{Com}$, which consists of all finite groups and all finite commutative semigroups, is decidable in qAC^0 (and thus not NL-hard) while the Cayley semigroup membership problem for the minimal variety of finite semigroups containing $\mathbf{G} \cup \mathbf{Com}$ is NL-complete.

Finally, we discuss the extent to which our approach can be used to establish membership of Cayley semigroup membership variants to the complexity class FOLL. Here, instead of simulating all circuits in parallel, we use an idea based on repeated squaring. This technique generalizes some of the main concepts used in [9].

2 Preliminaries

Algebra. A semigroup T is a *subsemigroup* of S if T is a subset of S closed under multiplication. The *direct product* of two semigroups S and T is the Cartesian product $S \times T$ equipped with componentwise multiplication. A subsemigroup of a direct product is also called *subdirect product*. A semigroup T is a *quotient* of a semigroup S if there exists a surjective morphism $\varphi\colon S \to T$.

A *variety of finite semigroups* is a class of finite semigroups which is closed under finite subdirect products and under quotients. Since we are only interested in finite semigroups, we will henceforth use the term *variety* for a variety of finite semigroups. Note that in the literature, such classes of semigroups are often called *pseudovarieties*, as opposed to Birkhoff varieties which are also closed under infinite subdirect products. The following varieties play an important role in this paper:

- **G**, the class of all finite groups,
- **Ab**, the class of all finite Abelian groups,
- **Com**, the class of all finite commutative semigroups,
- **N**, the class of all finite nilpotent semigroups, i.e., semigroups where the only idempotent is a zero element.

The *join* of two varieties **V** and **W**, denoted by $\mathbf{V} \vee \mathbf{W}$, is the smallest variety containing both **V** and **W**. A semigroup S is 0-*simple* if it contains a zero element 0 and if for each $s \in S \setminus \{0\}$, one has $SsS = S$. The class of finite 0-simple semigroups does not form a variety.

Complexity. We assume familiarity with standard definitions from circuit complexity. A function has *quasi-polynomial* growth if it is contained in $2^{\mathcal{O}(\log^c n)}$ for some fixed $c \in \mathbb{N}$.

Throughout the paper, we consider the following unbounded fan-in Boolean circuit families:

- AC^0, languages decidable by circuit families of depth $\mathcal{O}(1)$ and polynomial size,
- qAC^0, languages decidable by circuit families of depth $\mathcal{O}(1)$ and quasi-polynomial size,
- FOLL, languages decidable by circuit families of depth $\mathcal{O}(\log \log n)$ and polynomial size,
- AC^1, languages decidable by circuit families of depth $\mathcal{O}(\log n)$ and polynomial size,
- $\mathsf{P/poly}$, languages decidable by circuit families of polynomial size (and unbounded depth).

We allow NOT gates but do not count them when measuring the depth or the size of a circuit. We will also briefly refer to the complexity classes ACC^0, TC^0, NC^1, L and NL.

It is known that the Parity function cannot be computed by AC^0, FOLL or qAC^0 circuits. This follows directly from Håstad's and Yao's famous lower bound results [19, 24], which state that the number of Boolean gates required for a depth-d circuit to compute Parity is exponential in $n^{1/(d-1)}$.

3 Hardness Results

Before looking at parallel algorithms for the Cayley semigroup membership problem, we establish two new NL-hardness results. To this end, we first analyze the construction already used by Jones, Lien and Laaser [21]. It turns out that the semigroups used in their reductions are 0-simple which leads to the following result.

▶ **Theorem 1.** *For a class containing all* 0*-simple semigroups, the Cayley semigroup membership problem is* NL*-complete.*

Proof. To keep the proof self-contained, we briefly describe the reduction from the connectivity problem for directed graphs (henceforth called STConn) to the Cayley semigroup membership problem given in [21].

Let $G = (V, E)$ be a directed graph. We construct a semigroup on the set $S = V \times V \cup \{0\}$ where 0 is a zero element and the multiplication rule for the remaining elements is

$$(v, w) \cdot (x, y) = \begin{cases} (v, y) & \text{if } w = x, \\ 0 & \text{otherwise.} \end{cases}$$

By construction, the subsemigroup of S generated by $E \cup \{(v, v) \mid v \in V\}$ contains an element (s, t) if and only if t is reachable from s in G. To see that the semigroup S is 0-simple, note that for pairs of arbitrary elements $(v, w) \in V \times V$ and $(x, y) \in V \times V$, one has $(x, v)(v, w)(w, y) = (x, y)$, which implies $S(v, w)S = S$. ◀

In order to prove NL-completeness for another common class of semigroups, we need a slightly more advanced construction reminiscent of the "layer technique", which is usually used to show that STConn remains NL-complete when the inputs are acyclic graphs.

▶ **Theorem 2.** $\mathrm{CSM}(\mathbf{N})$ *is* NL*-complete (under* AC^0 *many-one reductions).*

Proof. Following the proof of Theorem 1, we describe an AC^0 reduction of STConn to $\mathrm{CSM}(\mathbf{N})$.

Let $G = (V, E)$ be a directed graph with n vertices. We construct a semigroup on the set $S = V \times \{1, \dots, n-1\} \times V \cup \{0\}$ where 0 is a zero element and the multiplication rule for the remaining elements is

$$(v, i, w) \cdot (x, j, y) = \begin{cases} (v, i + j, y) & \text{if } w = x \text{ and } i + j < n, \\ 0 & \text{otherwise.} \end{cases}$$

The subsemigroup of S generated by $\{(v, 1, w) \mid v = w \text{ or } (v, w) \in E\}$ contains an element $(s, n-1, t)$ if and only if t is reachable (in less than n steps) from s in G. Clearly, the zero element is the only idempotent in S, so S is nilpotent. Also, it is readily verified that the reduction can be performed by an AC^0 circuit family. ◀

4 Parallel Algorithms for Cayley Semigroup Membership

Algebraic circuits can be used as a succinct representation of elements in an algebraic structure. This idea will be the basis of the proof that CSM($\mathbf{G}$) is in qAC^0. Unlike in usual algebraic circuits, in the context of the Cayley semigroup membership problem, the algebraic structure is not fixed but given as part of the input. We will introduce so-called Cayley circuits to deal with this setting. Since these circuits will be used for the Cayley semigroup membership problem only, we confine ourselves to cases where the algebraic structure is a finite semigroup.

4.1 Cayley Circuits

A *Cayley circuit* is a directed acyclic graph with topologically ordered vertices such that each vertex has in-degree 0 or 2. In the following, to avoid technical subtleties when squaring an element, we allow multi-edges. The vertices of a Cayley circuit are called *gates*. The vertices with in-degree 0 are called *input gates* and vertices with in-degree 2 are called *product gates*. Each Cayley circuit also has a designated gate of out-degree 0, called the *output gate*. For simplicity, we assume that the output gate always corresponds to the maximal gate with regard to the vertex order. The *size* of a Cayley circuit $\mathcal{C}$, denoted by $|\mathcal{C}|$, is the number of gates of $\mathcal{C}$. An *input* to a Cayley circuit $\mathcal{C}$ with k input gates consists of a finite semigroup S and elements $x_1, \dots, x_k$ of S. Given such an input, the *value* of the i-th input gate is x_i and the value of a product gate, whose predecessors have values x and y, is the product $x \cdot y$ in S. The *value of the circuit* $\mathcal{C}$ is the value of its output gate. We will denote the value of $\mathcal{C}$ under a finite semigroup S and elements $x_1, \dots, x_k \in S$ by $\mathcal{C}(S, x_1, \dots, x_k)$.

A Cayley circuit can be seen as a circuit in the usual sense: the finite semigroup S and the input gate values are given as part of the input and the functions computed by product gates map a tuple, consisting of semigroup S and two elements of S, to another element of S. We say that a Cayley circuit with k input gates can be *simulated* by a family of unbounded fan-in Boolean circuits $(\mathcal{C}_n)_{n \in \mathbb{N}}$ if, given the encodings of a finite semigroup S and of elements $x_1, \dots, x_k$ of S of total length n, the circuit $\mathcal{C}_n$ computes the encoding of $\mathcal{C}(S, x_1, \dots, x_k)$. For a semigroup S with N elements, we assume that the elements of S are encoded by the integers $\{0, \dots, N-1\}$ such that the encoding of a single element uses $\lceil \log N \rceil$ bits. The semigroup itself is given as a multiplication table with N^2 entries of $\lceil \log N \rceil$ bits each.

▶ **Proposition 3.** *Let $\mathcal{C}$ be a Cayley circuit of size m. Then, $\mathcal{C}$ can be simulated by a family of unbounded fan-in constant depth Boolean circuits $(\mathcal{C}_n)_{n \in \mathbb{N}}$ of size at most n^m.*

Proof. Let $\mathcal{C}$ be a Cayley circuit with k input gates and $m-k$ product gates. We want to construct a Boolean circuit which can be used for all finite semigroups S with a fixed number of elements N. The input to such a circuit consists of $n = (N^2 + k) \lceil \log N \rceil$ bits.

For a fixed vector $(y_1, \dots, y_m) \in S^m$, one can check using a single AND gate (and additional NOT gates at some of the incoming wires) whether $(y_1, \dots, y_m)$ corresponds to the sequence of values occurring at the gates of $\mathcal{C}$ under the given inputs. To this end, for each gate $i \in \{1, \dots, m\}$ of $\mathcal{C}$, we add $\lceil \log N \rceil$ incoming wires to this AND gate: if the i-th gate of $\mathcal{C}$ is an input gate, we feed the bits of the corresponding input value into the AND gate, complementing the j-th bit if the j-th bit of y_i is zero. If the i-th gate is a product gate and has incoming wires from gates ℓ and r, we connect the entry (y_ℓ, y_r) of the multiplication table to the AND gate, again complementing bits corresponding to 0-bits of y_i.

To obtain a Boolean circuit simulating $\mathcal{C}$, we put such AND gates for all vectors of the form $(y_1, \dots, y_m) \in S^m$ in parallel. In a second layer, we create $\lceil \log N \rceil$ OR gates and connect the AND gate for a vector $(y_1, \dots, y_m)$ to the j-th OR gate if and only if the j-th bit of y_m is one. The idea is that exactly one of the AND gates — the gate corresponding to the vector of correct guesses of the gate values of $\mathcal{C}$ — evaluates to 1 and the corresponding output value y_m then occurs as output value of the OR gates.

This circuit has depth 2 and size $N^m + \lceil \log N \rceil \leqslant n^m$. ◀

4.2 The Poly-Logarithmic Circuits Property

When analyzing the complexity of CSM(**Ab**), Barrington et al. introduced the so-called *logarithmic power basis property.* A class of semigroups has the logarithmic power basis property if any set of generators X for a semigroup S of cardinality N from the family has the property that every element of S can be written as a product of at most $\log(N)$ many powers of elements of X. In [9], it was shown that the class of Abelian groups has the logarithmic power basis property. Using a different technique, this result can easily be extended to arbitrary commutative semigroups.

▶ **Lemma 4.** *The variety* **Com** *has the logarithmic power basis property.*

Proof. Suppose that S is a commutative semigroup of size N and let X be a set of generators for S. Let $y \in S$ be an arbitrary element. We choose $k \in \mathbb{N}$ to be the smallest value such that there exist elements $x_1, \dots, x_k \in X$ and integers $i_1, \dots, i_k \in \mathbb{N}$ with $y = x_1^{i_1} \cdots x_k^{i_k}$. Assume, for the sake of contradiction, that $k > \log(N)$.

The power set $\mathcal{P}(\{1, \dots, k\})$ forms a semigroup when equipped with set union as binary operation. Consider the morphism $h \colon \mathcal{P}(\{1, \dots, k\}) \to S$ defined by $h(\{j\}) = x_j^{i_j}$ for all $j \in \{1, \dots, k\}$. This morphism is well-defined because S is commutative.

Since $|\mathcal{P}(\{1, \dots, k\})| = 2^k > 2^{\log(N)} = |S|$, we know by the pigeon hole principle that there exist two sets $K_1, K_2 \subseteq \{1, \dots, k\}$ with $K_1 \neq K_2$ and $h(K_1) = h(K_2)$. We may assume, without loss of generality, that there exists some $j \in K_1 \setminus K_2$. Now, because

$$y = h(\{1, \dots, k\}) = h(K_1)h(\{1, \dots, k\} \setminus K_1) = h(K_2)h(\{1, \dots, k\} \setminus K_1)$$

and since neither K_2 nor $\{1, \dots, k\} \setminus K_1$ contain j, we know that y can be written as a product of powers of elements x_i with $1 \leqslant i \leqslant k$ and $i \neq j$, contradicting the choice of k. ◀

For the analysis of arbitrary groups, we introduce a more general concept. It is based on the idea that algebraic circuits (Cayley circuits with fixed inputs) can be used for succinct representations of semigroup elements.

▶ **Example 5.** Let $e \in \mathbb{N}$ be a positive integer. Then, one can construct a Cayley circuit of size at most $2 \lceil \log e \rceil$ which computes, given a finite semigroup S and an element $x \in S$ as input, the power x^e in S. If $e = 1$, the circuit only consists of the input gate. If e is even, the circuit is obtained by taking the circuit for $e/2$, adding a product gate and creating two edges from the output gate of the circuit for $e/2$ to the new gate. If e is odd, the circuit is obtained by taking the circuit for $e - 1$ and connecting it to a new product gate. In this case, the second incoming edge for the new gate comes from the input gate.

A class of semigroups has the *poly-logarithmic circuits property* if there exists a constant $c \in \mathbb{N}$ such that for each semigroup S of cardinality N from the class, for each subset X of S and for each y in the subsemigroup generated by X, there exists a Cayley circuit $\mathcal{C}$ of size $\log^c(N)$ with k input gates and there exist $x_1, \dots, x_k \in X$ such that $\mathcal{C}(S, x_1, \dots, x_k) = y$.

▶ **Proposition 6.** *Let* $\mathbf{V}$ *be a family of semigroups which is closed under subsemigroups and has the logarithmic power basis property. Then* $\mathbf{V}$ *has the poly-logarithmic circuits property.*

Proof. Let X be a subset of a semigroup S of cardinality N. Let y be in the subsemigroup generated by X. Then, we have $y = x_1^{i_1} \cdots x_k^{i_k}$ for some $x_1, \dots, x_k \in X$ with $k \leqslant \log(N)$ and $i_1, \dots, i_k \in \mathbb{N}$. By the pigeon hole principle, we may assume without loss of generality that $1 \leqslant i_1, \dots, i_k \leqslant N$. Using the method from Example 5, one can construct Cayley circuits $\mathcal{C}_1, \dots, \mathcal{C}_k$ of size at most $2 \lceil \log N \rceil$ such that $\mathcal{C}_j(S, x) = x^{i_j}$ for all $j \in \{1, \dots, k\}$ and $x \in S$. Using $k - 1$ additional product gates, these circuits can be combined to a single circuit $\mathcal{C}$ with $\mathcal{C}(S, x_1, \dots, x_k) = x_1^{i_1} \cdots x_k^{i_k} = y$.

In total, the resulting circuit consists of $k \cdot 2 \lceil \log N \rceil + k - 1 < 5 \log^2(N)$ gates. ◀

Let G be a finite group and let X be a subset of G. A sequence $(g_1, \dots, g_\ell)$ of elements of G is a *straight-line program over* X if for each $i \in \{1, \dots, \ell\}$, we have $g_i \in X$ or $g_i = g_p^{-1}$ or $g_i = g_p g_q$ for some $p, q < i$. The number ℓ is the *length* of the straight-line program and the elements of the sequence are said to be *generated* by the straight-line program. The following result by Babai and Szemerédi [7] is commonly known as *Reachability Lemma.*

▶ **Lemma 7** (Reachability Lemma)**.** *Let* G *be a finite group and let* X *be a set of generators of* G*. Then, for each element* $t \in G$*, there exists a straight-line program over* X *generating* t *which has length at most* $(\log |G| + 1)^2$.

The proof of this lemma is based on a technique called "cube doubling". For details, we refer to [3]. It is now easy to see that groups admit poly-logarithmic circuits.

▶ **Lemma 8.** *The variety* $\mathbf{G}$ *has the poly-logarithmic circuits property.*

Proof. Let G be a group of order N, let X be a subset of G and let y be an element in the subgroup of G generated by X. By Lemma 7, we know that there exists a straight-line program $(g_1, \dots, g_\ell)$ over X with $\ell \leqslant (\log(N) + 1)^2$ and $g_\ell = y$. We may assume that the elements $g_1, \dots, g_\ell$ are pairwise distinct. It suffices to describe how to convert this straight-line program into a Cayley circuit $\mathcal{C}$ and values $x_1, \dots, x_k \in X$ such that $\mathcal{C}(S, x_1, \dots, x_k) = y$.

We start with an empty circuit and with $k = 0$ and process the elements of the straight-line program left to right. For each element g_i, we add gates to the circuit. The output gate of the circuit obtained after processing the element g_i will be called the *g_i-gate.*

If the current element g_i is contained in X, we increment k, add a new input gate to the circuit and let $x_k = g_i$. If the current element g_i can be written as a product $g_p g_q$ with $p, q < i$, we add a new product gate to the circuit and connect the g_p-gate as well as the g_q-gate to this new gate. If the current element g_i is an inverse g_p^{-1} with $p < i$, we take a circuit $\mathcal{C}'$ with $2 \lceil \log N \rceil$ gates and with $\mathcal{C}'(G, x) = x^{N-1}$ for all $x \in S$. Such a circuit can be built by using the powering technique illustrated in Example 5. We add $\mathcal{C}'$ to $\mathcal{C}$, replacing its input gate by an edge coming from the g_p-gate.

The resulting circuit has size at most $(\log(N) + 1)^2 \cdot 2 \lceil \log N \rceil \leqslant 2(\log(N) + 1)^3$. ◀

We will now show that for classes of semigroups with the poly-logarithmic circuits property, one can solve the Cayley semigroup membership problem in qAC^0.

▶ **Theorem 9.** *Let* $\mathbf{V}$ *be a class of semigroups with the poly-logarithmic circuits property. Then* $\mathrm{CSM}(\mathbf{V})$ *is in* qAC^0*.*

Proof. We construct a family of unbounded fan-in constant-depth Boolean circuits with quasi-polynomial size, deciding, given the multiplication table of a semigroup $S \in \mathbf{V}$, a set $X \subseteq S$ and an element $t \in S$ as inputs, whether t is in the subsemigroup generated by X.

Since $\mathbf{V}$ has the poly-logarithmic circuits property, we know that, for some constant $c \in \mathbb{N}$, the element t is in the subsemigroup generated by X if and only if there exist a Cayley circuit $\mathcal{C}$ of size $\log^c(n)$ and inputs $x_1, \dots, x_k \in X$ such that $\mathcal{C}(S, x_1, \dots, x_k) = t$. There are at most $(\log^c(n) \cdot \log^c(n))^{\log^c(n)} = 2^{\log^c(n)\log(2c\log n)}$ different Cayley circuits of this size. Let us consider one of these Cayley circuits $\mathcal{C}$. Suppose that $\mathcal{C}$ has k input gates. By Proposition 3, there exists a unbounded fan-in constant-depth Boolean circuit of size $n^{\log^c n} = 2^{\log^{c+1} n}$ deciding on input S and elements $x_1, \dots, x_k \in S$ whether $\mathcal{C}(S, x_1, \dots, x_k) = t$. There are at most $n^k \leqslant n^{\log^c n} = 2^{\log^{c+1} n}$ possibilities of connecting (not necessarily all) input gates corresponding to the elements of X to this simulation circuit.

Thus, we can check for all Cayley circuits of the given size and all possible input assignments in parallel, whether the value of the corresponding circuit is t, and feed the results of all these checks into a single OR gate to obtain a quasi-polynomial-size Boolean circuit. ◀

In conjunction with Lemma 4 and Lemma 8, we immediately obtain the following corollary.

▶ **Corollary 10.** *Both* $\mathrm{CSM}(\mathbf{G})$ *and* $\mathrm{CSM}(\mathbf{Com})$ *are contained in* qAC^0*.*

As stated in the preliminaries, problems in qAC^0 cannot be hard for any complexity class containing Parity. Thus, we also obtain the following statement.

▶ **Corollary 11.** *Let* $\mathbf{V}$ *be a class of semigroups with the poly-logarithmic circuits property, such as the variety of finite groups* $\mathbf{G}$ *or the variety of finite commutative semigroups* $\mathbf{Com}$*. Then* $\mathrm{CSM}(\mathbf{V})$ *is not hard for any complexity class containing* Parity*, such as* ACC^0*,* TC^0*,* NC^1*,* L *or* NL*.*

4.3 The Complexity Landscape of Cayley Semigroup Membership

Our hardness results and qAC^0-algorithms have an immediate consequence on algebraic properties of maximal classes of finite semigroups for which the Cayley semigroup membership problem can be decided in qAC^0. It relies on the following result, which can be seen as a consequence of [1] and the fact that the zero element in a semigroup is always central. For completeness, we provide a short and self-contained proof.

▶ **Proposition 12.** *The variety* $\mathbf{N}$ *is included in* $\mathbf{G} \vee \mathbf{Com}$*.*

Proof. We show that every finite nilpotent semigroup is a quotient of a subdirect product of a finite group and a finite commutative semigroup. Note that in a finite nilpotent semigroup S, there exists an integer $e \geqslant 0$ such that for each $x \in S$, the power x^e is the zero element. Let $T = \{1, \dots, e\}$ be the commutative semigroup with the product of two elements i and j defined as $\min\{i + j, e\}$.

Let G be a finite group generated by the set X of non-zero elements of S such that no two products of less than e elements of X evaluate to the same element of G. Such a group exists because the free group over X is residually finite [22].

Let U be the subsemigroup of $G \times T$ generated by $\{(x, 1) \mid x \in X\}$. Now, we define a mapping $\varphi\colon U \to S$ as follows. Each element of the form (g, e) is mapped to zero. For every (g, ℓ) with $\ell < e$, there exists, by choice of G and by the definition of U, a unique factorization

$g = x_1 \cdots x_\ell$ with $x_1, \dots, x_\ell \in X$. We map (g, ℓ) to the product $x_1 \cdots x_\ell$ evaluated in S. It is straightforward to verify that φ is a surjective morphism and thus, S is a quotient of U. ◀

▶ **Corollary 13.** *There exist two varieties* $\mathbf{V}$ *and* $\mathbf{W}$ *such that both* $\mathrm{CSM}(\mathbf{V})$ *and* $\mathrm{CSM}(\mathbf{W})$ *are contained in* qAC^0 *(and thus not hard for any class containing* Parity*) but* $\mathrm{CSM}(\mathbf{V} \vee \mathbf{W})$ *is* NL*-complete.*

The corollary is a direct consequence of the previous proposition, Corollary 10 and Theorem 2. As was observed in [9] already, Cayley semigroup problems seem to have "strange complexity". The previous result makes this intuition more concrete and suggests that it is difficult to find "nice" descriptions of maximal classes of semigroups for which the Cayley semigroup membership problem is easier than any NL-complete problem.

4.4 Connections to FOLL

In a first attempt to solve outstanding complexity questions related to the Cayley semigroup membership problem, Barrington et al. introduced the complexity class FOLL. The approach presented in the present paper is quite different. This raises the question of whether our techniques can be used to design FOLL-algorithms for Cayley semigroup membership. Note that FOLL and qAC^0 are known to be incomparable, so we cannot use generic results from complexity theory to simulate qAC^0 circuits using families of FOLL circuits or vice versa. The direction $\mathsf{FOLL} \not\subseteq \mathsf{qAC}^0$ follows from bounds on the average sensitivity of bounded-depth circuits [16]; using these bounds, one can show that there exists a padded version of the Parity function which can be computed by a FOLL circuit family and cannot be computed by any qAC^0 circuit family. Conversely, each subset of $\{0,1\}^n$ of cardinality at most $n^{\log n}$ is decidable by a depth-2 circuit of size $n^{\log n} + 1$, but for each fixed $k \in \mathbb{N}$, there is some large value $n \geqslant 1$ such that the number of such subsets exceeds the number of different circuits of size n^k. This shows that there exist languages in qAC^0 which are not contained in $\mathsf{P/poly} \supseteq \mathsf{FOLL}$.

Designing an FOLL-algorithm which works for arbitrary classes of semigroups with the poly-logarithmic circuits property seems difficult. However, for certain special cases, there is an interesting approach, based on the repeated squaring technique. In the remainder of this section, we sketch one such special case.

For a Cayley circuit, the *width* of a topological ordering $(v_1, \dots, v_m)$ of the gates is the smallest number $w \in \mathbb{N}$ such that for each $i \in \{1, \dots, m-1\}$, at most w product gates from the set $A_i = \{v_1, \dots, v_i\}$ are connected to gates in $B_i = \{v_{i+1}, \dots, v_m\}$. Let C_i be the set of product gates, which belong to A_i and are connected to gates in B_i. The subcircuit induced by A_i can be interpreted as a Cayley circuit computing multiple output values C_i. The subcircuit induced by B_i can be seen as a circuit which, in addition to the input gates of the original circuit, uses the gates from C_i as input gates. The *width* of a Cayley circuit is the smallest width of a topological ordering of its gates. Let us fix some width $w \in \mathbb{N}$.

We introduce a predicate $P(z_1, \dots, z_w, y_1, \dots, y_w, i)$ which is true if there exists a Cayley circuit of width at most w and size at most 2^i with w additional input gates and w additional *passthrough gates* (which have in-degree 1 and replicate the value of their predecessors), such that the elements $y_1, \dots, y_w \in S$ occur as values of the passthrough gates when using $z_1, \dots, z_w \in S$ as values for the additional input gates and using any subset of the original inputs X as values for the remaining input gates. The additional input gates (resp. passthrough gates) are not counted when measuring the circuit size but are considered as product gates when measuring width and they have to be the first (resp. last) gates in all topological orderings considered for width measurement. For each fixed i, there are only n^{2w} such predicates.

The truth value of a predicate with $i = 0$ can be computed by a constant-depth unbounded fan-in Boolean circuit of polynomial size. This is achieved by computing all binary products of the elements $z_1, \ldots, z_w$ and elements of the input set X. For $i \geqslant 1$, the predicate $P(z_1, \ldots, z_w, y_1, \ldots, y_w, i)$ is true if and only if there exist $z'_1, \ldots, z'_w \in S$ such that both $P(z_1, \ldots, z_w, z'_1, \ldots, z'_w, i-1)$ and $P(z'_1, \ldots, z'_w, y_1, \ldots, y_w, i-1)$ are true. Having the truth values of all tuples for $i-1$ at hand, this can be checked with a polynomial number of gates in constant depth because there are only n^w different vectors $(z'_1, \ldots, z'_w) \in S^w$.

For a class of semigroups with Cayley circuits of bounded width and poly-logarithmic size, we obtain a circuit family of depth $\mathcal{O}(\log \log n)$ deciding Cayley semigroup membership: the predicates are computed for increasing values of i, until i exceeds the logarithm of an upper bound for the Cayley circuit size and then, we return $P(x, \ldots, x, t, \ldots, t, i)$ for the element t given in the input and for an arbitrary element $x \in X$. It is worth noting that the circuits constructed in the proof of Proposition 6 have width at most 2, so our FOLL-algorithm is a generalization of the *Double-Barrelled Recursive Strategy* and the proof that $\mathrm{CSM}(\mathbf{Ab}) \in$ FOLL presented in [9]. In particular, the procedure above yields a self-contained proof of the following result.

▶ **Theorem 14.** *Let* $\mathbf{V}$ *be a class of semigroups which is closed under taking subsemigroups and has the logarithmic power basis property. Then* $\mathrm{CSM}(\mathbf{V})$ *is in* FOLL.

By Lemma 4, we obtain the following corollary.

▶ **Corollary 15.** $\mathrm{CSM}(\mathbf{Com})$ *is contained in* FOLL.

5 Summary and Outlook

We provided new insights into the complexity of the Cayley semigroup membership problem for classes of finite semigroups, giving parallel algorithms for the variety of finite commutative semigroups and the variety of finite groups. We also showed that a maximal class of semigroups with Cayley semigroup membership decidable by qAC^0 circuits does not form a variety. Afterwards, we discussed applicability to FOLL.

It is tempting to ask whether one can find nice connections between algebra and the complexity of the Cayley semigroup membership problem by conducting a more fine-grained analysis. For example, it is easy to see that for the varieties of *rectangular bands* and *semilattices*, the Cayley semigroup membership problem is in AC^0. Does the maximal class of finite semigroups, for which the Cayley semigroup membership problem is in AC^0, form a variety of finite semigroups? Is it possible to show that AC^0 does not contain $\mathrm{CSM}(\mathbf{G})$? Potential approaches to tackling the latter question are reducing small distance connectivity for paths of non-constant length [17] to $\mathrm{CSM}(\mathbf{G})$ or developing a suitable switching lemma. Another related question is whether there exist classes of semigroups for which the Cayley semigroup membership problem cannot be NL-hard but, at the same time, is not contained within qAC^0.

Moreover, it would be interesting to see whether the Cayley semigroup membership problem can be shown to be in FOLL for all classes of semigroups with the poly-logarithmic circuits property. More generally, investigating the relation between FOLL and qAC^0, as well as their relationships to other complexity classes, remains an interesting subject for future research.

References

1 Jorge Almeida. Some pseudovariety joins involving the pseudovariety of finite groups. *Semigroup Forum*, 37(1):53–57, Dec 1988. doi:10.1007/BF02573123.

2 László Babai. Trading group theory for randomness. In Robert Sedgewick, editor, *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*, pages 421–429. ACM, 1985. doi:10.1145/22145.22192.

3 László Babai. Local expansion of vertex-transitive graphs and random generation in finite groups. In Cris Koutsougeras and Jeffrey Scott Vitter, editors, *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, pages 164–174. ACM, 1991. doi:10.1145/103418.103440.

4 László Babai, Robert Beals, Jin-Yi Cai, Gábor Ivanyos, and Eugene M. Luks. Multiplicative equations over commuting matrices. In *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '96, pages 498–507, Philadelphia, PA, USA, 1996. Society for Industrial and Applied Mathematics. URL: http://dl.acm.org/citation.cfm?id=313852.314109.

5 László Babai, Eugene M. Luks, and Ákos Seress. Permutation groups in NC. In Alfred V. Aho, editor, *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 409–420. ACM, 1987. doi:10.1145/28395.28439.

6 László Babai, Eugene M. Luks, and Ákos Seress. Permutation groups in NC. In Alfred V. Aho, editor, *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 409–420. ACM, 1987. doi:10.1145/28395.28439.

7 László Babai and Endre Szemerédi. On the complexity of matrix group problems I. In *25th Annual Symposium on Foundations of Computer Science, West Palm Beach, Florida, USA, 24-26 October 1984*, pages 229–240. IEEE Computer Society, 1984. doi:10.1109/SFCS.1984.715919.

8 David A. Mix Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in nc^1. In Juris Hartmanis, editor, *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA*, pages 1–5. ACM, 1986. doi:10.1145/12130.12131.

9 David A. Mix Barrington, Peter Kadau, Klaus-Jörn Lange, and Pierre McKenzie. On the complexity of some problems on groups input as multiplication tables. *J. Comput. Syst. Sci.*, 63(2):186–200, 2001. doi:10.1006/jcss.2001.1764.

10 David A. Mix Barrington and Pierre McKenzie. Oracle branching programs and logspace versus P. *Inf. Comput.*, 95(1):96–115, 1991. doi:10.1016/0890-5401(91)90017-V.

11 David A. Mix Barrington and Denis Thérien. Finite monoids and the fine structure of NC^1. *J. ACM*, 35:941–952, 1988.

12 Martin Beaudry. Membership testing in commutative transformation semigroups. *Inf. Comput.*, 79(1):84–93, 1988. doi:10.1016/0890-5401(88)90018-1.

13 Martin Beaudry. *Membership Testing in Transformation Monoids*. PhD thesis, McGill University, Montreal, Quebec, 1988.

14 Martin Beaudry. Membership testing in threshold one transformation monoids. *Inf. Comput.*, 113(1):1–25, 1994. doi:10.1006/inco.1994.1062.

15 Martin Beaudry, Pierre McKenzie, and Denis Thérien. The membership problem in aperiodic transformation monoids. *J. ACM*, 39(3):599–616, 1992. doi:10.1145/146637.146661.

16 Ravi B. Boppana. The average sensitivity of bounded-depth circuits. *Inf. Process. Lett.*, 63(5):257–261, 1997. doi:10.1016/S0020-0190(97)00131-2.

17 Xi Chen, Igor Carboni Oliveira, Rocco A. Servedio, and Li-Yang Tan. Near-optimal small-depth lower bounds for small distance connectivity. In Daniel Wichs and Yishay Mansour, editors, *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing,*

STOC 2016, Cambridge, MA, USA, June 18-21, 2016, pages 612–625. ACM, 2016. doi:10.1145/2897518.2897534.

18 Merrick L. Furst, John E. Hopcroft, and Eugene M. Luks. Polynomial-time algorithms for permutation groups. In *21st Annual Symposium on Foundations of Computer Science, Syracuse, New York, USA, 13-15 October 1980*, pages 36–41. IEEE Computer Society, 1980. doi:10.1109/SFCS.1980.34.

19 Johan Håstad. Almost optimal lower bounds for small depth circuits. In Juris Hartmanis, editor, *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA*, pages 6–20. ACM, 1986. doi:10.1145/12130.12132.

20 Neil D. Jones and William T. Laaser. Complete problems for deterministic polynomial time. *Theor. Comput. Sci.*, 3(1):105–117, 1976. doi:10.1016/0304-3975(76)90068-2.

21 Neil D. Jones, Y. Edmund Lien, and William T. Laaser. New problems complete for nondeterministic loc space. *Mathematical Systems Theory*, 10:1–17, 1976. doi:10.1007/BF01683259.

22 P. Levi. Über die Untergruppen der freien Gruppen. (2. Mitteilung). *Mathematische Zeitschrift*, 37:90–97, 1933. URL: http://eudml.org/doc/168437.

23 Omer Reingold. Undirected connectivity in log-space. *J. ACM*, 55(4):17:1–17:24, 2008. doi:10.1145/1391289.1391291.

24 Andrew Chi-Chih Yao. Separating the polynomial-time hierarchy by oracles (preliminary version). In *26th Annual Symposium on Foundations of Computer Science, Portland, Oregon, USA, 21-23 October 1985*, pages 1–10. IEEE Computer Society, 1985. doi:10.1109/SFCS.1985.49.