Emptiness Problems for Integer Circuits

Dominik Barth[1], Moritz Beck[2], Titus Dose[3], Christian Glaßer[4], Larissa Michler[5], and Marc Technau[6]

1 Institute of Computer Science, University of Würzburg, Germany
2 Institute of Computer Science, University of Würzburg, Germany
3 Institute of Computer Science, University of Würzburg, Germany
4 Institute of Computer Science, University of Würzburg, Germany
5 Institute of Computer Science, University of Würzburg, Germany
6 Institute of Computer Science, University of Würzburg, Germany

Abstract

We study the computational complexity of emptiness problems for circuits over sets of natural numbers with the operations union, intersection, complement, addition, and multiplication. For most settings of allowed operations we precisely characterize the complexity in terms of completeness for classes like NL, NP, and PSPACE. The case where intersection, addition, and multiplication is allowed turns out to be equivalent to the complement of polynomial identity testing (PIT).

Our results imply the following improvements and insights on problems studied in earlier papers. We improve the bounds for the membership problem $\mathrm{MC}(\cup, \cap, ^-, +, \times)$ studied by McKenzie and Wagner 2007 and for the equivalence problem $\mathrm{EQ}(\cup, \cap, ^-, +, \times)$ studied by Glaßer et al. 2010. Moreover, it turns out that the following problems are equivalent to PIT, which shows that the challenge to improve their bounds is just a reformulation of a major open problem in algebraic computing complexity:

- membership problem $\mathrm{MC}(\cap, +, \times)$ studied by McKenzie and Wagner 2007
- integer membership problems $\mathrm{MC}_{\mathbb{Z}}(+, \times)$ and $\mathrm{MC}_{\mathbb{Z}}(\cap, +, \times)$ studied by Travers 2006
- equivalence problem $\mathrm{EQ}(+, \times)$ studied by Glaßer et al. 2010

1998 ACM Subject Classification F.2.2 Nonnumerical Algorithms and Problems

Keywords and phrases computational complexity, integer expressions, integer circuits, polynomial identity testing

Digital Object Identifier 10.4230/LIPIcs.MFCS.2017.33

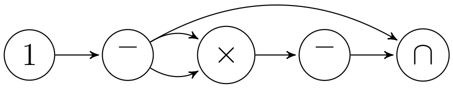
1 Introduction

Stockmeyer and Meyer [31] investigated membership and equivalence problems for *integer expressions*, which are built up from single natural numbers using set operations $(^-, \cup, \cap)$ and pairwise addition $(+)$. They also suggested to study expressions involving pairwise multiplication $(\times)$. For example, the expression $\overline{\overline{1} \times \overline{1}} \cap \overline{1}$ describes the set of primes $\mathbb{P}$.

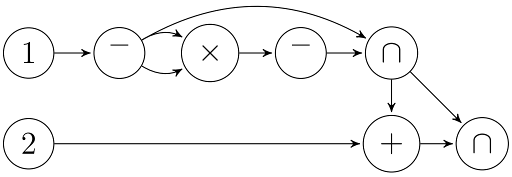
The *membership problem for expressions* is the question of whether the set described by a given expression contains some given natural number. The *equivalence problem for expressions* asks whether two given expressions describe the same set. Restricting the set of allowed operations results in problems of different complexities.

Wagner [33] introduced *circuits over sets of natural numbers*. These circuits describe expressions in a succinct way. The input gates of such a circuit are labeled with natural numbers, the inner gates compute set operations $(^-, \cup, \cap)$ and arithmetic operations $(+, \times)$. The following circuit has only 4 inner gates and describes the set of primes $\overline{\overline{1} \times \overline{1}} \cap \overline{1}$.

42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017).
Editors: Kim G. Larsen, Hans L. Bodlaender, and Jean-Francois Raskin; Article No. 33; pp. 33:1–33:14
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



A slightly larger circuit describes the set $\{n \in \mathbb{P} \mid n-2 \in \mathbb{P}\}$, i.e., the set of those twin primes p for which $p-2$ is also prime. Hence the set described by this circuit is infinite if and only if the twin prime conjecture holds.



Wagner [33], Yang [34], and McKenzie and Wagner [22] studied the complexity of membership problems for circuits over natural numbers (MC): Here, for a given circuit C with numbers assigned to the input gates, one has to decide whether a given number b belongs to the set described by the circuit. Travers [32] and Breunig [6] considered membership problems for circuits over integers ($\mathrm{MC}_{\mathbb{Z}}$) and positive integers ($\mathrm{MC}_{\mathbb{N}+}$), respectively. Glaßer et al [11] investigated *equivalence problems for circuits over sets of natural numbers* (EQ), i.e., the problem of deciding whether two given circuits compute the same set.

Satisfiability problems for circuits over sets of natural numbers, studied by Glaßer et al [13], are a generalization of the membership problems investigated by McKenzie and Wagner [22]: Here the circuits can have *unassigned input gates.* The question is, given a circuit C with gates from $\mathcal{O} \subseteq \{\cup, \cap, {}^{-}, +, \times\}$, and given a natural number b, does there exist an assignment of natural numbers to the unassigned input gates such that b is contained in the set described by the circuit?

Apart from the mentioned research on circuit problems there has been work on related variants like functions computed by circuits [24] and constraint satisfaction problems over natural numbers [12, 8].

In the present paper, we study *emptiness problems for circuits over sets of natural numbers.* In contrast to membership and satisfiability problems, here the question is whether a given circuit C with gates from $\mathcal{O} \subseteq \{\cup, \cap, {}^{-}, +, \times\}$ computes the empty set. We denote this problem with $\mathrm{EC}(\mathcal{O})$. In extension of that, we also consider circuits with unassigned input gates. For these we consider the problem Σ_1-$\mathrm{EC}(\mathcal{O})$ (resp., Π_1-$\mathrm{EC}(\mathcal{O})$), which asks whether the circuit computes the empty set for at least one assignment (resp., for all assignments).

Our contribution to emptiness problems. For most of the emptiness problems we precisely characterize the complexity in terms of completeness for classes like NL, P, NP, PSPACE, and coNEXP. In the remaining cases we obtain lower and upper bounds that do not match. Our results are summarized in Table 1 in Section 6.

The case of $\mathrm{EC}(\cap, +, \times)$ is particularly interesting. We show that it is logspace many-one equivalent to the complement of the polynomial identity testing (PIT), which asks whether a polynomial (given as a circuit) is identically zero. The problems are similar, still the proof of $\overline{\mathrm{PIT}} \leq_{\mathrm{m}}^{\log} \mathrm{EC}(\cap, +, \times)$ has to address two essential differences: First, PIT contains a universal quantifier (for all assignments the polynomial has to be zero), while $\mathrm{EC}(\cap, +, \times)$ does not. Second, PIT is defined over $\mathbb{Z}$, while $\mathrm{EC}(\cap, +, \times)$ is defined over $\mathbb{N}$.

In several cases we obtain upper bounds for Σ_1-$\mathrm{EC}(\mathcal{O})$ and Π_1-$\mathrm{EC}(\mathcal{O})$ by observing that if *some* assignment makes a circuit (non-)empty, then there exists a *small* such assignment.

Depending on $\mathcal{O}$ we obtain this observation by one of the following techniques: The first technique (e.g., used for Π_1-EC$(\cap,+) \in$ coNP in Theorem 6) uses specific systems of linear equations that consist of a large number of short equations. Such systems of equations have small solutions by the theory of integer programming. The second technique (e.g., used for EC$(\cap,+,\times) \equiv_{\mathrm{m}}^{\log} \Sigma_1$- EC$(\cap,+,\times)$ in Corollary 21) exploits the fact that the test of whether a multivariate polynomial is identically zero is possible by evaluating this polynomial for a fixed argument. The third technique (e.g., used for Σ_1-EC$(\cup,\cap,^{-},+) \in$ 2EXPSPACE and Σ_1-EC$(\cup,\cap,^{-},\times) \in$ 3EXPSPACE in Theorem 8) applies the decidability of Presburger and Skolem arithmetic.

Regarding the most general case EC$(\cup,\cap,^{-},+,\times)$ we show that this problem is logspace many-one equivalent to MC$(\cup,\cap,^{-},+,\times)$ and EQ$(\cup,\cap,^{-},+,\times)$, belongs to $\mathcal{R}_{\mathrm{tt}}(\Sigma_1)$, and is $\leq_{\mathrm{m}}^{\log}$-hard for $\mathrm{L}^{\mathrm{NEXP}}$. We leave open whether EC$(\cup,\cap,^{-},+,\times)$ is decidable and give evidence for the difficulty of finding a decision algorithm.

Our contribution to questions from previous work. By the equivalence mentioned above, our bounds for EC$(\cup,\cap,^{-},+,\times)$ improve the bounds for the problems MC$(\cup,\cap,^{-},+,\times)$ [22] and EQ$(\cup,\cap,^{-},+,\times)$ [11] as follows. The lower bound is raised from NEXP to $\mathrm{L}^{\mathrm{NEXP}}$ and the upper bound is slightly reduced from $\mathcal{R}_{\mathrm{T}}(\Sigma_1)$ to $\mathcal{R}_{\mathrm{tt}}(\Sigma_1)$.

We prove that PIT is logspace many-one equivalent to MC$(\cap,+,\times)$ studied in [22], $\mathrm{MC}_{\mathbb{Z}}(+,\times), \mathrm{MC}_{\mathbb{Z}}(\cap,+,\times)$ studied in [32], and EQ$(+,\times)$ studied in [11]. This characterizes the complexity of these problems and shows that the question for improved bounds is equivalent to a well-studied, open problem in algebraic computing complexity.

Finally we show that EQ$(\cap,+,\times)$ is $\leq_{\mathrm{m}}^{\log}$-complete for the complement of the second level of the Boolean hierarchy over PIT. This characterizes the complexity of this equivalence problem and explains the difficulty of improving the known upper bound [11].

The intention of this article is to summarize results and to develop a feeling for the proofs. The emphasis is on sketching several ideas at the expense of details. A comprehensive presentation is provided in the technical report [4].

2 Preliminaries

Basic Notations. Let $\mathbb{N}$ (resp., $\mathbb{Z}$) denote the set of natural numbers (resp., integers). $\mathbb{N}^+$ is the set of positive integers. For $x \in \mathbb{Z}$ the absolute value of x is denoted by $\mathrm{abs}(x)$, and for a matrix of integers $A = (a_{i,j}) \in \mathbb{Z}^{m \times n}$ for positive natural numbers m and n we define $||A||_\infty = \max\{\mathrm{abs}(a_{i,j}) \mid 1 \leq i \leq m \text{ and } 1 \leq j \leq n\}$.

L, NL, P, RP, BPP, NP, PSPACE, and NEXP denote standard complexity classes [23]. For a nondeterministic machine M, let $\mathrm{acc}_M(x)$ be the number of accepting paths of M on input x. The class #L consists of all functions acc_M, where M is a nondeterministic logarithmic-space-bounded machine. $\mathrm{C}_{=}\mathrm{L}$ is the class of problems A for which there exist $f, g \in \#\mathrm{L}$ such that for all inputs x it holds that $x \in A \Leftrightarrow f(x) = g(x)$. Further information on counting classes can be found in [2].

Let Σ_i and Π_i denote the levels of the arithmetical hierarchy. 2EXPSPACE, i.e., the class of problems decidable by a deterministic algorithm in double exponential space $2^{2^{n^k}}$ for some $k \in \mathbb{N}$, and 3EXPSPACE, which consists of the problems decidable in triple exponential space. For complexity classes $\mathcal{C}$ let $\mathrm{co}\mathcal{C} = \{\overline{A} \mid A \in \mathcal{C}\}$. We denote by K the Σ_1-complete halting problem (for some fixed Gödelization).

Addition and multiplication are extended to sets of integers: Let $A, B \subseteq \mathbb{Z}$. Then $A + B = \{a + b \mid a \in A, b \in B\}$ and $A \times B = \{a \cdot b \mid a \in A, b \in B\}$.

An oracle Turing machine is nonadaptive, if its queries are independent of the oracle (i.e., for all x and all oracles B and B', the computations $M^B(x)$ and $M^{B'}(x)$ have the same sequence of queries). For sets A and B we say that A is Turing reducible to B ($A \leq_{\mathrm{T}} B$), if there exists an oracle Turing machine M that accepts A with B as its oracle. If M is nonadaptive, then A is truth-table reducible to B ($A \leq_{\mathrm{tt}} B$). A is logspace Turing reducible to B ($A \leq_{\mathrm{T}}^{\log} B$), if there exists a logarithmic-space-bounded oracle Turing machine M (with one oracle tape) that accepts A with B as its oracle. If M's queries are nonadaptive (i.e., independent of the oracle), then A is logspace truth-table reducible to B ($A \leq_{\mathrm{tt}}^{\log} B$). A is logspace disjunctive-truth-table reducible to B ($A \leq_{\mathrm{dtt}}^{\log} B$), if there exists a logspace computable function f such that for all x, $f(x) = (y_1, y_2, \ldots, y_n)$ for some $n \geq 1$ and $\chi_A(x) = \max\{\chi_B(y_1), \chi_B(y_2), \ldots, \chi_B(y_n)\}$, where χ_S for a set S is the characteristic function of S. A set A is logspace (resp., polynomial time) many-one reducible to B, in notation $A \leq_{\mathrm{m}}^{\log} B$ (resp., $A \leq_{\mathrm{m}}^{\mathrm{p}} B$), if there exists a logarithmic-space-computable (resp., polynomial-time-computable) function f such that $\chi_A(x) = \chi_B(f(x))$. For a complexity class $\mathcal{C}$ we define $\mathcal{R}_{\mathrm{tt}}(\mathcal{C}) = \{A \mid \text{there is a } C \in \mathcal{C} \text{ with } A \leq_{\mathrm{tt}} C\}$.

Definition of circuits. A *circuit* $C = (V, E, g_C)$ is a finite, directed, acyclic graph with vertex set $V \subseteq \mathbb{N}$ and a designated vertex $g_C \in V$. Here, graphs are allowed to have multi-edges and are not required to be connected. We require that C is topologically ordered, that is, if $v, v' \in V$ are vertices with $v < v'$, then there is no edge from v' to v.

Let $\mathcal{O} \subseteq \{\cup, \cap, ^-, +, \times\}$. A *partially assigned $\mathcal{O}$-circuit* (*$\mathcal{O}$-circuit* for short) $C = (V, E, g_C, \alpha)$ is a circuit (V, E, g_C) whose nodes are labeled by the *labeling function* $\alpha : V \to \mathcal{O} \cup \mathbb{N} \cup \{\square\}$ such that each node has indegree ≤ 2, nodes with indegree 0 have labels from $\mathbb{N} \cup \{\square\}$, nodes with indegree 1 have label $^-$, and nodes with indegree 2 have labels from $\mathcal{O} \setminus \{^-\}$. In the context of circuits, nodes are also called *gates. Input gates* (i.e., gates with indegree 0) with labels from $\mathbb{N}$ are called *assigned* input gates. Input gates with label $\square$ are called *unassigned.* An $\mathcal{O}$-circuit whose input gates are all assigned is called *completely assigned $\mathcal{O}$-circuit.* We use the term *integer circuit* for both partially assigned $\mathcal{O}$-circuits and completely assigned $\mathcal{O}$-circuits.

There exists a deterministic logarithmic-space-bounded algorithm which on input of a graph decides whether the input is a partially assigned $\mathcal{O}$-circuit.

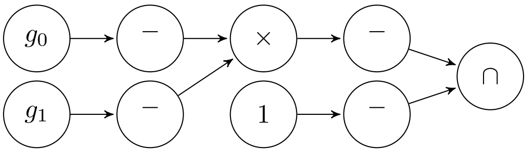
The set computed by a circuit. For an $\mathcal{O}$-circuit C with unassigned input gates $g_1 < \cdots < g_n$ and $x_1, \ldots, x_n \in \mathbb{N}$, let $C(x_1, \ldots, x_n)$ be the completely assigned $\mathcal{O}$-circuit that is obtained from C by modifying the labeling function α such that $\alpha(g_i) = x_i$ for $i = 1, \ldots, n$.

For a completely assigned $\mathcal{O}$-circuit $C = (V, E, g_C, \alpha)$ we inductively define the *set* $I(g; C)$ *computed by a gate* $g \in V$ by

$$I(g; C) = \begin{cases} \{\alpha(g)\} \subseteq \mathbb{N} & \text{if } g \text{ has indegree } 0 \quad (g \text{ is an input gate}), \\ \mathbb{N} \setminus I(g'; C) & \text{if } g = \overline{g'} \quad (g \text{ is a complement gate}), \\ I(g'; C) \otimes I(g''; C) & \text{if } g = g' \otimes g'' \quad (g \text{ is a gate of type } \otimes \in \{\cup, \cap, +, \times\}). \end{cases}$$

The *set computed by* C is defined as $I(C) = I(g_C; C)$.

Example. For unassigned inputs g_0 and g_1, consider the circuit C:



We write $C = \overline{\overline{g_0} \times \overline{g_1}} \cap \overline{1}$ as an abbreviation. $C(1, 1)$ computes the set of all primes, $C(x, y)$ for $x = y \in \mathbb{P} \cup \{0\}$ computes the set $\{x\}$, and $C(x, y)$ for all other (x, y) computes the empty set.

▶ **Definition 1.** Let $\mathcal{O} \subseteq \{\cup, \cap, {}^{-}, +, \times\}$. We define *membership*, *emptiness*, *equivalence*, and *satisfiability* problems for circuits.

$$\begin{aligned}
\mathrm{MC}(\mathcal{O}) &\overset{\mathit{df}}{=} \{(C, b) \mid C \text{ is a completely assigned } \mathcal{O}\text{-circuit and } b \in I(C)\} \\
\Sigma_1\text{-MC}(\mathcal{O}) &\overset{\mathit{df}}{=} \{(C, b) \mid C \text{ is a partially assigned } \mathcal{O}\text{-circuit with } n \text{ unassigned inputs,} \\
&\qquad\qquad \text{there exist } x_1, \ldots, x_n \in \mathbb{N} \text{ s.t. } b \in I(C(x_1, \ldots, x_n))\} \\
\mathrm{EQ}(\mathcal{O}) &\overset{\mathit{df}}{=} \{(C_1, C_2) \mid C_1, C_2 \text{ are completely assigned } \mathcal{O}\text{-circuits, } I(C_1) = I(C_2)\}^{1} \\
\mathrm{EC}(\mathcal{O}) &\overset{\mathit{df}}{=} \{C \mid C \text{ is a completely assigned } \mathcal{O}\text{-circuit and } I(C) = \emptyset\} \\
\Sigma_1\text{-EC}(\mathcal{O}) &\overset{\mathit{df}}{=} \{C \mid C \text{ is a partially assigned } \mathcal{O}\text{-circuit with } n \text{ unassigned inputs,} \\
&\qquad\qquad \text{there exist } x_1, \ldots, x_n \in \mathbb{N} \text{ s.t. } I(C(x_1, \ldots, x_n)) = \emptyset\} \\
\Pi_1\text{-EC}(\mathcal{O}) &\overset{\mathit{df}}{=} \{C \mid C \text{ is a partially assigned } \mathcal{O}\text{-circuit with } n \text{ unassigned inputs,} \\
&\qquad\qquad \text{for all } x_1, \ldots, x_n \in \mathbb{N} \text{ it holds } I(C(x_1, \ldots, x_n)) = \emptyset\} \\
\Sigma_1\text{-NEC}(\mathcal{O}) &\overset{\mathit{df}}{=} \overline{\Pi_1\text{-EC}(\mathcal{O})}
\end{aligned}$$

The integer variants $\mathrm{MC}_{\mathbb{Z}}(\mathcal{O})$, $\mathrm{EC}_{\mathbb{Z}}(\mathcal{O})$, and $\Sigma_1\text{-EC}_{\mathbb{Z}}(\mathcal{O})$ are defined analogously (assigned and unassigned inputs are from $\mathbb{Z}$, the complement is defined with respect to $\mathbb{Z}$). A systematic study of the membership problems $\mathrm{MC}_{\mathbb{Z}}(\mathcal{O})$ was done by Travers [32].

We use the following abbreviations: we write n for the singleton $\{n\}$; we write C for $I(C)$, where C is a circuit; we write $\mathrm{MC}(\cup, \cap, {}^{-}, +, \times)$ for $\mathrm{MC}(\{\cup, \cap, {}^{-}, +, \times\})$ and the like.

3 Basic Results

We start with easy reductions between $\mathrm{EC}(\mathcal{O})$, $\Sigma_1\text{-EC}(\mathcal{O})$, $\Pi_1\text{-EC}(\mathcal{O})$, and $\mathrm{MC}(\mathcal{O})$.

▶ **Lemma 2.** *Let $\mathcal{O} \subseteq \{\cup, \cap, {}^{-}, +, \times\}$ and $\mathcal{E} \in \{\mathrm{EC}, \Sigma_1\text{- EC}, \Pi_1\text{- EC}\}$.*

1. *If $\cap \in \mathcal{O}$, then $\overline{\mathrm{MC}(\mathcal{O})} \leq_{\mathrm{m}}^{\log} \overline{\mathrm{EC}(\mathcal{O})}$ and $\Sigma_1\text{-MC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \Sigma_1\text{-NEC}(\mathcal{O})$.*
2. *If $\times \in \mathcal{O}$, then $\overline{\mathrm{EC}(\mathcal{O})} \leq_{\mathrm{m}}^{\log} \mathrm{MC}(\mathcal{O})$ and $\Sigma_1\text{-NEC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \Sigma_1\text{-MC}(\mathcal{O})$.*
3. *If $\mathcal{O} \subseteq \{\cup, +, \times\}$ or $\mathcal{O} \subseteq \{{}^{-}\}$, then $\mathrm{EC}(\mathcal{O}) = \Sigma_1\text{-EC}(\mathcal{O}) = \Pi_1\text{-EC}(\mathcal{O}) = \emptyset$.*
4. *$\mathcal{E}(\{\cup, {}^{-}\} \cup \mathcal{O}) \equiv_{\mathrm{m}}^{\log} \mathcal{E}(\{\cap, {}^{-}\} \cup \mathcal{O}) \equiv_{\mathrm{m}}^{\log} \mathcal{E}(\{\cup, \cap, {}^{-}\} \cup \mathcal{O})$ for $\mathcal{O} \subseteq \{+, \times\}$.*
5. *$\mathcal{E}(\mathcal{O}') \leq_{\mathrm{m}}^{\log} \mathcal{E}(\mathcal{O})$ for $\mathcal{O}' \subseteq \mathcal{O}$.*
6. *$\mathrm{EC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \Sigma_1\text{-EC}(\mathcal{O})$ and $\mathrm{EC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \Pi_1\text{-EC}(\mathcal{O})$.*

The following bounds are obtained with minor effort from known results and Lemma 2.

▶ **Theorem 3** ([22, 11, 13])**.**

1. *$\mathrm{EC}(\cup, \cap, +, \times)$ is $\leq_{\mathrm{m}}^{\log}$-complete for* coNEXP*.*
2. *$\mathrm{EC}(\cup, \cap, {}^{-}, +), \mathrm{EC}(\cup, \cap, {}^{-}, \times) \in \mathrm{PSPACE}$.*

[1] In [11], equivalence problems for circuits are denoted by $\mathrm{EC}(\mathcal{O})$, which is in conflict with our notation for emptiness problems. Therefore, we use the notation $\mathrm{EQ}(\mathcal{O})$ for equivalence problems.

3. $\mathrm{EC}(\cap, +)$ *and* $\mathrm{EC}(\cap, \times)$ *are* $\leq_{\mathrm{m}}^{\log}$*-hard for* $\mathrm{coC_{=}L}$.
4. Π_1-$\mathrm{EC}(\cap, \times)$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* coNP.

Circuits with solely set operations can express graph accessibility as well as evaluation and satisfiability of Boolean circuits. This leads to the following results.

▶ **Proposition 4.**
1. $\mathrm{EC}(\cap)$, Σ_1-$\mathrm{EC}(\cap)$, *and* Π_1-$\mathrm{EC}(\cap)$ *are* $\leq_{\mathrm{m}}^{\log}$*-complete for* NL.
2. $\mathrm{EC}(\cup, \cap, {}^{-})$, $\mathrm{EC}(\cup, \cap)$, Σ_1-$\mathrm{EC}(\cup, \cap)$, *and* Π_1-$\mathrm{EC}(\cup, \cap)$ *are* $\leq_{\mathrm{m}}^{\log}$*-complete for* P.
3. Σ_1-$\mathrm{EC}(\cup, \cap, {}^{-})$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* NP *and* Π_1-$\mathrm{EC}(\cup, \cap, {}^{-})$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* coNP.

4 Circuits with One Arithmetic Operation

4.1 Circuits without Complement

Here only those problems are relevant that admit intersection, since otherwise the circuits compute non-empty sets.

By an induction on the structure of the circuit we obtain: $C \in \Sigma_1$-$\mathrm{EC}(\cap, +)$ if and only if at least one of the circuits $C(0, \dots, 0)$, $C(1, 0, \dots, 0)$, $C(0, 1, \dots, 0)$, $\dots$, $C(0, 0, \dots, 1)$ belongs to $\mathrm{EC}(\cap, +)$. Hence Σ_1-$\mathrm{EC}(\cap, +) \leq_{\mathrm{dtt}}^{\log} \mathrm{EC}(\cap, +)$. It is known that $\mathrm{EC}(\cap, +) \in \mathrm{coC_{=}L}$ [11] and $\mathrm{coC_{=}L}$ is closed under $\leq_{\mathrm{dtt}}^{\log}$ [3]. This yields:

▶ **Theorem 5.** Σ_1-$\mathrm{EC}(\cap, +) \in \mathrm{coC_{=}L}$.

We obtain several results that rely on an estimation by Schrijver [28] saying that systems of linear equations consisting of arbitrarily many equations have solutions whose greatest component is at most $(32k)^{12n^4}$, where k is the greatest constant in the system and n the number of variables. So there are "small solutions for huge systems of small equations".

It is straightforward to see that the question of whether an $\{\cap, +\}$-circuit C is in $\mathcal{E}(\cap, +)$ for $\mathcal{E} \in \{\mathrm{EC}, \Sigma_1\text{-}\mathrm{EC}, \Pi_1\text{-}\mathrm{EC}\}$ can be answered by solving a system of linear equations in which each unassigned input gate is represented by one variable and constants have polynomial length in the size of the circuit. We extend this idea such that also emptiness problems that allow unions can be reduced to similar problems regarding (sets of) equation systems. This leads to the following results.

▶ **Theorem 6.** **1.** Π_1-$\mathrm{EC}(\cap, +)$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* coNP.
2. $\mathrm{EC}(\cup, \cap, +)$ *and* $\mathrm{EC}(\cup, \cap, \times)$ *are* $\leq_{\mathrm{m}}^{\log}$*-hard for* PSPACE.
3. Σ_1-$\mathrm{EC}(\cup, \cap, +), \Pi_1$-$\mathrm{EC}(\cup, \cap, +), \Pi_1$-$\mathrm{EC}(\cup, \cap, \times) \in \mathrm{PSPACE}$.

The problems Σ_1-EC and EC for the sets of operations $\{\cap, \times\}$ and $\{\cup, \cap, \times\}$ will be solved by a general tool given in Theorems 19, 20, and Corollary 21.

4.2 Circuits with Complement

4.2.1 Upper Bounds

$\mathrm{Th}(\mathbb{N}; +, =)$ denotes the Presburger arithmetic, i.e., the first-order theory of $\mathbb{N}$ with addition. $\mathrm{Th}(\mathbb{N}; \times, =, \mathbb{P} \cup \{0, 1\})$ denotes the Skolem arithmetic with constants, i.e., the first-order theory of $\mathbb{N}$ with multiplication and constants for 0, 1, and all primes.

▶ **Theorem 7** ([9, 10, 14, 5])**.**
1. $\mathrm{Th}(\mathbb{N}; +, =) \in \mathrm{2EXPSPACE}$.
2. $\mathrm{Th}(\mathbb{N}; \times, =, \mathbb{P} \cup \{0, 1\}) \in \mathrm{3EXPSPACE}$.

The sets computed in the nodes of circuits over $\{\cup,\cap,^-,+\}$ and $\{\cup,\cap,^-,\times\}$ can be expressed by Presburger and Skolem formulas. These formulas can be constructed in polynomial time, which allows to transfer the upper bounds of Presburger and Skolem arithmetic.

▶ **Theorem 8.**
1. $\Sigma_1\text{-EC}(\cup,\cap,^-,+), \Pi_1\text{-EC}(\cup,\cap,^-,+) \in \text{2EXPSPACE}$.
2. $\Sigma_1\text{-EC}(\cup,\cap,^-,\times), \Pi_1\text{-EC}(\cup,\cap,^-,\times) \in \text{3EXPSPACE}$.

4.2.2 Lower Bounds

All emptiness problems covered by Section 4.2 – in particular $\text{EC}(^-,+)$ and $\text{EC}(^-,\times)$ – are $\leq_\text{m}^\text{log}$-hard for PSPACE. We show the same for $\text{MC}(^-,+)$ and $\text{MC}(^-,\times)$ improving unpublished results by Reinhardt, which were announced by McKenzie and Wagner [22] and which state that these problems are $\leq_\text{m}^\text{p}$-hard for PSPACE. This section mainly sketches our proof for the $\leq_\text{m}^\text{log}$-hardness of $\text{MC}(^-,+)$ for PSPACE. For that we define a further problem.

▶ **Definition 9.** A $\{^-,+\}$-circuit over $\mathbb{N}^k$ is a completely assigned $\{^-,+\}$-circuit $C = ((V,E),g_C,\alpha)$ where all constants are elements of $\mathbb{N}^k$. The set $I(g;C) \subseteq \mathbb{N}^k$ computed by a node g is defined analogously to the one-dimensional case. Further let $I(C) = I(g_C;C)$ and

$$\begin{aligned}\text{MC}^+(^-,+) = \{(C,b) \mid\ & C \text{ is a completely assigned } \{^-,+\}\text{-circuit over } \mathbb{N}^k, \\ & ||c||_\infty \leq 1 \text{ for every input } c,\ ||b||_\infty \leq 3, \text{ and } b \in I(C)\}.\end{aligned}$$

The PSPACE-hardness of this problem is obtained by reducing CNF-QBF, which is the problem of whether a given quantified Boolean formula F in conjunctive normal form is true. It is known that CNF-QBF is $\leq_\text{m}^\text{log}$-complete for PSPACE.

The proof of the following lemma is based on an unpublished proof by Reinhardt [25] showing the $\leq_\text{m}^\text{p}$-hardness of $\text{MC}(^-,\times)$ for PSPACE.

▶ **Lemma 10.** $\text{MC}^+(^-,+)$ *is* $\leq_\text{m}^\text{log}$*-hard for* PSPACE.

From now on our proof differs from Reinhardt's proof. Instead of showing directly $\text{MC}^+(^-,+) \leq_\text{m}^\text{p} \overline{\text{MC}(^-,\times)}$ via a simple reduction, we first prove $\text{MC}^+(^-,+) \leq_\text{m}^\text{log} \text{MC}(^-,+)$ and then show $\overline{\text{MC}(^-,+)} \leq_\text{m}^\text{log} \text{EC}(^-,+) \leq_\text{m}^\text{log} \text{EC}(^-,\times) \leq_\text{m}^\text{log} \overline{\text{MC}(^-,\times)}$.

To show $\text{MC}^+(^-,+) \leq_\text{m}^\text{log} \text{MC}(^-,+)$ it is convenient to represent a vector of natural numbers $a = (a_0,\dots,a_k)$ as a natural number $\text{ad}_n(a) = \sum_{i=0}^k a_{k-i}n^i$ for $n \geq 2$. We denote the function mapping (C,b) onto $(C',\text{ad}_n(b))$ by ad_n, where C' is the circuit obtained from C by replacing each input x with $\text{ad}_n(x)$.

Indeed, ad_n for sufficiently large n works as reduction if for example union and intersection are allowed instead of complement. However, in our case we have $(0,1,0) \notin \overline{(0,0,0)} + (0,0,1)$, but $\text{ad}_8(0,1,0) = \text{ad}_8(0,0,7) + \text{ad}_8(0,0,1) \in \overline{\text{ad}_8(0,0,0)} + \text{ad}_8(0,0,1)$. Such "overflows" are the reason why ad_n is not a reduction $\text{MC}^+(^-,+) \leq_\text{m}^\text{log} \text{MC}(^-,+)$ for any n.

To address this problem we implement an operation similar to the bitwise 'or' for characteristic sequences: for two finite sets A and B (note that for problems of the form "$(C,b) \in \text{MC}^+(^-,+)$?" it suffices to consider the first $b+1$ bits of characteristic sequences of sets) let $m = \max(A \cup B)$ and consider $M = \overline{\overline{A + \{m-1\}} + 1} + \overline{\overline{B + \{m-1\}} + 1} = ((A+\{m\}) \cup \{0\}) + ((B+\{m\}) \cup \{0\})$. Observe that $M \cap \{m,\dots,2m\} = \{m+x \mid x \in A \cup B\}$, which equals the union of A and B shifted by the offset m.

Now a circuit over $\mathbb{N}^k$ can be simulated by a circuit over $\mathbb{N}$: Roughly speaking, we use ad_8 and after computing the operation of some node g, the numbers x with $||\text{ad}_8^{-1}(x)|| > 3$ can be deleted from $I(g)$ by adding them into $\overline{I(g)}$ via the 'or'-operation mentioned above. Every 'or'-operation yields an offset which has to be taken into account. This leads to:

▶ **Theorem 11.** $\mathrm{MC}(^-,+)$ *is* $\leq_{\mathrm{m}}^{\log}$*-hard for* PSPACE*.*

The following theorem is essentially due to Sigmund [30]. He provided the proof of the second reduction and the main idea of the proof of the first one.

▶ **Theorem 12.** $\overline{\mathrm{MC}(^-,+)} \leq_{\mathrm{m}}^{\log} \mathrm{EC}(^-,+)$ *and* $\mathrm{EC}(^-,+) \leq_{\mathrm{m}}^{\log} \mathrm{EC}(^-,\times)$*.*

▶ **Corollary 13.** $\mathrm{EC}(^-,+)$*,* $\mathrm{EC}(^-,\times)$*, and* $\mathrm{MC}(^-,\times)$ *are* $\leq_{\mathrm{m}}^{\log}$*-hard for* PSPACE*.*

5 Circuits with both Arithmetic Operations

Besides proving bounds for emptiness problems with + and ×, we improve the known lower and upper bounds for $\mathrm{MC}(\cup,\cap,^-,+,\times)$ [22] and $\mathrm{EQ}(\cup,\cap,^-,+,\times)$ [11]. Then we provide arguments that suggest the difficulty of proving the decidability of $\mathrm{EC}(^-,+,\times)$ and $\mathrm{EC}(\cup,\cap,^-,+,\times,)$. Finally we draw connections to polynomial identity testing (PIT) and show that the open questions for the complexities of $\mathrm{MC}(\cap,+,\times)$ [22], $\mathrm{MC}_{\mathbb{Z}}(\cap,+,\times)$, $\mathrm{MC}_{\mathbb{Z}}(+,\times)$ [32], and $\mathrm{EQ}(+,\times)$ [11] are equivalent to the well-studied, open question for the complexity of PIT.

5.1 Upper and Lower Bounds for Possibly Undecidable Problems

We obtain upper bounds by improving a known decision algorithm [11] and lower bounds via the Matiyasevich-Robinson-Davis-Putnam theorem [21, 7].

▶ **Theorem 14.**

1. $\mathrm{EC}(\cup,\cap,^-,+,\times) \in \mathcal{R}_{\mathrm{tt}}(\Sigma_1)$*.*
2. $\Sigma_1\text{-}\mathrm{EC}(\cup,\cap,^-,+,\times) \in \Sigma_2$ *and* $\Pi_1\text{-}\mathrm{EC}(\cup,\cap,^-,+,\times) \in \Pi_2$*.*
3. $\Pi_1\text{-}\mathrm{EC}(\cap,+,\times)$ *and* $\Pi_1\text{-}\mathrm{EC}(\cup,\cap,+,\times)$ *are* $\leq_{\mathrm{m}}^{\log}$*-complete for* Π_1*.*
4. $\Sigma_1\text{-}\mathrm{MC}(^-,+,\times)$ *and* $\Sigma_1\text{-}\mathrm{EC}(^-,+,\times)$ *are* $\leq_{\mathrm{m}}^{\log}$*-hard for* Σ_1*.*
5. $\Pi_1\text{-}\mathrm{EC}(^-,+,\times)$ *is* $\leq_{\mathrm{m}}^{\log}$*-hard for* Π_1*.*

5.2 Connecting Emptiness with Membership and Equivalence Problems

We show that with the operations $^-$, +, and × one can express a Boolean combination of emptiness problems as a single emptiness problem. Therefore, truth-table reductions to certain emptiness problems can be transformed into many-one reductions. This allows us to show certain emptiness problems to be many-one equivalent to membership problems and equivalence problems. As a byproduct we improve the known lower and upper bounds of $\mathrm{MC}(\cup,\cap,^-,+,\times)$ [22] and $\mathrm{EQ}(\cup,\cap,^-,+,\times)$ [11].

▶ **Proposition 15.** *The following holds if* $\{^-,+,\times\} \subseteq \mathcal{O}$*.*

1. *If* $A \leq_{\mathrm{tt}}^{\log} \mathrm{EC}(\mathcal{O})$*, then* $A \leq_{\mathrm{m}}^{\log} \mathrm{EC}(\mathcal{O})$*. If* $A \leq_{\mathrm{tt}} \mathrm{EC}(\mathcal{O})$*, then* $A \leq_{\mathrm{m}} \mathrm{EC}(\mathcal{O})$*.*
2. *If* $\mathrm{EC}(\mathcal{O})$ *is* $\leq_{\mathrm{m}}$*-hard for* Σ_1*, then it is* $\leq_{\mathrm{m}}$*-hard for* $\mathcal{R}_{\mathrm{tt}}(\Sigma_1)$*.*
3. *If* $\mathrm{EC}(\mathcal{O}) \in \Sigma_1 \cup \Pi_1$*, then* $\mathrm{EC}(\mathcal{O}) \in \Sigma_0$*.*

▶ **Corollary 16.**

1. $\mathrm{MC}(\cup,\cap,^-,+,\times) \equiv_{\mathrm{m}}^{\log} \mathrm{EQ}(\cup,\cap,^-,+,\times) \equiv_{\mathrm{m}}^{\log} \mathrm{EC}(\cup,\cap,^-,+,\times) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{EC}(\cup,\cap,^-,+,\times)}$*.*
2. $\Sigma_1\text{-}\mathrm{MC}(\cup,\cap,^-,+,\times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cup,\cap,^-,+,\times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{NEC}(\cup,\cap,^-,+,\times)$*.*
3. $\mathrm{EC}(\cup,\cap,^-,+,\times), \mathrm{MC}(\cup,\cap,^-,+,\times), \mathrm{EQ}(\cup,\cap,^-,+,\times) \in \mathcal{R}_{\mathrm{tt}}(\Sigma_1)$ *and these problems are* $\leq_{\mathrm{m}}^{\log}$*-hard for* $\mathcal{R}_{\mathrm{T}}^{\log}(\mathrm{NEXP}) = \mathrm{L}^{\mathrm{NEXP}}$*.*
4. $\mathrm{EC}(^-,+,\times)$ *is* $\leq_{\mathrm{m}}$*-hard for* Σ_1 *if and only if it is* $\leq_{\mathrm{m}}$*-complete for* $\mathcal{R}_{\mathrm{tt}}(\Sigma_1)$*.*
5. $\mathrm{EC}(\cup,\cap,^-,+,\times)$ *is* $\leq_{\mathrm{m}}$*-hard for* Σ_1 *if and only if it is* $\leq_{\mathrm{m}}$*-complete for* $\mathcal{R}_{\mathrm{tt}}(\Sigma_1)$*.*

For $\{^-, +, \times\}$-circuits there are further equivalences between membership and emptiness problems.

▶ **Proposition 17.**

1. $\mathrm{MC}(^-, +, \times) \equiv_{\mathrm{m}}^{\log} \mathrm{EC}(^-, +, \times) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{EC}(^-, +, \times)}$.
2. $\Sigma_1\text{-MC}(^-, +, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-EC}(^-, +, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-NEC}(^-, +, \times)$.

5.3 The Difficulty of $\mathrm{EC}(^-, +, \times)$ and $\mathrm{EC}(\cup, \cap, ^-, +, \times)$

In the Corollaries 13 and 16 we showed that $\mathrm{EC}(^-, +, \times)$ is $\leq_{\mathrm{m}}^{\log}$-hard for PSPACE and $\mathrm{EC}(\cup, \cap, ^-, +, \times,)$ is $\leq_{\mathrm{m}}^{\log}$-hard for $\mathrm{L}^{\mathrm{NEXP}}$. By Theorem 14, both problems belong to $\mathcal{R}_{\mathrm{tt}}(\Sigma_1)$. It is an open question whether these problems are decidable. This subsection explains the difficulty of finding decision algorithms for these problems.

Goldbach conjectured that every even integer greater than 2 is the sum of two primes. At the time the conjecture was made 1 was considered to be prime, but later the opposite view became accepted. Let $\mathbb{P}_1 = \mathbb{P} \cup \{1\}$. Below we formulate both variants, Goldbach's original conjecture (GC_1) and the one that nowadays is called *Goldbach's conjecture* (GC).

$$\begin{aligned} \mathrm{GC}_1 &= \forall n \geq 1\, \exists p, q \in \mathbb{P}_1\ [2n = p + q] \\ \mathrm{GC} &= \forall n \geq 2\, \exists p, q \in \mathbb{P}\ [2n = p + q] \end{aligned}$$

We define circuits that express the truth of these conjectures, where $\mathbb{P}_1$ stands for $\overline{\overline{1} \times \overline{1}}$, $\mathbb{P}$ for $\overline{\overline{1} \times \overline{1}} \cap \overline{1}$, and $\{0, 1\}$ for $\overline{\overline{0} + 1}$.

$$\begin{aligned} C_1 &= \overline{((\mathbb{P}_1 + \mathbb{P}_1) \times \{0, 1\}) + \{0, 1\}} \\ C &= \overline{\mathbb{P} + \mathbb{P}} \cap (2 \times \overline{\{0, 1\}}) \end{aligned}$$

GC_1 is true if any only if $C_1 \in \mathrm{EC}(^-, +, \times)$. GC is true if and only if $C \in \mathrm{EC}(\cup, \cap, ^-, +, \times,)$. This tells us: If one finds a decision algorithm for $\mathrm{EC}(^-, +, \times)$ or $\mathrm{EC}(\cup, \cap, ^-, +, \times)$ and proves its correctness, then in a sense this solves Goldbach's conjecture, since the computation of this algorithm is a proof or refutation. In particular, this would imply that Goldbach's conjecture is provable or refutable, which is unknown (cf. [17]). This underlines the difficulty of finding decision algorithms for $\mathrm{EC}(^-, +, \times)$ and $\mathrm{EC}(\cup, \cap, ^-, +, \times)$.

5.4 Connection between Emptiness and Σ_1-Emptiness

We show that several emptiness problems are equivalent to their Σ_1-emptiness variants. The proof exploits the fact that the test of whether a multivariate polynomial with coefficients bounded by some constant K is identically zero is possible by evaluating this polynomial for one fixed argument only dependent on K and the total degree of the polynomial. The following lemma shows that the test of whether multivariate polynomials are identically zero reduces to the univariate case.

▶ **Lemma 18** ([20]). *Given a polynomial $f(x_1, \ldots, x_n)$ over $\mathbb{R}$ with total degree at most d, the substitution $x_i \mapsto x^{(d+1)^{i-1}}$ has the property that f is identically zero on $\mathbb{R}^n$ if and only if the obtained univariate polynomial is identically zero on $\mathbb{R}$.*

The lemma allows a reduction from Σ_1- $\mathrm{EC}(\cap, +, \times)$ to $\mathrm{EC}(\cap, +, \times)$: Consider a circuit $C \in \Sigma_1$- $\mathrm{EC}(\cap, +, \times)$ with unassigned inputs $u_1, \ldots, u_n$ and let $z_1, \ldots, z_n \in \mathbb{N}$ such that $C(z_1, \ldots, z_n) = \emptyset$. So under this assignment there exists a $\cap$-gate g connected to the output and computing $\emptyset$ such that no ancestor of g computes $\emptyset$. The unique number computed in the left\right predecessor $g_l \backslash g_r$ of g (note that due to the absence of $^-$ and $\cup$ each gate computes a set containing at most one element) can be written as a multivariate polynomial $p_l \backslash p_r$ with variables $u_1, \ldots, u_n$. It holds that $p_l \neq p_r$, since g computes $\emptyset$. By Lemma 18, the same holds for the univariate polynomials $p'_l \backslash p'_r$ obtained by the substitution. Note that $p'_l(x) \neq p'_r(x)$ for every large enough x. Moreover, there is a circuit computable in logarithmic space that generates such an x. So the substitution rule provides the assignment $x^{(d+1)^0}, x^{(d+1)^1}, \ldots, x^{(d+1)^{n-1}}$ under which g and hence also C computes $\emptyset$. This yields the following theorem.

▶ **Theorem 19.**
1. $\mathrm{EC}(\cap, +, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cap, +, \times)$.
2. $\mathrm{EC}_{\mathbb{Z}}(\cap, +, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}_{\mathbb{Z}}(\cap, +, \times)$.
3. $\mathrm{EC}(\cap, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cap, \times)$.

We generalize this argument to $\{\cup, \cap, +, \times\}$-circuits by unfolding such circuits C to a tree D, which exponentially increases the size, but not the depth. Then we observe that $C(z_1, \ldots, z_n) = \emptyset$ if and only if for all possibilities to prune D to some D' such that each $\cup$-gate has exactly one predecessor it holds that $D'(z_1, \ldots, z_n) = \emptyset$. Since a $\cup$-gate with exactly one predecessor acts like a wire, the D' are $\{\cap, +, \times\}$-circuits. Hence $C \in \Sigma_1\text{-}\mathrm{EC}(\cup, \cap, +, \times)$ if and only if for all D' it holds that $D' \in \Sigma_1\text{-}\mathrm{EC}(\cap, +, \times)$. So we reached a situation similar to Theorem 19.1 with the difference that D' has exponential size and polynomial depth, which translates to polynomials with an exponential number of monomials and polynomially bounded degrees. Since the argument for Theorem 19 depends only on the polynomial's degree, but not on the number of monomials we obtain:

▶ **Theorem 20.**
1. $\mathrm{EC}(\cup, \cap, +, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cup, \cap, +, \times)$.
2. $\mathrm{EC}(\cup, \cap, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cup, \cap, \times)$.

From known results on $\mathrm{MC}(\cap, +, \times)$ and $\mathrm{MC}(\cap, \times)$ [22] and Theorem 6 we obtain:

▶ **Corollary 21.**
1. $\mathrm{EC}(\cap, +, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cap, +, \times) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{MC}(\cap, +, \times)} \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{EQ}(+, \times)}$.
2. Σ_1-$\mathrm{EC}(\cap, +, \times) \in \mathrm{RP}$.
3. Σ_1-$\mathrm{EC}(\cup, \cap, +, \times)$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* coNEXP.
4. Σ_1-$\mathrm{EC}(\cap, \times) \in \mathrm{P}$.
5. $\mathrm{EC}(\cap, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cap, \times) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{MC}(\cap, \times)}$.
6. Σ_1-$\mathrm{EC}(\cup, \cap, \times)$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* PSPACE.

The 5th statement shows that improving the non-matching bounds for $\mathrm{EC}(\cap, \times)$ is as difficult as improving the bounds for $\mathrm{MC}(\cap, \times)$, which is an open problem from [22].

5.5 Connection to Polynomial Identity Testing

We extend the equivalence in statement 1 of Corollary 21 by $\mathrm{EC}_{\mathbb{Z}}(\cap, +, \times)$, $\Sigma_1\text{-}\mathrm{EC}_{\mathbb{Z}}(\cap, +, \times)$, $\overline{\mathrm{MC}_{\mathbb{Z}}(\cap, +, \times)}$, $\overline{\mathrm{MC}_{\mathbb{Z}}(+, \times)}$, and $\overline{\mathrm{PIT}}$. The connection to PIT is interesting as it explains the difficulty of several open questions, namely the non-matching lower and upper bounds of $\mathrm{MC}(\cap, +, \times)$ in [22], $\mathrm{MC}_{\mathbb{Z}}(\cap, +, \times)$ and $\mathrm{MC}_{\mathbb{Z}}(+, \times)$ in [32], and $\mathrm{EQ}(+, \times)$ in [11]. In addition, it settles the question for the complexity of $\mathrm{EC}(\cap, +, \times)$ and $\Sigma_1\text{-}\mathrm{EC}(\cap, +, \times)$.

PIT (polynomial identity testing) is the following problem: For a given integer circuit consisting of input gates associated with variables/constants from $\mathbb{Z}$ and internal gates for addition/multiplication over $\mathbb{Z}$, one has to decide whether the polynomial described by the circuit is identically zero or not. The term *identically zero* means that the polynomial must be formally zero, i.e., if we write it as a linear combination of monomials with coefficients from $\mathbb{Z}$, then all coefficients are zero. For the ring $\mathbb{Z}$ this is equivalent to requiring that the polynomial is zero on $\mathbb{Z}^n$, where n is the number of unassigned input gates. (For other rings this makes a difference: for example over $\mathbb{F}_2$, the polynomial $x^2 + x$ is not identically zero, although it is zero on $\mathbb{F}_2$.) Formally, we can define PIT as the following problem concerning $\{+, \times\}$-circuits over $\mathbb{Z}$:

$$\begin{aligned}\mathrm{PIT} \overset{\mathit{df}}{=} \{\, C \mid {} & C \text{ is a } \{+,\times\}\text{-circuit with unassigned inputs } u_1 < \cdots < u_n \text{ such that}\\ & \text{the assigned inputs have labels from } \mathbb{Z} \text{ and for all } x_1, \dots, x_n \in \mathbb{Z} \text{ it holds}\\ & \text{that } I(C(x_1, \dots, x_n)) = \{0\} \,\}.\end{aligned}$$

It is known that PIT $\in$ coRP [15], but proving the exact complexity of PIT is considered as one of the greatest challenges in algebraic computing complexity [26] and theoretical computer science in general [29]. This fundamental problem has many applications, e.g., a deterministic primality test [1]. For further background on PIT we refer to the articles [26, 29, 27, 19]. Let $\mathcal{PIT}$ denote the class of problems that are $\leq_{\mathrm{m}}^{\log}$-reducible to PIT.

▶ **Theorem 22.** $\mathrm{EC}(\cap,+,\times) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{MC}(\cap,+,\times)} \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{EQ}(+,\times)} \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{PIT}} \equiv_{\mathrm{m}}^{\log} \mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)$.

We sketch the proof: By Corollary 21, $\mathrm{EC}(\cap,+,\times) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{MC}(\cap,+,\times)} \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{EQ}(+,\times)}$. Theorem 19 implies $\overline{\mathrm{EQ}(+,\times)} \leq_{\mathrm{m}}^{\log} \overline{\mathrm{PIT}} \leq_{\mathrm{m}}^{\log} \Sigma_1\text{-}\,\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times) \leq_{\mathrm{m}}^{\log} \mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)$. It remains to show $\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times) \leq_{\mathrm{m}}^{\log} \mathrm{EC}(\cap,+,\times)$.

We simulate a $\{\cap,+,\times\}$-circuit C over $\mathbb{Z}$ by a $\{\cap,+,\times\}$-circuit C' over $\mathbb{N}$ such that the value $v \in \mathbb{Z}$ computed in gate i of C is represented in C' by two positive numbers $\widetilde{i} + v$ and $\widetilde{i} - v$, where $\widetilde{i} = 2^{3^i}$. This shift by $\widetilde{i}$ allows $\{\cap,+,\times\}$-circuits over $\mathbb{N}$ to represent numbers from $\mathbb{Z}$. A technical elaboration shows that the circuits can also *process* numbers represented in this way, i.e., there are subcircuits that simulate the operations $\cap$, $+$, and $\times$.

Together with the Theorems 19 and 22 we obtain:

▶ **Corollary 23.** *The following problems are $\leq_{\mathrm{m}}^{\log}$-equivalent to $\overline{\mathrm{PIT}}$:* $\mathrm{EC}(\cap,+,\times)$, $\Sigma_1\text{-}\,\mathrm{EC}(\cap,+,\times)$, $\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)$, $\Sigma_1\text{-}\,\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)$, $\overline{\mathrm{MC}_{\mathbb{Z}}(\cap,+,\times)}$, $\overline{\mathrm{MC}_{\mathbb{Z}}(+,\times)}$.

The equivalence to $\overline{\mathrm{PIT}}$ shows the difficulty of understanding the complexity of the problems $\mathrm{EC}(\cap,+,\times)$ and $\Sigma_1\text{-}\,\mathrm{EC}(\cap,+,\times)$ as well as the open problems from [22, 32, 11] mentioned above. Kabanets and Impagliazzo [16] substantiate the hardness of obtaining subexponential algorithms for PIT by showing that it implies that NEXP $\not\subseteq$ P/poly or the permanent is not computable by polynomial size arithmetic circuits over $\mathbb{Q}$ with divisions. Both statements are expected to be difficult to prove.

In view of Theorem 22 it seems unlikely that $\mathrm{EQ}(\cap,+,\times)$ is equivalent to PIT: A straightforward proof shows that $\mathrm{EQ}(\cap,+,\times)$ is $\leq_{\mathrm{m}}^{\log}$-complete for $\mathcal{PIT} \vee \mathrm{co}\mathcal{PIT} = \{L \cup L' \mid L \in \mathcal{PIT}, L' \in \mathrm{co}\mathcal{PIT}\}$, which is the complement of the second level of the Boolean hierarchy [18] over $\mathcal{PIT}$. If $\mathrm{EQ}(\cap,+,\times) \equiv_{\mathrm{m}}^{\log} \mathrm{PIT}$, then $\mathcal{PIT} = \mathcal{PIT} \vee \mathrm{co}\mathcal{PIT}$ and hence $\mathrm{PIT} \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{PIT}} \in \mathrm{RP} \subseteq \mathrm{NP}$. Kabanets and Impagliazzo [16] show that PIT $\in$ NP is unlikely, since it implies NEXP$\cap$coNEXP $\not\subseteq$ P/poly or the permanent is not computable by polynomial-size arithmetic circuits over $\mathbb{Q}$ with divisions. This also explains the difficulty of improving the upper bound for $\mathrm{EQ}(\cap,+,\times)$ from BPP [11] to coRP, since this implies $\overline{\mathrm{PIT}} \leq_{\mathrm{m}}^{\log} \mathrm{EQ}(\cap,+,\times) \in \mathrm{coRP}$.

6 Conclusions and Open Questions

The results of this paper are summarized in Table 1. For most of the emptiness problems it was possible to precisely characterize their complexity.

Table 1 Upper bounds mean membership in the class, lower bounds stand for $\leq_m^{\log}$-hardness for the class. Numbers refer to results in this paper. Gray cells do not contain references, since by statement 5 of Lemma 2 these results are obtained from white cells. Subsets $\mathcal{O}$ that are missing in the first column either correspond to trivial problems (statement 3 of Lemma 2) or can be transformed by De Morgan's law to an equivalent subset (statement 4 of Lemma 2). $\mathcal{PIT}$ is the class of problems that are logspace many-one reducible to polynomial identity testing, which is a well-studied problem in algebraic computing complexity. It is known that $\mathrm{P} \subseteq \mathcal{PIT} \subseteq \mathrm{coRP}$ and it is an open problem to improve these bounds.

$\mathcal{O}$	EC l.b.	EC u.b.	Σ_1-EC l.b.	Σ_1-EC u.b.	Π_1-EC l.b.	Π_1-EC u.b.
$\cap$	NL, 4	NL	NL	NL, 4	NL	NL, 4
$\cup\cap$	P, 4	P	P	P, 4	P	P, 4
$\cap +$	$\mathrm{coC_=L}$, 3	$\mathrm{coC_=L}$	$\mathrm{coC_=L}$	$\mathrm{coC_=L}$, 5	coNP, 6	coNP, 6
$\cap \times$	$\mathrm{coC_=L}$, 3	P	$\mathrm{coC_=L}$	P, 21	coNP, 3	coNP, 3
$^- +$	PSPACE, 13	PSPACE	PSPACE	2EXPSPACE	PSPACE	2EXPSPACE
$^- \times$	PSPACE, 13	PSPACE	PSPACE	3EXPSPACE	PSPACE	3EXPSPACE
$\cup\cap^-$	P	P, 4	NP, 4	NP, 4	coNP, 4	coNP, 4
$\cup\cap +$	PSPACE, 6	PSPACE	PSPACE	PSPACE, 6	PSPACE	PSPACE, 6
$\cup\cap\times$	PSPACE, 6	PSPACE	PSPACE	PSPACE, 21	PSPACE	PSPACE, 6
$\cap + \times$	co$\mathcal{PIT}$, 22	co$\mathcal{PIT}$	co$\mathcal{PIT}$	co$\mathcal{PIT}$, 23	Π_1, 14	Π_1
$^- + \times$	PSPACE	$\mathcal{R}_{tt}(\Sigma_1)$	Σ_1, 14	Σ_2	Π_1, 14	Π_2
$\cup\cap^-+$	PSPACE	PSPACE, 3	PSPACE	2EXPSPACE, 8	PSPACE	2EXPSPACE, 8
$\cup\cap^-\times$	PSPACE	PSPACE, 3	PSPACE	3EXPSPACE, 8	PSPACE	3EXPSPACE, 8
$\cup\cap+\times$	coNEXP, 3	coNEXP	coNEXP	coNEXP, 21	Π_1	Π_1, 14
$\cup\cap^-+\times$	$\mathrm{L}^{\mathrm{NEXP}}$, 16	$\mathcal{R}_{tt}(\Sigma_1)$, 14	Σ_1	Σ_2, 14	Π_1	Π_2, 14

The results provide insights and improved complexity bounds for the following problems: $\mathrm{MC}(\cup,\cap,^-,+,\times), \mathrm{MC}(\cap,+,\times)$ studied in [22], $\mathrm{MC}_{\mathbb{Z}}(+,\times), \mathrm{MC}_{\mathbb{Z}}(\cap,+,\times)$ studied in [32], and $\mathrm{EQ}(\cup,\cap,^-,+,\times), \mathrm{EQ}(+,\times), \mathrm{EQ}(\cap,+,\times)$ studied in [11].

A challenging open problem is to improve the bounds for the problems $\mathrm{EC}(^-,+,\times)$ and $\mathrm{EC}(\cup,\cap,^-,+,\times)$. Here the state of knowledge is as follows (cf. Propositions 15, 17, and Corollary 16):

1. Both problems are equivalent to problems investigated in [22, 11]: $\mathrm{EC}(^-,+,\times) \equiv_m^{\log} \mathrm{MC}(^-,+,\times)$ and $\mathrm{EC}(\cup,\cap,^-,+,\times) \equiv_m^{\log} \mathrm{MC}(\cup,\cap,^-,+,\times) \equiv_m^{\log} \mathrm{EQ}(\cup,\cap,^-,+,\times)$.
2. Finding a decision algorithm and proving its correctness is at least as difficult as showing that Goldbach's conjecture is provable or refutable, which is an open problem.
3. The problems are either decidable or outside $\Sigma_1 \cup \Pi_1$.
4. The problems are $\leq_m$-hard for Σ_1 if and only if they are $\leq_m$-complete for $\mathcal{R}_{tt}(\Sigma_1)$.

Another open problem is to improve the complexity bounds whenever we have one of the classes 2EXPSPACE and 3EXPSPACE as upper bound. The latter are consequences of the decidability of the Presburger and Skolem arithmetic. It is possible that more specific proof techniques can improve these bounds. By Lemma 2, Π_1-$\mathrm{EC}(\cup,\cap,^-,\times)$ is equivalent to the complement of Σ_1-$\mathrm{MC}(\cup,\cap,^-,\times)$, which has already been investigated in [13, 12].

A third open problem is to improve the bounds for $\mathrm{EC}(\cap,\times)$ and Σ_1-$\mathrm{EC}(\cap,\times)$. Both problems are equivalent to $\mathrm{MC}(\cap,\times)$, which has already been studied in [22].

Acknowledgements. We thank Klaus Reinhardt for sharing an unpublished proof for the $\leq_m^{p}$-hardness of $\mathrm{MC}(^-,\times)$ for PSPACE, which we slightly adapted to show the $\leq_m^{\log}$-hardness of $\mathrm{MC}^+(^-,+)$ for PSPACE (Lemma 10), and for helpful discussions on the $\leq_m^{\log}$-hardness of MC($^{-}, +$) for PSPACE (Theorem 11). Moreover, we thank Jakob Sigmund for helpful discussions and contributions to the proof of Theorem 12.

References

1 M. Agrawal, N. Kayal, and N. Saxena. Primes is in P. *Annals of Mathematics*, 160:781–793, 2004.

2 E. Allender. Making computation count: Arithmetic circuits in the nineties. *SIGACT NEWS*, 28(4):2–15, 1997.

3 E. Allender and M. Ogihara. Relationships among PL, #L, and the determinant. *RAIRO Theoretical Informatics and Applications*, 30:1–21, 1996.

4 D. Barth, M. Beck, T. Dose, C. Glaßer, L. Michler, and M. Technau. Emptiness problems for integer circuits. Technical Report 17-012, Electronic Colloquium on Computational Complexity (ECCC), 2017.

5 A. Bès. A survey of arithmetical definability. *Soc. Math. Belgique*, pages 1–54, 2002.

6 H. Breunig. The complexity of membership problems for circuits over sets of positive numbers. In *International Symposium on Fundamentals of Computation Theory*, volume 4639 of *Lecture Notes in Computer Science*, pages 125–136. Springer, 2007.

7 M. Davis, H. Putnam, and J. Robinson. The decision problem for exponential Diophantine equations. *Annals of Mathematics*, 74(2):425–436, 1961.

8 T. Dose. Complexity of constraint satisfaction problems over finite subsets of natural numbers. In *41st International Symposium on Mathematical Foundations of Computer Science*, volume 58 of *Leibniz International Proceedings in Informatics*, pages 32:1–32:13. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2016.

9 J. Ferrante and C. Rackoff. A decision procedure for the first order theory of real addition with order. *SIAM J. Comput.*, 4:69–76, 1975.

10 J. Ferrante and C. W. Rackoff. *The Computational Complexity of Logical Theories*, volume 718 of *Lecture Notes in Mathematics*. Springer Verlag, 1979.

11 C. Glaßer, K. Herr, C. Reitwießner, S. D. Travers, and M. Waldherr. Equivalence problems for circuits over sets of natural numbers. *Theory of Computing Systems*, 46(1):80–103, 2010.

12 C. Glaßer, P. Jonsson, and B. Martin. Circuit satisfiability and constraint satisfaction around skolem arithmetic. In *12th Conference on Computability in Europe*, volume 9709 of *Lecture Notes in Computer Science*, pages 323–332. Springer, 2016.

13 C. Glaßer, C. Reitwießner, S. D. Travers, and M. Waldherr. Satisfiability of algebraic circuits over sets of natural numbers. *Discrete Applied Mathematics*, 158(13):1394–1403, 2010.

14 E. Grädel. Dominoes and the complexity of subclasses of logical theories. *Annals of Pure and Applied Logic*, 43(1):1–30, 1989.

15 O. Ibarra and S. Moran. Probabilistic algorithms for deciding equivalence of straight-line programs. *Journal of the ACM*, 30(1):217–228, 1983.

16 V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1):1–46, 2004.

17 D. E. Knuth. All questions answered. *Notices of the AMS*, 49(3):318–324, 2002.

18 J. Köbler, U. Schöning, and K. W. Wagner. The difference and the truth-table hierarchies for NP. *RAIRO Inform. Théor.*, 21:419–435, 1987.

19 D. König and M. Lohrey. Parallel identity testing for skew circuits with big powers and applications. *CoRR*, abs/1502.04545, 2015.

20 R. J. Lipton and N. K. Vishnoi. Deterministic identity testing for multivariate polynomials. In *Proceedings of the 14th Symposium on Discrete Algorithms*, pages 756–760. ACM/SIAM, 2003.

21 Y. V. Matiyasevich. Enumerable sets are diophantine. *Doklady Akad. Nauk SSSR*, 191:279–282, 1970. Translation in Soviet Math. Doklady, 11:354–357, 1970.

22 P. McKenzie and K. W. Wagner. The complexity of membership problems for circuits over sets of natural numbers. *Computational Complexity*, 16(3):211–244, 2007.

23 C. M. Papadimitriou. *Computational complexity*. Addison-Wesley, Reading, Massachusetts, 1994.

24 I. Pratt-Hartmann and I. Düntsch. Functions definable by arithmetic circuits. In *Conference on Mathematical Theory and Computational Practice*, volume 5635 of *Lecture Notes in Computer Science*, pages 409–418. Springer, 2009.

25 K. Reinhardt, 2016. Personal communication.

26 N. Saxena. Progress on polynomial identity testing. *Electronic Colloquium on Computational Complexity (ECCC)*, 16:101, 2009.

27 N. Saxena. Progress on polynomial identity testing - II. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:186, 2013.

28 A. Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, Inc., New York, NY, USA, 1986.

29 A. Shpilka and A. Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, 2010.

30 J. Sigmund, 2016. Personal communication.

31 L. J. Stockmeyer and A. R. Meyer. Word problems requiring exponential time: Preliminary report. In *Proceedings of the Fifth Annual ACM Symposium on Theory of Computing*, STOC'73, pages 1–9, New York, NY, USA, 1973. ACM.

32 S. D. Travers. The complexity of membership problems for circuits over sets of integers. *Theoretical Computer Science*, 369(1-3):211–229, 2006.

33 K. Wagner. The complexity of problems concerning graphs with regularities (extended abstract). In *Proceedings of the Mathematical Foundations of Computer Science 1984*, pages 544–552, London, UK, UK, 1984. Springer-Verlag.

34 K. Yang. Integer circuit evaluation is PSPACE-complete. *Journal of Computer and System Sciences*, 63(2):288–303, 2001. An extended abstract of appeared at CCC 2000.