Electronic Colloquium on Computational Complexity, Report No. 12 (2017)

Emptiness Problems for Integer Circuits

Dominik Barth Moritz Beck Titus Dose Christian Glaßer
Larissa Michler Marc Technau

Julius-Maximilians-Universität Würzburg
Germany

17th January 2017

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 well-studied, major open problem in algebraic computing complexity:

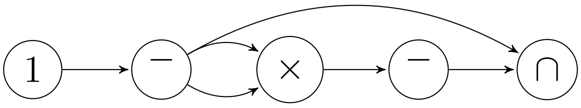
- membership problem $\mathrm{MC}(\cap, +, \times)$ studied by McKenzie and Wagner 2007
- integer membership problems $\mathrm{MC}_{\mathbb{Z}}(+, \times)$, $\mathrm{MC}_{\mathbb{Z}}(\cap, +, \times)$ studied by Travers 2006
- equivalence problem $\mathrm{EQ}(+, \times)$ studied by Glaßer et al. 2010

1 Introduction

Stockmeyer and Meyer [SM73] defined and investigated membership and equivalence problems for *integer expressions.* They considered expressions built up from single natural numbers by using set operations (${}^{-}$, $\cup$, $\cap$), pairwise addition (+), and pairwise multiplication (×). For example, the integer expression $\overline{\overline{1} \times \overline{1}} \cap \overline{1}$ describes the set of primes $\mathbb{P}$.

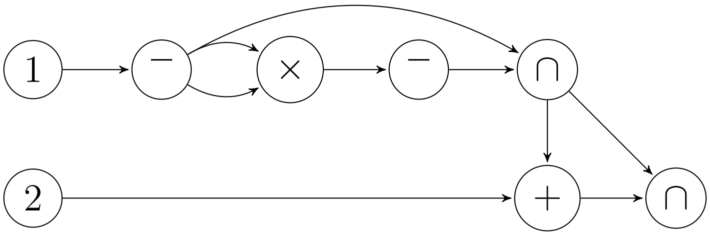
The *membership problem for integer expressions* is the question of whether the set described by a given integer expression contains some given natural number. The *equivalence problem for integer expressions* asks whether two given integer expressions describe the same set. Restricting the set of allowed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

Wagner [Wag84] introduced *circuits over sets of natural numbers.* These circuits describe integer expressions in a more 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 (+, ×). The following circuit has only 4 inner gates and describes the set of primes.



ISSN 1433-8092

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 [Wag84], Yang [Yan01], and McKenzie and Wagner [MW07] 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 n belongs to the set described by C. Travers [Tra06] and Breunig [Bre07] considered membership problems for circuits over integers ($\mathrm{MC}_{\mathbb{Z}}$) and positive integers ($\mathrm{MC}_{\mathbb{N}^+}$), respectively. Glaßer et al [GHR$^+$10] 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 [GRTW10], are a generalization of the membership problems investigated by McKenzie and Wagner [MW07]: Here the circuits can have *unassigned input gates*. The question is, given a circuit C with gate labels from $\mathcal{O} \subseteq \{\cup, \cap, ^-, +, \times\}$, and given a natural number n, does there exist an assignment of natural numbers to the variable input gates such that n 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 [PD09] and constraint satisfaction problems over natural numbers [GJM16, Dos16].

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 some given circuit C with gate labels 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 Figure 2 in Section 7.

The case of $\mathrm{EC}(\cap, +, \times)$ is particularly interesting. We show that it is logspace many-one equivalent to the complement of the well-known 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 an existential quantifier (the existence of assignments where the polynomial is non-zero), while $\mathrm{EC}(\cap, +, \times)$ does not. Second, PIT is defined over $\mathbb{Z}$, while $\mathrm{EC}(\cap, +, \times)$ is defined over $\mathbb{N}$.

To show the connection to PIT and to obtain upper bounds for Σ_1-$\mathrm{EC}(\mathcal{O})$ and Π_1-$\mathrm{EC}(\mathcal{O})$ it is favorable to estimate the smallest assignments that makes the circuit empty or non-empty, respectively. If $\times$ and $^-$ are not available (e.g., Π_1-$\mathrm{EC}(\cap, +) \in \mathrm{coNP}$ in Theorem 20), then this estimate is obtained by using 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. If $+$ and $\times$ are both available, (e.g., $\mathrm{EC}(\cap, +, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cap, +, \times)$ in Corollary 54), then we exploit the fact that the test of whether a multivariate polynomial is identically zero is possible by evaluating this polynomial for one fixed, but large argument. If Boolean operations and one arithmetic operation is available, (e.g., $\Sigma_1\text{-EC}(\cup, \cap, ^{-}, +) \in$ 2EXPSPACE and $\Sigma_1\text{-EC}(\cup, \cap, ^{-}, \times) \in$ 3EXPSPACE in Theorem 31), then we obtain upper bounds for the complexity by applying the decidability of Presburger and Skolem arithmetic.

Regarding our most general problem $\mathrm{EC}(\cup, \cap, ^{-}, +, \times)$ we show that it is logspace many-one equivalent to $\mathrm{MC}(\cup, \cap, ^{-}, +, \times)$ and $\mathrm{EQ}(\cup, \cap, ^{-}, +, \times)$, it belongs to $\mathcal{R}_{\mathrm{tt}}(\Sigma_1)$, and is $\leq_{\mathrm{m}}^{\log}$-hard for $\mathrm{L}^{\mathrm{NEXP}}$. We leave open whether $\mathrm{EC}(\cup, \cap, ^{-}, +, \times)$ is decidable and we explain the difficulty of this question: Finding a decision algorithm is at least as difficult as solving Goldbach's conjecture.

Our contribution to questions from previous work. Our results on emptiness problems provide new insights and improved bounds for some problems studied in the literature.

By the equivalence mentioned above, our bounds for $\mathrm{EC}(\cup, \cap, ^{-}, +, \times)$ improve the bounds for $\mathrm{MC}(\cup, \cap, ^{-}, +, \times)$ [MW07] and $\mathrm{EQ}(\cup, \cap, ^{-}, +, \times)$ [GHR+10] 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 $\mathrm{MC}(\cap, +, \times)$ studied in [MW07], $\mathrm{MC}_{\mathbb{Z}}(+, \times), \mathrm{MC}_{\mathbb{Z}}(\cap, +, \times)$ studied in [Tra06], and $\mathrm{EQ}(+, \times)$ studied in [GHR+10]. This characterizes the complexity of these problems and shows that the challenge to improve their known bounds is a reformulation of a well-studied, major open problem in algebraic computing complexity.

Finally we show that $\mathrm{EQ}(\cap, +, \times)$ 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 also explains the difficulty of improving the known upper bound [GHR+10].

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, NP, PSPACE, and NEXP denote standard complexity classes [Pap94]. 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 [All97].

Let Σ_i and Π_i denote the levels of the arithmetical hierarchy. Moreover we use the classes

$$\mathrm{2EXPSPACE} = \bigcup_{k \geq 1} \mathrm{DSPACE}\left(2^{2^{n^k}}\right) \qquad \text{and} \qquad \mathrm{3EXPSPACE} = \bigcup_{k \geq 1} \mathrm{DSPACE}\left(2^{2^{2^{n^k}}}\right).$$

For complexity classes $\mathcal{C}$ and $\mathcal{C}'$ let $\mathrm{co}\mathcal{C} = \{\overline{A} \mid A \in \mathcal{C}\}$, $\mathcal{C} \wedge \mathcal{C}' = \{A \cap B \mid A \in \mathcal{C}, B \in \mathcal{C}'\}$, and $\mathcal{C} \vee \mathcal{C}' = \{A \cup B \mid A \in \mathcal{C}, B \in \mathcal{C}'\}$. We denote by K the Σ_1-complete halting problem (for some fixed Gödelization).

The arithmetical operations $+$ and $\cdot$ 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 $c_A(x) = \max\{c_B(y_1), c_B(y_2), \ldots, c_B(y_n)\}$. The logspace conjunctive-truth-table reducibility $\leq_{\mathrm{ctt}}^{\log}$ is defined analogously. A is logspace many-one reducible to B ($A \leq_{\mathrm{m}}^{\log} B$), if there exists a logarithmic-space-computable function f such that $c_A(x) = c_B(f(x))$.

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, non-empty, 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. This requirement helps us to compare circuit problems with respect to logspace many-one reducibility, since in logarithmic space one can test the topological ordering and hence the validity of the input (i.e., the property that we are given an acyclic graph). Moreover, w.l.o.g. we may assume that $V = \{1, \ldots, r\}$ for some $r \in \mathbb{N}$, since circuits can be renumbered in logarithmic space.

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. If g is some gate of C with predecessors g', g'' and $\otimes = \alpha(g)$, then we also write $g = g' \otimes g''$. If g has indegree 1 and predecessor g' we write $g = \overline{g'}$.

In addition to the remark regarding the topological ordering we state that there is a deterministic algorithm which on input of a graph decides in logarithmic space whether the input is an encoding of a partially or completely 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 $i = 1, \ldots, n$.

Starting from a completely assigned $\mathcal{O}$-circuit $C = (V, E, g_C, \alpha)$, we inductively define the *set $I(g; C)$ computed by a gate $g \in V$* for $g = 1, \ldots, |V|$ by

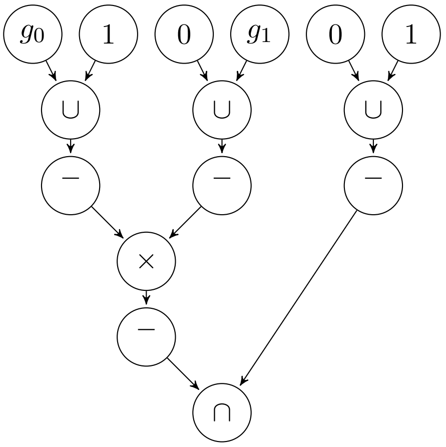
$$I(g; C) = \begin{cases} \{\alpha(g)\} \subseteq \mathbb{N} & \text{if } g \text{ has indegree } 0, \\ \mathbb{N} \setminus I(g', C) & \text{if } g = \overline{g'}, \\ I(g', C) \otimes I(g'', C) & \text{if } g = g' \otimes g''. \end{cases}$$

The *set computed by* C is defined as $I(C) = I(g_C; C)$. In some cases we consider circuits C with both assigned and unassigned inputs from $\mathbb{Z}$. Here, the sets $I(g; C)$ for a gate g and the set $I(C)$ are defined analogously (the complement is defined with respect to $\mathbb{Z}$ instead of $\mathbb{N}$).

Basic constructions. It is convenient to introduce notations for basic constructions of circuits. For $x \in \mathbb{N}$ we use x as an abbreviation for the circuit $(\{1\}, \varnothing, \{1\}, 1 \mapsto x)$. For $\mathcal{O}$-circuits C, C' for some $\mathcal{O}$ and $\otimes \in \{\cup, \cap, +, \times\}$ let $C \otimes C'$ be the circuit obtained from C' and C'' by feeding their output gates to the new output gate $\otimes$. This construction is possible in logarithmic space. Similarly, we define $\overline{C}$ to be the circuit obtained from C by adding a new output gate with label $^-$.

As an example, for unassigned inputs g_0 and g_1, consider the circuit

$$C = \overline{\overline{g_0 \cup \{1\}} \times \overline{\{0\} \cup g_1}} \cap \overline{\{0\} \cup \{1\}}.$$



Note that the circuit $C(0, 1)$ computes the set of all prime numbers.

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

$$\begin{aligned}
\mathrm{MC}(\mathcal{O}) &\overset{\text{df}}{=} \{(C, b) \mid C \textit{ is a completely assigned } \mathcal{O}\textit{-circuit and } b \in I(C)\} \\
\Sigma_1\text{-}\mathrm{MC}(\mathcal{O}) &\overset{\text{df}}{=} \{(C, b) \mid C \textit{ is a partially assigned } \mathcal{O}\textit{-circuit } u_1 < \cdots < u_n \textit{ and there} \\
&\qquad\qquad \textit{exist } x_1, \ldots, x_n \in \mathbb{N} \textit{ such that } b \in I(C(x_1, \ldots, x_n))\} \\
\mathrm{EQ}(\mathcal{O}) &\overset{\text{df}}{=} \{(C_1, C_2) \mid C_1, C_2 \textit{ are completely assigned } \mathcal{O}\textit{-circuits and } I(C_1) = I(C_2)\}^{1} \\
\mathrm{EC}(\mathcal{O}) &\overset{\text{df}}{=} \{C \mid C \textit{ is a completely assigned } \mathcal{O}\textit{-circuit and } I(C) = \emptyset\} \\
\Sigma_1\text{-}\mathrm{EC}(\mathcal{O}) &\overset{\text{df}}{=} \{C \mid C \textit{ is a partially assigned } \mathcal{O}\textit{-circuit with unassigned inputs } u_1 < \cdots < u_n \\
&\qquad\qquad \textit{and there exist } x_1, \ldots, x_n \in \mathbb{N} \textit{ such that } I(C(x_1, \ldots, x_n)) = \emptyset\} \\
\Pi_1\text{-}\mathrm{EC}(\mathcal{O}) &\overset{\text{df}}{=} \{C \mid C \textit{ is a partially assigned } \mathcal{O}\textit{-circuit with unassigned inputs } u_1 < \cdots < u_n \\
&\qquad\qquad \textit{and for all } x_1, \ldots, x_n \in \mathbb{N} \textit{ we have } I(C(x_1, \ldots, x_n)) = \emptyset,\ n \in \mathbb{N}\} \\
\Sigma_1\text{-}\mathrm{NEC}(\mathcal{O}) &\overset{\text{df}}{=} \overline{\Pi_1\text{-}\mathrm{EC}(\mathcal{O})}
\end{aligned}$$

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

[1] In [GHR$^+$10], 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 General Reductions between Circuit Classes

This section provides easy reductions and equivalences between the problems $\mathrm{EC}(\mathcal{O})$, Σ_1-$\mathrm{EC}(\mathcal{O})$, Π_1-$\mathrm{EC}(\mathcal{O})$, and $\mathrm{MC}(\mathcal{O})$.

Lemma 2. *Let $\mathcal{O} \subseteq \{\cup, \cap, {}^-, +, \times\}$. Then the following holds:*

1. *If $\cap \in \mathcal{O}$, then $\mathrm{MC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \overline{\mathrm{EC}(\mathcal{O})}$ and Σ_1-$\mathrm{MC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \Sigma_1$-$\mathrm{NEC}(\mathcal{O})$.*
2. *If $\times \in \mathcal{O}$, then $\overline{\mathrm{EC}(\mathcal{O})} \leq_{\mathrm{m}}^{\log} \mathrm{MC}(\mathcal{O})$ and Σ_1-$\mathrm{NEC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \Sigma_1$-$\mathrm{MC}(\mathcal{O})$.*

Proof. 1. follows directly from the observation

$$(C, d) \in \mathrm{MC}(\mathcal{O}) \iff d \in I(C) \iff I(C \cap [d]) \neq \emptyset \iff C \cap [d] \in \overline{\mathrm{EC}(\mathcal{O})}.$$

2. is a consequence of the equivalence

$$C \in \overline{\mathrm{EC}(\mathcal{O})} \iff I(C) \neq \emptyset \iff 0 \in I(C \times [0]) \iff (C \times \{0\}, 0) \in \mathrm{MC}(\mathcal{O}).$$

□

Corollary 3. 1. *$\mathrm{EC}(\cap, +, \times)$ is $\leq_{\mathrm{m}}^{\log}$-hard for* P.

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

Proof. By Lemma 2, $\overline{\mathrm{EC}(\cap, +, \times)} \equiv_{\mathrm{m}}^{\log} \mathrm{MC}(\cap, +, \times)$, which is $\leq_{\mathrm{m}}^{\log}$-hard for P [MW07]. By Lemma 2, $\overline{\mathrm{EC}(\cup, \cap, +, \times)} \equiv_{\mathrm{m}}^{\log} \mathrm{MC}(\cup, \cap, +, \times)$, which is $\leq_{\mathrm{m}}^{\log}$-complete for NEXP [MW07]. □

Proposition 4. *If $\mathcal{O} \subseteq \{\cup, +, \times\}$ or $\mathcal{O} \subseteq \{{}^-\}$, then*

$$\mathrm{EC}(\mathcal{O}) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\mathcal{O}) \equiv_{\mathrm{m}}^{\log} \Pi_1\text{-}\mathrm{EC}(\mathcal{O}) \equiv_{\mathrm{m}}^{\log} \emptyset.$$

Proof. For such $\mathcal{O}$ and any $\mathcal{O}$-circuit C, the set $I(C)$ is always non-empty. □

Proposition 5. *For $\mathcal{O} \subseteq \{+, \times\}$ the following holds.*

1. *$\mathrm{EC}(\cup, {}^-\} \cup \mathcal{O}) \equiv_{\mathrm{m}}^{\log} \mathrm{EC}(\cap, {}^-\} \cup \mathcal{O}) \equiv_{\mathrm{m}}^{\log} \mathrm{EC}(\cup, \cap, {}^-\} \cup \mathcal{O})$,*
2. *Σ_1-$\mathrm{EC}(\cup, {}^-\} \cup \mathcal{O}) \equiv_{\mathrm{m}}^{\log} \Sigma_1$-$\mathrm{EC}(\cap, {}^-\} \cup \mathcal{O}) \equiv_{\mathrm{m}}^{\log} \Sigma_1$-$\mathrm{EC}(\cup, \cap, {}^-\} \cup \mathcal{O})$,*
3. *Π_1-$\mathrm{EC}(\cup, {}^-\} \cup \mathcal{O}) \equiv_{\mathrm{m}}^{\log} \Pi_1$-$\mathrm{EC}(\cap, {}^-\} \cup \mathcal{O}) \equiv_{\mathrm{m}}^{\log} \Pi_1$-$\mathrm{EC}(\cup, \cap, {}^-\} \cup \mathcal{O})$.*

Proof. This is immediate from De Morgan's laws. □

Proposition 6. *For $\mathcal{O} \subseteq \mathcal{O}' \subseteq \{\cup, \cap, {}^-, +, \times\}$ it holds that*

1. *$\mathrm{EC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \mathrm{EC}(\mathcal{O}')$,*
2. *Σ_1-$\mathrm{EC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \Sigma_1$-$\mathrm{EC}(\mathcal{O}')$,*
3. *Π_1-$\mathrm{EC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \Pi_1$-$\mathrm{EC}(\mathcal{O}')$,*
4. *$\mathrm{EC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \Sigma_1$-$\mathrm{EC}(\mathcal{O})$,*
5. *$\mathrm{EC}(\mathcal{O}) \leq_{\mathrm{m}}^{\log} \Pi_1$-$\mathrm{EC}(\mathcal{O})$.*

4 Circuits without Arithmetic Operations

In this section we consider those emptiness problems which solely admit set operations. Apart from the trivial problems, which belong to L, all problems are shown to be $\leq_{\mathrm{m}}^{\log}$-complete for one of the classes NL, P, NP, and coNP.

If we only allow intersection, then the emptiness problems turn out to be equivalent to the graph accessibility problem for directed graphs. The question basically is whether certain input nodes are connected with the output node.

Theorem 7. *$\mathrm{EC}(\cap)$, Σ_1-$\mathrm{EC}(\cap)$, and Π_1-$\mathrm{EC}(\cap)$ are $\leq_{\mathrm{m}}^{\log}$-complete for* NL*.*

Proof. By Proposition 6, it suffices to show the NL-hardness of $\mathrm{EC}(\cap)$ and the NL-membership of Σ_1-$\mathrm{EC}(\cap)$ and Π_1-$\mathrm{EC}(\cap)$.

$\mathrm{MC}(\cap)$ is $\leq_{\mathrm{m}}^{\log}$-complete for NL [MW07] and hence $\overline{\mathrm{MC}(\cap)}$ is $\leq_{\mathrm{m}}^{\log}$-hard for NL, since NL is closed under complement. By Lemma 2, $\overline{\mathrm{MC}(\cap)} \leq_{\mathrm{m}}^{\log} \mathrm{EC}(\cap)$. Thus $\mathrm{EC}(\cap)$ is $\leq_{\mathrm{m}}^{\log}$-hard for NL.

To obtain the NL-membership, note that the output of an $\{\cap\}$-circuit is the intersection of all input gates that are connected to the output node. It follows that a partially assigned $\{\cap\}$-circuit C is in Σ_1-$\mathrm{EC}(\cap)$ if and only if the output gate g_C is connected to at least two input gates, which are not assigned the same number, though both may have $\square$ as their label. Similarly, C is in Π_1-$\mathrm{EC}(\cap)$ if and only if there are at least two assigned input gates with different labels that are connected to g_C. Both properties can be tested in NL. □

Once union and intersection are available, it is possible to simulate the evaluation of monotone Boolean circuits and hence the corresponding problems are hard for P. As the sets of natural numbers associated to gates in the circuit are computable in polynomial time (they are finite or cofinite), we have $\mathrm{EC}(\mathcal{O}) \in \mathrm{P}$ for each $\mathcal{O} \subseteq \{\cup, \cap, {}^{-}\}$. For emptiness problems allowing partially assigned circuits it suffices to consider polynomially many assignments for the input gates in order to decide whether there is an assignment for which the circuit computes the empty set (resp., a non-empty set). Hence several problems can be shown to be P-complete.

Theorem 8. *$\mathrm{EC}(\cup, \cap, {}^{-})$, $\mathrm{EC}(\cup, \cap)$, Σ_1-$\mathrm{EC}(\cup, \cap)$, and Π_1-$\mathrm{EC}(\cup, \cap)$ are $\leq_{\mathrm{m}}^{\log}$-complete for* P*.*

Proof. By Proposition 6 it suffices to show the following.

1. $\mathrm{EC}(\cup, \cap)$ is $\leq_{\mathrm{m}}^{\log}$-hard for P
2. $\mathrm{EC}(\cup, \cap, {}^{-}) \in \mathrm{P}$
3. Σ_1-$\mathrm{EC}(\cup, \cap) \in \mathrm{P}$
4. Π_1-$\mathrm{EC}(\cup, \cap) \in \mathrm{P}$

For statement 1, we reduce the monotone circuit value problem MCVP (which is $\leq_{\mathrm{m}}^{\log}$-complete for P [Gol77]) to the emptiness problem for $\{\cap, \cup\}$-circuits. If we identify *false* with $\{1\}$ and *true* with $\emptyset$, we observe that intersection acts like logical disjunction and union like logical conjunction. We describe the reduction function f that transforms a Boolean circuit into an integer circuit:

- Every input gate that is labeled *true* is replaced with the circuit $\{0\} \cap \{1\}$.
- Every input gate that is labeled *false* is replaced with an input gate labeled with 1.
- Every $\wedge$-gate is replaced with a $\cup$-gate.
- Every $\vee$-gate is replaced with an $\cap$-gate.

This reduction is computable in logarithmic space, since all replacements are of fixed size. By induction we obtain the following equivalence for all Boolean circuits C.

$$C \in \mathrm{MCVP} \Leftrightarrow C \text{ evaluates to true } \Leftrightarrow f(C) \text{ computes } \emptyset \Leftrightarrow f(C) \in \mathrm{EC}(\cup, \cap).$$

Thus $\mathrm{EC}(\cap, \cup)$ is $\leq_{\mathrm{m}}^{\log}$-hard for P.

For the second statement we make the following observation: In a $\{\cup, \cap, \overline{}\}$-circuit the set computed by a node has a linear-space representation, since it either contains only numbers that are labels of input nodes, or it is the complement of such a set. Therefore, the following algorithm works in polynomial time: Traverse the circuit, calculate the set computed by each gate, and check whether the set computed by the output gate is empty.

For statement 3, let C be a $\{\cup, \cap\}$-circuit with n unassigned input gates. Now consider the completely assigned circuit $C(x_1, \ldots, x_n)$, where the x_i are pairwise distinct numbers that are different from the labels of the other input gates. We argue that if $I(C(x_1, \ldots, x_n))$ is not empty, then any other assignment $y_1, \ldots, y_n$ of the unassigned gates will generate a non-empty output as well. For that purpose we prove the following stronger statement:

Claim 9. *For every gate v of C, $x_1, \ldots, x_n$ as above, and all $y_1, \ldots, y_n \in \mathbb{N}$ it holds that*

$$x_i \in I(v; C(x_1, \ldots, x_n)) \Longrightarrow y_i \in I(v; C(y_1, \ldots, y_n)) \text{ for } i \in \{1, \ldots, n\} \text{ and}$$
$$x \in I(v; C(x_1, \ldots, x_n)) \Longrightarrow x \in I(v; C(y_1, \ldots, y_n)) \text{ for } x \notin \{x_1, \ldots, x_n\}.$$

Proof of Claim 9. The statement is shown by induction on the structure of the circuit.

Base case (i.e., v is an input gate): If x_i is in $I(v; C(x_1, \ldots, x_n))$, then v has the label x_i and hence is the unique input gate with that label. Therefore, $I(v; C(y_1, \ldots, y_n))$ contains y_i. If $x \in I(v; C(x_1, \ldots, x_n))$ and $x \notin \{x_1, \ldots, x_n\}$, then v is some assigned input gate labeled with x. Hence v has label x also in $C(y_1, \ldots, y_n)$, which shows $x \in I(v; C(y_1, \ldots, y_n))$.

Inductive step: Let $v \in V$ be an arbitrary $\cup$-node with predecessors v_1, v_2 and $x_i \in I(v; C(x_1, \ldots, x_n)) = I(v_1; C(x_1, \ldots, x_n)) \cup I(v_2; C(x_1, \ldots, x_n))$. Without loss of generality we assume $x_i \in I(v_1; C(x_1, \ldots, x_n))$. By the induction hypothesis, $y_i \in I(v_1; C(y_1, \ldots, y_n))$. This implies $y_i \in I(v_1; C(y_1, \ldots, y_n)) \cup I(v_2; C(y_1, \ldots, y_n)) = I(v; C(y_1, \ldots, y_n))$. For $\cap$-nodes we argue analogously: Let $v \in V$ be an arbitrary $\cap$-node with predecessors v_1, v_2 and $x_i \in I(v; C(x_1, \ldots, x_n) = I(v_1; C(x_1, \ldots, x_n)) \cap I(v_2; C(x_1, \ldots, x_n))$. Hence $x_i \in I(v_1; C(x_1, \ldots, x_n))$ and $x_i \in I(v_2; C(x_1, \ldots, x_n))$. By the induction hypothesis, $y_i \in I(v_1; C(y_1, \ldots, y_n))$ and $y_i \in I(v_2; C(y_1, \ldots, y_n))$. Hence $y_i \in I(v_1; C(y_1, \ldots, y_n)) \cap I(v_2; C(y_1, \ldots, y_n)) = I(v; C(y_1, \ldots, y_n))$.

The inductive step for the second implication can be shown analogously. □

The claim shows that we can test whether a partially assigned circuit is in Σ_1-$\mathrm{EC}(\cup, \cap)$ by evaluating the completely assigned circuit with the described labeling. By statement 2, this can be done in polynomial time.

Finally we turn to statement 4. Suppose that we are given a circuit $C \in \Sigma_1$-$\mathrm{NEC}(\cup, \cap)$ with n unassigned input gates. Then there are $x_1, \ldots, x_n \in \mathbb{N}$ such that $I(C(x_1, \ldots, x_n)) \neq \emptyset$. Without loss of generality, $x_1, \ldots, x_n$ can be chosen from the set S of numbers that occur as labels of assigned input gates. It follows that there is an $x \in S \cap I(C(x_1, \ldots, x_n))$.

By induction on the structure of the circuit it can be argued that for each gate v of C it holds that $x \in I(v; C(x_1, \ldots, x_n)) \Longrightarrow x \in I(v; C(x, \ldots, x))$.

In particular, it holds $I(C(x, \ldots, x)) \neq \emptyset$. So, in order to check whether some given partially assigned $\{\cup, \cap\}$-circuit C is in Σ_1-$\mathrm{NEC}(\cup, \cap)$, it suffices to check whether there exists some $x \in S$ such that $C(x, \ldots, x) \notin \mathrm{EC}(\cap, \cup)$. As $\mathrm{EC}(\cup, \cap)$ is in P and the set S has not more than $|C|$ elements, we obtain Σ_1-$\mathrm{NEC}(\cup, \cap) \in \mathrm{P}$ and hence Π_1-$\mathrm{EC}(\cup, \cap) \in \mathrm{P}$. □

If $\mathcal{O}$ contains all three set operations, then Σ_1-EC($\mathcal{O}$) (resp., Π-EC($\mathcal{O}$)) can be shown to be NP-complete (resp., coNP-complete).

Theorem 10. *1.* Σ_1-EC$(\cup, \cap, ^-)$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* NP*.*

2. Π_1-EC$(\cup, \cap, ^-)$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* coNP*.*

Proof. 1. For a Boolean formula F, let C_F be the $\{\cup, \cap, ^-\}$-circuit obtained by replacing $\vee, \wedge, \neg$ with $\cup, \cap, ^-$ respectively. Observe that SAT $\leq_{\mathrm{m}}^{\log}$ Σ_1-EC$(\cup, \cap, ^-)$ via $F \mapsto \overline{C_F} \cap \{1\}$: If we interpret sets containing 1 as true and all other sets as false, then each satisfying assignment of F induces an assignment that generates the empty set in $\overline{C_F} \cap \{1\}$ and vice versa.

We now argue that Σ_1-EC$(\cup, \cap, ^-) \in$ NP. Let $C \in \Sigma_1$-EC$(\cup, \cap, ^-)$ with n unassigned inputs, assigned inputs $a_1, \ldots, a_m$, and labeling function α. Moreover, let $u_1, \ldots, u_n \in \mathbb{N}$ such that $C(u_1, \ldots, u_n) = \emptyset$. For $A = \{\alpha(a_1), \ldots, \alpha(a_m)\}$ and $B = \{1 + \max A, \ldots, n + \max A\}$ there exist $v_1, \ldots, v_n \in A \cup B$ such that $C(v_1, \ldots, v_n) = \emptyset$ (for all $u_i \in A \cup B$ let $v_i := u_i$, then choose the remaining v_i from B such that $v_i = v_j \Leftrightarrow u_i = u_j$). This shows $C \in \Sigma_1$-EC$(\cup, \cap, ^-)$ if and only if there exist $v_1, \ldots, v_n \in A \cup B$ such that $C(v_1, \ldots, v_n) = \emptyset$. Hence Σ_1-EC$(\cup, \cap, ^-) \in$ NP, since EC$(\cup, \cap, ^-) \in$ P by Theorem 8.

2. The proof is similar to the proof of 1, since $\overline{\text{SAT}} \leq_{\mathrm{m}}^{\log}$ Π_1-EC$(\cup, \cap, ^-)$ via $F \mapsto C_F \cap \{1\}$. □

5 Circuits with One Arithmetic Operation

We divide this section into two parts: the emptiness problems for circuits without complement and those with complement. Whereas we are able to show almost all of the problems of the first part to be complete for some natural complexity class, for most problems in the second part there are gaps between lower and upper bound. Generally, it holds that the complement increases the complexity of the problems as it is the only operation which "produces" infinite sets.

5.1 Circuits without Complement

In this section only those problems are relevant which admit the intersection. Otherwise the circuits compute always non-empty sets. We start with problems admitting intersection as the only set operation.

Theorem 11. *1.* EC$(\cap, \times)$ *is* $\leq_{\mathrm{m}}^{\log}$*-hard for* coC$_=$L*.*

2. EC$(\cap, +)$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* coC$_=$L*.*

3. Σ_1-EC$(\cap, +) \in$ coC$_=$L*.*

Proof. MC$(\cap, \times)$ is $\leq_{\mathrm{m}}^{\log}$-hard for C$_=$L [MW07] and MC$(\cap, \times) \leq_{\mathrm{m}}^{\log} \overline{\text{EC}(\cap, \times)}$ by Lemma 2. This proves the first statement. The second statement follows from [GHR$^+$10, Lemma 2].

For the third statement, let C be a partially assigned $\{\cap, +\}$-circuit with unassigned input gates $g_1 < \cdots < g_n$ and output gate g_C.

Claim 12. *For all $x, y, z, x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{N}$ and every gate g in C the following holds. If g computes the set $\{x\}$ in $C(x_1, \ldots, x_n)$, g computes the set $\{y\}$ in $C(y_1, \ldots, y_n)$, and g computes the set $\{z\}$ in $C(0, \ldots, 0)$, then g computes the set $\{x + y - z\}$ in $C(x_1 + y_1, \ldots, x_n + y_n)$.*

The claim is shown by induction on the structure of C.

If $g = g_i$ is an unassigned input gate, then it computes the sets $\{x_i\}$, $\{y_i\}$, $\{0\}$, and $\{x_i+y_i\} = \{x_i + y_i - 0\}$ in the circuits $C(x_1, \dots, x_n)$, $C(y_1, \dots, y_n)$, $C(0, \dots, 0)$, $C(x_1 + y_1, \dots, x_n + y_n)$, respectively. If g is an assigned input gate labeled with $c \in \mathbb{N}$, then of course it always computes the set $\{c\} = \{c + c - c\}$. This proves the induction base.

Now assume that g is an inner gate connected to the output with predecessors g_a and g_b. By assumption, g_a and g_b compute singletons in $C(x_1, \dots, x_n)$, $C(y_1, \dots, y_n)$, and $C(0, \dots, 0)$. These are denoted by $\{x_a\}$, $\{y_a\}$, $\{z_a\}$, $\{x_b\}$, $\{y_b\}$, and $\{z_b\}$. By induction hypothesis, g_a computes $\{x_a + y_a - z_a\}$ and g_b computes $\{x_b + y_b - z_b\}$ in $C(x_1 + y_1, \dots, x_n + y_n)$.

If g is an $\cap$-gate, then $x = x_a = x_b$, $y = y_a = y_b$, $z = z_a = z_b$, hence g_a and g_b both compute $\{x + y - z\}$ in $C(x_1 + y_1, \dots, x_n + y_n)$ and thus the same holds for g. If g is a $+$-gate, then $x = x_a+x_b$, $y = y_a+y_b$, $z = z_a+z_b$, and hence g computes $\{x_a+y_a-z_a+x_b+y_b-z_b\} = \{x+y-z\}$ in $C(x_1 + y_1, \dots, x_n + y_n)$. This proves Claim 12.

Claim 13. *$C \in \Sigma_1$-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* EC$(\cap, +)$.

The direction from right to left is trivial. For the other direction observe that if non of the circuits belongs to EC$(\cap, +)$, then by Claim 12, $C(x_1, \dots, x_n) \neq \emptyset$ for all $x_1, \dots, x_n \in \mathbb{N}$ and hence $C \notin \Sigma_1$-EC$(\cap, +)$. This proves Claim 13.

From Claim 13 it follows that $\overline{\Sigma_1\text{-EC}(\cap, +)} \leq^{\log}_{\text{ctt}} \overline{\text{EC}(\cap, +)} \in \text{C}_{=}\text{L}$. The statement follows, since $\text{C}_{=}\text{L}$ is closed under $\leq^{\log}_{\text{ctt}}$ [AO96, Proposition 17]. □

Proposition 14. *Π_1-EC$(\cap, \times)$ is $\leq^{\log}_{\text{m}}$-complete for* coNP.

Proof. The statement follows from the $\leq^{\log}_{\text{m}}$-completeness of Σ_1-MC$(\cap, \times)$ for NP [GRTW10] and Lemma 2. □

Results Obtained from Finding Small Solutions for Systems of Linear Equations The results in this paragraph are obtained due to the fact that there are small solutions for specific systems of linear equations. Our systems consist of arbitrarily many equations, yet each equation has to be short, i.e., there are not allowed to be many variables or large coefficients.

We first show Π_1-EC$(\cap, +) \in$ coNP. However, we define our systems of linear equations such that they can also be applied in the more general case where union is admitted.

Definition 15. *Let C be a $\{\cup, \cap, +\}$-circuit with n unassigned input gates $u_1 < \dots < u_n$ and assigned input gates $v_1, \dots, v_k$. We denote the unique element of $I(v_i)$ by ζ_i.*

For each node v of C we inductively define a finite set B_v of sets of linear terms. For this we introduce a variable x_i for each unassigned input node u_i. For each gate v the set B_v contains only sets of terms of the form $\sum_{i=1}^{n} \alpha_i x_i + \alpha_0$ with $\alpha_i \in \mathbb{N}$.

Basis: *Define $B_{v_i} = \{\{\zeta_i\}\}$ and $B_{u_i} = \{\{x_i\}\}$.*

Inductive step: *Let $\otimes \in \{\cup, \cap, +\}$. For each $\otimes$-node u with predecessors v and w we define:*

- *If $\otimes = \cup$, then $B_u \overset{df}{=} B_v \cup B_w$.*
- *If $\otimes = \cap$, then $B_u \overset{df}{=} \{A \cup B \mid A \in B_v, B \in B_w\}$.*
- *If $\otimes = +$, then $B_u \overset{df}{=} \{A + B \mid A \in B_v, B \in B_w\}$ where $A + B = \{t + t' \mid t \in A, t' \in B\}$ for sets of terms A and B.*

Furthermore, for each node v, all $a_1, \dots, a_n \in \mathbb{N}$ and each $A \in B_v$ we define

$$\begin{aligned}
L_{a_1,\dots,a_n}(A) &\overset{df}{=} \{y \in \mathbb{N} \mid \forall \big(\sum_{i=1}^{n} \alpha_i x_i + \alpha_0\big) \in A : \, y = \sum_{i=1}^{n} \alpha_i a_i + \alpha_0\} \\
L_{a_1,\dots,a_n}(B_v) &\overset{df}{=} \bigcup_{A \in B_v} L_{a_1,\dots,a_n}(A) \\
L(B_v) &\overset{df}{=} \bigcup_{a_1,\dots,a_n \in \mathbb{N}} L_{a_1,\dots,a_n}(B_v).
\end{aligned}$$

We see $A \neq \emptyset$ for each $A \in B_v$ and hence $L_{a_1,\dots,a_n}(A)$ is always a singleton or empty. In the first case it contains the unique number which is obtained by each of the terms in A when assigning a_i to x_i. The following lemma states that for an arbitrary node u the set $L_{a_1,\dots,a_n}(B_u)$ is equal to the set computed by u when a_i is assigned to u_i.

Lemma 16. *Let $\mathcal{O} \subseteq \{\cup, \cap, +\}$ and let $C = (V, E, g_C, \alpha)$ be an $\mathcal{O}$-circuit with unassigned input gates $u_1 < \cdots < u_n$. Then the following holds.*

1. *For each node u of C and all $a_1, \dots, a_n \in \mathbb{N}$ it holds that $L_{a_1,\dots,a_n}(B_u) = I(u; C(a_1, \dots, a_n))$.*
2. *For each node u of C it holds that $L(B_u) = \bigcup_{a_1,\dots,a_n \in \mathbb{N}} I(u; C(a_1, \dots, a_n))$.*
3. *The following statements are equivalent:*
   (a) $C \in \Sigma_1\text{-NEC}(\mathcal{O})$
   (b) $C \notin \Pi_1\text{-EC}(\mathcal{O})$
   (c) $L(B_{g_C}) \neq \emptyset$.
4. *The following statements are equivalent:*
   (a) $C \in \Sigma_1\text{-EC}(\mathcal{O})$
   (b) There are $a_1, \dots, a_n$ such that $L_{a_1,\dots,a_n}(B_{g_C}) = \emptyset$.

Proof. 1. We show the statement by structural induction over the definition of circuits. The statement is true for all input gates.

Let u be an arbitrary node with predecessors v and w. By induction hypothesis (ih) the statement is true for the nodes v and w, i.e., $L_{a_1,\dots,a_n}(B_v) = I(v; C(a_1, \dots, a_n))$ and $L_{a_1,\dots,a_n}(B_w) = I(w; C(a_1, \dots, a_n))$. In the following we distinguish three cases.

- u is a $\cup$-node: then it holds

$$\begin{aligned}
L_{a_1,\dots,a_n}(B_u) &= \bigcup_{A \in B_u} L_{a_1,\dots,a_n}(A) = \bigcup_{A \in B_v \cup B_w} L_{a_1,\dots,a_n}(A) \\
&= \bigcup_{A \in B_v} L_{a_1,\dots,a_n}(A) \cup \bigcup_{A \in B_w} L_{a_1,\dots,a_n}(A) = L_{a_1,\dots,a_n}(B_v) \cup L_{a_1,\dots,a_n}(B_w) \\
&\overset{\text{ih}}{=} I(v; C(a_1, \dots, a_n)) \cup I(w; C(a_1, \dots, a_n)) = I(u; C(a_1, \dots, a_n)).
\end{aligned}$$

- u is an $\cap$-node: We first observe that for sets of terms B and C and all $a_1, \dots, a_n \in \mathbb{N}$ it holds that $L_{a_1,\dots,a_n}(B \cup C) = L_{a_1,\dots,a_n}(B) \cap L_{a_1,\dots,a_n}(C)$. Furthermore, note that by definition, for each $A \in B_u$ there are $B \in B_v$ and $C \in B_w$ such that $A = B \cup C$. Conversely, for each $B \in B_v$ and $C \in B_w$ there is an $A \in B_u$ such that $A = B \cup C$.

Hence we obtain

$$\begin{aligned}
L_{a_1,\dots,a_n}(B_u) &= \bigcup_{A\in B_u} L_{a_1,\dots,a_n}(A) = \bigcup_{B\in B_v}\bigcup_{C\in B_w} L_{a_1,\dots,a_n}(B\cup C)\\
&= \bigcup_{B\in B_v}\bigcup_{C\in B_w} (L_{a_1,\dots,a_n}(B)\cap L_{a_1,\dots,a_n}(C))\\
&= \bigcup_{B\in B_v} L_{a_1,\dots,a_n}(B)\cap \bigcup_{C\in B_w} L_{a_1,\dots,a_n}(C) = L_{a_1,\dots,a_n}(B_v)\cap L_{a_1,\dots,a_n}(B_w)\\
&\overset{\text{ih}}{=} I(v;C(a_1,\dots,a_n))\cap I(w;C(a_1,\dots,a_n)) = I(u;C(a_1,\dots,a_n)).
\end{aligned}$$

- u is a +-node: For each $A\in B_u$ there are $B\in B_v$ and $C\in B_w$ such that $A=B+C$. Conversely, for each $B\in B_v$ and $C\in B_w$ there is an $A\in B_u$ with $A=B+C$. Thus, for all $a_1,\dots,a_n\in\mathbb{N}$ it holds that $\bigcup_{A\in B_u} L_{a_1,\dots,a_n}(A)=\bigcup_{B\in B_v}\bigcup_{C\in B_w} L_{a_1,\dots,a_n}(B+C)$.

Claim 17. *For non-empty sets of terms B and C and $a_1,\dots,a_n\in\mathbb{N}$ it holds that $L_{a_1,\dots,a_n}(B+C)=L_{a_1,\dots,a_n}(B)+L_{a_1,\dots,a_n}(C)$.*

Proof of Claim 17. Let us write a for $a_1,\dots,a_n$ in the proof of the claim. If $L_a(B)$ and $L_a(C)$ are both non-empty, say $L_a(B)=\{y\}$ and $L_a(C)=\{y'\}$, then we have $t(a)=y$ and $t'(a)=y'$ for all $t\in B$ and $t'\in C$. In particular $(t+t')(a)=y+y'$ and thus $\tau(a)=y+y'$ for all $\tau\in B+C$. Hence $L_a(B+C)=\{y+y'\}$. In the other case if, say, $L_a(B)$ is empty then there are $t_1,t_2\in B$ such that $t_1(a)\neq t_2(a)$. It follows $(t_1+t)(a)\neq(t_2+t)(a)$ for $t\in C$ and in particular $L_a(B+C)=\emptyset$ as wanted. This proves the claim. □

Hence we obtain

$$\begin{aligned}
L_{a_1,\dots,a_n}(B_u) &= \bigcup_{A\in B_u} L_{a_1,\dots,a_n}(A) = \bigcup_{B\in B_v}\bigcup_{C\in B_w} L_{a_1,\dots,a_n}(B+C)\\
&\overset{\text{Claim 17}}{=} \bigcup_{B\in B_v}\bigcup_{C\in B_w} (L_{a_1,\dots,a_n}(B)+L_{a_1,\dots,a_n}(C))\\
&= \bigcup_{B\in B_v} L_{a_1,\dots,a_n}(B)+\bigcup_{C\in B_w} L_{a_1,\dots,a_n}(C) = L_{a_1,\dots,a_n}(B_v)+L_{a_1,\dots,a_n}(B_w)\\
&\overset{\text{ih}}{=} I(v;C(a_1,\dots,a_n))+I(w;C(a_1,\dots,a_n)) = I(u;C(a_1,\dots,a_n)).
\end{aligned}$$

2. follows from 1.
3. It holds (a) ⇔ (b). The equivalence (a) ⇔ (c) follows from 2.
4. follows from 1. □

For further arguments we need the following result, which is obtained by an estimation by Schrijver [Sch86].

Lemma 18. *Let $k,m,n\in\mathbb{N}^+$, $A=(a_{i,j})\in\mathbb{Z}^{m\times n}$ and $b\in\mathbb{Z}^m$ such that $||A||_\infty,||b||_\infty\leq k$. If there exists $y\in\mathbb{N}^n$ with $Ay=b$, then there exists $z\in\mathbb{N}^n$ such that $Az=b$ and $||z||_\infty\leq(32k)^{12n^4}$.*

Proof. We adopt the following definitions from Schrijver [Sch86]. The size of a rational number $r = p/q$ where p and q are relatively prime integers is $\text{size}(r) = 1 + \lceil \log_2(\text{abs}(p) + 1)\rceil + \lceil \log_2(\text{abs}(q)+1)\rceil$. The size of a rational vector $v = (v_1, \dots, v_n) \in \mathbb{Q}^n$ is $\text{size}(v) = n + \text{size}(v_1) + \cdots + \text{size}(v_n)$. The size of a rational matrix $A = (a_{i,j}) \in \mathbb{Q}^{m\times n}$ is $\text{size}(A) = mn + \sum_{i,j}\text{size}(a_{i,j})$. The size of a system $Ax \le b$ of rational linear inequalities is $\text{size}(Ax \le b) = 1 + \text{size}(A) + \text{size}(b)$. A rational polyhedron is a set $\{x \in \mathbb{R}^n \mid Ax \le b\}$ for some $A \in \mathbb{Q}^{m\times n}$ and $b \in \mathbb{Q}^m$. The facet complexity of a rational polyhedron $P \subseteq \mathbb{R}^n$ is the smallest number φ such that $\varphi \ge n$ and there exists a system $Ax \le b$ of rational linear inequalities defining P, where each inequality in $Ax \le b$ has size at most φ, i.e., there exist $m \in \mathbb{N}$, $A = (a_{i,j}) \in \mathbb{Q}^{m\times n}$, and $b = (b_1, \dots, b_m) \in \mathbb{Q}^m$ such that $P = \{x \in \mathbb{R}^n \mid Ax \le b\}$ and $\forall i\,[1 + n + \text{size}(b_i) + \sum_{j=1}^n \text{size}(a_{i,j}) \le \varphi]$.

Let $C = \begin{pmatrix} A \\ -A \\ -I_n \end{pmatrix} \in \mathbb{Z}^{(2m+n)\times n}$ and $d = \begin{pmatrix} b \\ -b \\ 0 \end{pmatrix} \in \mathbb{Z}^{2m+n}$, where I_n denotes the identity matrix of size n and 0 the zero element in $\mathbb{Z}^n$. Consider the rational polyhedron $P = \{x \in \mathbb{R}^n \mid Cx \le d\}$ and let φ be its facet complexity. Observe that $\varphi \le 1 + n + \text{size}(k) + n\cdot\text{size}(k) = (n+1)(1+\text{size}(k)) \le (n+1)(1+1+1+\log_2(k+1)+1) = (n+1)\cdot\log_2 16(k+1)$. By definition, $Cx \le d$ if and only if $Ax \le b$ and $-Ax \le -b$ and $-I_n x \le 0$ if and only if $Ax = b$ and $x \in (\mathbb{R}^{\ge 0})^n$. Therefore, $P = \{x \in (\mathbb{R}^{\ge 0})^n \mid Ax = b\}$. By assumption, $y \in P \cap \mathbb{Z}^n$ and hence $P \cap \mathbb{Z}^n \ne \emptyset$. By [Sch86, Corollary 17.1b], there exists $z \in P \cap \mathbb{Z}^n = P \cap \mathbb{N}^n$ such that $\text{size}(z) \le 6n^3\varphi$. So $\text{size}(z) \le 6n^3(n+1)\cdot\log_2 16(k+1) \le 12n^4\cdot\log_2 32k$ and hence $||z||_\infty \le (32k)^{12n^4}$. □

Lemma 19. *Let $\mathcal{O} \subseteq \{\cup, \cap, +\}$ and let $C = (V, E, g_C, \alpha)$ be an $\mathcal{O}$-circuit with unassigned input gates $u_1 < \cdots < u_n$ and assigned input gates $v_1, \dots, v_k$. Moreover, let $|C|$ denote the length of the encoding of C and $\xi = \max(\alpha(v_1), \dots, \alpha(v_k)) + 1$. Then it holds:*

1. *For all $A \in B_{g_C}$, each $\sum_{i=1}^n \alpha_i x_i + \alpha_0 \in A$, and all i it holds $\alpha_i < \xi 2^{|C|}$.*
2. *If there are $a_1, \dots, a_n \in \mathbb{N}$ such that $I(C(a_1, \dots, a_n)) \ne \emptyset$, then there are $y, b_1, \dots, b_n \in \{0, 1, \dots, (32\cdot\xi\cdot 2^{|C|})^{12\cdot(n+1)^4}\}$ such that $y \in I(C(b_1, \dots, b_n))$.*
3. *Let $A \in B_{g_C}$ and $t(x_1, \dots, x_n) = \sum_{i=1}^n \alpha_i x_i + \alpha_0, t'(x_1, \dots, x_n) = \sum_{i=1}^n \alpha'_i x_i + \alpha'_0 \in A$. Then for $\zeta_i = \xi^i 2^{i|C|}$ it holds that $t(\zeta_1, \dots, \zeta_n) = t'(\zeta_1, \dots, \zeta_n)$ if and only if $\alpha_i = \alpha'_i$ for all $i = 1, \dots, n$.*
4. *Let $a_i = \xi^i 2^{i|C|}$ for $i = 1, \dots, n$. If there are $b_1, \dots, b_n \in \mathbb{N}$ such that $L_{b_1,\dots,b_n}(B_{g_C}) = \emptyset$, then $L_{a_1,\dots,a_n}(B_{g_C}) = \emptyset$.*

Proof. 1. The statement is shown by an induction.

2. Because of Lemma 16 there is an $A \in B_{g_C}$ such that the set of linear equations $\{y = \sum_{i=1}^n \alpha_i x_i + \alpha_0 \mid \sum_{i=1}^n \alpha_i x_i + \alpha_0 \in A\}$ has a solution in the $n+1$ variables $y, x_1, \dots, x_n$. Due to Lemma 18 it holds: there is a solution $y, b_1, \dots, b_n \in \mathbb{N}$ such that $||(y, b_1, \dots, b_n)||_\infty \le (32\cdot\xi\cdot 2^{|C|})^{12\cdot(n+1)^4}$. Hence $y \in L_{b_1,\dots,b_n}(A) \overset{\text{Lemma 16}}{\subseteq} I(C(b_1, \dots, b_n))$.

3. It suffices to show that if $t(\zeta_1, \dots, \zeta_n) = t'(\zeta_1, \dots, \zeta_n)$, then $\alpha_i = \alpha'_i$ for all $i = 1, \dots, n$. Assume $t(\zeta_1, \dots, \zeta_n) = t'(\zeta_1, \dots, \zeta_n)$ but there is a j such that $\alpha_j \ne \alpha'_j$. Now choose a minimal j such that $\alpha_j \ne \alpha'_j$, hence $\alpha_i = \alpha'_i$ for all $i = 1, \dots, j-1$.

We calculate $0 = t(\zeta_1, \dots, \zeta_n) - t'(\zeta_1, \dots, \zeta_n) = \sum_{i=0}^n (\alpha_i - \alpha'_i)\xi^i 2^{i|C|} = \xi^j 2^{j|C|}\cdot\sum_{i=j}^n (\alpha_i - \alpha'_i)\xi^{i-j}2^{(i-j)|C|}$ which implies $0 \ne \alpha'_j - \alpha_j = \sum_{i=j+1}^n (\alpha_i - \alpha'_i)\xi^{i-j}2^{(i-j)|C|} = \xi 2^{|C|}\cdot\sum_{i=j+1}^n (\alpha_i - \alpha'_i)\xi^{i-j-1}2^{(i-j-1)|C|}$ follows. This contradicts $\text{abs}(\alpha'_j - \alpha_j) < \xi 2^{|C|}$ from 1.

4. Assume there is an $A \in B_{g_C}$ with $L_{a_1,\dots,a_n}(A) \ne \emptyset$. Then because of 3, it holds that $|A| = 1$. Let $\sum_{i=1}^n \alpha_i x_i + \alpha_0$ be the unique term in A. Then $\sum_{i=1}^n \alpha_i b_i + \alpha_0 \in L_{b_1,\dots,b_n}(A)$, which is a contradiction to the assumption that $L_{b_1,\dots,b_n}(B_{g_C}) = \emptyset$. □

Theorem 20. Π_1-EC$(\cap,+)$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* coNP*.*

Proof. As Σ_1-MC$(\cap,+)$ is $\leq_{\mathrm{m}}^{\log}$-hard for NP [GRTW10] and Σ_1-MC$(\cap,+) \leq_{\mathrm{m}}^{\log} \Sigma_1$-NEC$(\cap,+)$ according to Lemma 2, it suffices to show that $\overline{\Pi_1\text{-EC}(\cap,+)} = \Sigma_1$-NEC$(\cap,+) \in$ NP. Due to statement 2 of Lemma 19 for an $\mathcal{O}$-circuit $C = (V, E, g_C, \alpha)$ with unassigned input gates $u_1 < \cdots < u_n$ we have $C \in \Sigma_1$-NEC$(\cap,+)$ if and only if there exist $x_1, \ldots, x_n \in \{0, 1, \ldots, (32 \cdot \xi \cdot 2^{|C|})^{12\cdot(n+1)^4}\}$ such that $C(x_1, \ldots, x_n) \neq \emptyset$. As EC$(\cap,+) \in$ coC$_=$L $\subseteq$ P (cf. Theorem 11) and $(32 \cdot \xi \cdot 2^{|C|})^{12\cdot(n+1)^4} \in 2^{O(|C|^5)}$, this can be done in non-deterministic polynomial time. □

Theorem 21.

1. EC$(\cup,\cap,+)$ *and* EC$(\cup,\cap,\times)$ *are* $\leq_{\mathrm{m}}^{\log}$*-hard for* PSPACE*.*
2. Σ_1-EC$(\cup,\cap,+)$, Π_1-EC$(\cup,\cap,+)$, Π_1-EC$(\cup,\cap,\times) \in$ PSPACE*.*

Proof. 1. The statement follows from Lemma 2, since both MC$(\cup,\cap,+)$ and MC$(\cup,\cap,\times)$ are $\leq_{\mathrm{m}}^{\log}$-hard for PSPACE [MW07] and PSPACE is closed under complement.

2. Let $C = (V, E, g_C, \alpha)$ be an $\{\cup,\cap,+\}$-circuit with unassigned input gates $u_1 < \cdots < u_n$ and assigned input nodes $v_1, \ldots, v_k$. Moreover, let $|C|$ denote the length of the encoding of C and $\xi = \max(\alpha(v_1), \ldots, \alpha(v_k)) + 1$.

According to Lemma 19.4, in order to test whether $C \in \Sigma_1$-EC$(\cup,\cap,+)$ it suffices to verify $C(\xi 2^{|C|}, \ldots, \xi^n 2^{n|C|}) = \emptyset$. The latter is equivalent to $i \notin C(\xi 2^{|C|}, \ldots, \xi^n 2^{n|C|})$ for all $i = 0, \ldots, \xi^n 2^{n|C|+|C|}$ as the circuit cannot produce larger numbers. From MC$(\cup,\cap,+) \in$ PSPACE [MW07] it follows Σ_1-EC$(\cup,\cap,+) \in$ PSPACE.

According to statement 2 of Lemma 19 the circuit C is in $C \in \Sigma_1$-NEC$(\cup,\cap,+)$ if and only if there are $y, b_1, \ldots, b_n \in \{0, 1, \ldots, (32 \cdot \xi \cdot 2^{|C|})^{12\cdot(n+1)^4}\}$ such that $(C(b_1, \ldots, b_n), y) \in$ MC$(\cup,\cap,+)$. Thus Σ_1-NEC$(\cup,\cap,+) \in$ PSPACE.

From Lemma 2 and Σ_1-MC$(\cup,\cap,\times) \in$ PSPACE [GJM16, Theorem 2] we obtain that Σ_1-NEC$(\cup,\cap,\times) \in$ PSPACE. Since PSPACE is closed under complement, the proof is complete. □

The problems Σ_1-EC and EC for the sets of operations $\{\cap,\times\}$ and $\{\cup,\cap,\times\}$ should belong to this subsection, but have not been mentioned so far. The reason is that Theorem 50 below yields a general tool that in particular is applicable to these problems. The corresponding results can be found in the Corollaries 56 and 57.

5.2 Circuits with Complement

We start with a preliminary subsection providing results on the complexity of Presburger and Skolem arithmetic. Then we prove upper bounds for the problems over $\{^-,\cup,\cap,+\}$ and $\{^-,\cup,\cap,\times\}$. These are also our best upper bounds for the problems over $\{^-,+\}$ and $\{^-,\times\}$. Finally, we show that PSPACE is a lower bound for EC$(^-,+)$ and EC$(^-,\times)$, which is the best known lower bound for all problems in this section.

5.2.1 Preliminaries from Presburger and Skolem Arithmetic

We consider first-order formulas over $\mathbb{N}$ or $\mathbb{N}^+$ that consist of variables $x_0, x_1, \ldots$, logical symbols $\neg, \vee, \exists$, function symbols $+, \times$, and symbols $0, 1, 2, 3, 5, 7, \ldots$ for constants. We use $(H_1 \wedge H_2)$, $(H_1 \rightarrow H_2)$, and $\forall x H$ as abbreviation for $\neg(\neg H_1 \vee \neg H_2)$, $(\neg H_1 \vee H_2)$, and $\neg\exists x \neg H$ respectively. When formulas are used as inputs of algorithms, we assume that the subscripts of variables and constants are encoded in binary. Th$(\mathbb{N}; +, =)$ denotes the Presburger arithmetic, which is the first-order theory of the natural numbers with addition (and without constants). $\mathrm{Th}(\mathbb{N}^+; \times, =)$ denotes the Skolem arithmetic, which is the first-order theory of the positive natural numbers with multiplication (and without constants). $\mathrm{Th}(\mathbb{N}; \times, =, 0, 1, 2, 3, 5, 7, \ldots)$ denotes the first-order theory of the natural numbers with multiplication and constants for 0, 1, and all prime numbers. $\mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots)$ denotes the first-order theory of the positive natural numbers with multiplication and constants for 1 and all prime numbers.

Theorem 22. *1.* $\mathrm{Th}(\mathbb{N}; +, =) \in \mathrm{DSPACE}\big(2^{2^{cn}}\big) \subseteq \mathrm{2EXPSPACE}$ *for some* $c > 0$*. [FR75]*

2. Any positive integer of binary length n *can be encoded by a formula of length* $O(n)$ *in the Presburger arithmetic* $\mathrm{Th}(\mathbb{N}; +, =)$*. [Opp78]*

Regarding the Skolem arithmetic we need the statement

$$\mathrm{Th}(\mathbb{N}; \times, =, 0, 1, 2, 3, 5, 7, \ldots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =),$$

which appears implicitly in the literature (e.g., [Bès02]). For the sake of completeness we provide a proof which is divided into two parts:

1. $\mathrm{Th}(\mathbb{N}; \times, =, 0, 1, 2, 3, 5, 7, \ldots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots)$
2. $\mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =)$.

We start with the first reduction and sketch the idea of the non-trivial part of the proof, namely $\mathrm{Th}(\mathbb{N}; \times, =, 1, 2, 3, 5, 7, \ldots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots)$. The reduction modifies a given formula as follows (where we assume that all atoms of H are of the form either $x \cdot y = z$ or $x = c$ for variables x, y, z, and a constant c):

1. each quantifier $\exists x$ is replaced with $\exists x \exists x'$, where x' is a new variable
2. each term $x = c$ is replaced with $(x = c \wedge x' = 1)$
3. each term $x \cdot y = z$ is replaced with $(x' = y' = z' = 1 \wedge x \cdot y = z) \vee ((x' \neq 1 \vee y' \neq 1) \wedge z' \neq 1)$

The idea is that each variable x is represented by a pair of variables (x, x'), which stands for the value x if $x' = 1$, and for the value 0 otherwise.

We will need the following definition:

Definition 23. *For two interpretations* I *and* I' *and variables* $y_1, \ldots, y_k$ *for* $k \in \mathbb{N}$ *it holds* $I \overset{y_1,\ldots,y_k}{=} I'$ *if and only if* $I(y) = I'(y)$ *for all* $y \notin \{y_1, \ldots, y_k\}$*.*
Moreover, for a quantifier-free formula H *with variables* $y_1, \ldots, y_n$ *and* $a_1, \ldots, a_n \in \mathbb{N}$ *we denote by* $H(a_1, \ldots, a_n)$ *the formula obtained from* H *by replacing every occurrence of* y_i *with* a_i *and write* $[H(a_1, \ldots, a_n)]$ *for the truth value of* $H(a_1, \ldots, a_n)$*.*

Proposition 24. $\mathrm{Th}(\mathbb{N}; \times, =, 0, 1, 2, 3, 5, 7, \ldots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots)$

Proof. It holds that $\mathrm{Th}(\mathbb{N}; \times, =, 0, 1, 2, 3, 5, 7, \ldots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}; \times, =, 1, 2, 3, 5, 7, \ldots)$, since $z = 0$ for a variable z can be expressed by $\forall x (x \cdot z = z)$.

Next we argue for $\mathrm{Th}(\mathbb{N}; \times, =, 1, 2, 3, 5, 7, \ldots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots)$. Let H be a given first-order formula, which is interpreted over $\mathbb{N}$. We may assume that the atoms of H are of the form either $x_i \cdot x_j = x_k$ or $x_i = c$ for a constant $c \in \mathbb{N}^+$. We construct an equivalent first-order formula H^+ which is interpreted over $\mathbb{N}^+$. Each variable x_i in H is represented by the pair of variables (x_{2i}, x_{2i+1}) in H^+. More precisely, H^+ is obtained from H as follows:

1. each variable x_i is replaced by x_{2i}
2. each quantifier $\exists x_{2i} H_1$ is replaced with
$\exists x_{2i} \exists x_{2i+1} (x_{2i+1} = 1 \vee x_{2i+1} = 2) \wedge (x_{2i+1} = 1 \vee x_{2i} = 1) \wedge H_1$
3. each term $x_{2i} = c$ is replaced with $(x_{2i+1} = 1 \wedge x_{2i} = c)$
4. each term $x_{2i} \cdot x_{2j} = x_{2k}$ is replaced with
$((x_{2i+1} = x_{2j+1} = x_{2k+1} = 1 \wedge x_{2i} \cdot x_{2j} = x_{2k}) \vee ((x_{2i+1} \neq 1 \vee x_{2j+1} \neq 1) \wedge x_{2k+1} \neq 1))$

We show

$$H \in \mathrm{Th}(\mathbb{N}; \times, =, 1, 2, 3, 5, 7, \ldots) \iff H^+ \in \mathrm{Th}(\mathbb{N} \setminus \{0\}; \times, =, 1, 2, 3, 5, 7, \ldots). \tag{1}$$

For each interpretation I over $\mathbb{N}$ we define a corresponding interpretation I^+ over $\mathbb{N}^+$ as follows:

$$I^+(x_j) = \begin{cases} I(x_i) & \text{if } j = 2i \text{ and } I(x_i) \neq 0 \\ 1 & \text{if } j = 2i + 1 \text{ and } I(x_i) \neq 0 \\ 1 & \text{if } j = 2i \text{ and } I(x_i) = 0 \\ 2 & \text{if } j = 2i + 1 \text{ and } I(x_i) = 0 \end{cases}$$

Claim 25. *For each formula H and all interpretations I over $\mathbb{N}$ it holds that $I(H) = I^+(H^+)$.*

Proof. (IB) If $H = (x_i \cdot x_j = x_k)$, then

$$H^+ = ((x_{2i+1} = x_{2j+1} = x_{2k+1} = 1 \wedge x_{2i} \cdot x_{2j} = x_{2k}) \vee ((x_{2i+1} \neq 1 \vee x_{2j+1} \neq 1) \wedge x_{2k+1} \neq 1))$$

and we obtain:

$$\begin{array}{rcl} I^+(H^+) & = & [((I^+(x_{2i+1}) = I^+(x_{2j+1}) = I^+(x_{2k+1}) = 1 \wedge I^+(x_{2i}) \cdot I^+(x_{2j}) = I^+(x_{2k})) \vee ((I^+(x_{2i+1}) \neq 1 \vee I^+(x_{2j+1}) \neq 1) \wedge I^+(x_{2k+1}) \neq 1))] \\ & = & [(I^+(x_{2i+1}) = I^+(x_{2j+1}) = I^+(x_{2k+1}) = 1 \wedge I^+(x_{2i}) \cdot I^+(x_{2j}) = I^+(x_{2k}))] \vee [(I(x_i) = 0 \vee I(x_j) = 0) \wedge I(x_k) = 0] \\ & = & [(I(x_i) \neq 0 \wedge I(x_j) \neq 0 \wedge I(x_k) \neq 0 \wedge I^+(x_{2i}) \cdot I^+(x_{2j}) = I^+(x_{2k}))] \vee [I(x_i) \cdot I(x_j) = I(x_k) = 0] \\ & = & [(I(x_i) \neq 0 \wedge I(x_j) \neq 0 \wedge I(x_k) \neq 0 \wedge I(x_i) \cdot I(x_j) = I(x_k))] \vee [I(x_i) \cdot I(x_j) = I(x_k) = 0] \\ & = & [I(x_i) \cdot I(x_j) = I(x_k) \neq 0] \vee [I(x_i) \cdot I(x_j) = I(x_k) = 0] \\ & = & [I(x_i) \cdot I(x_j) = I(x_k)] \\ & = & I(H) \end{array}$$

If $H = (x_i = c)$ for a constant $c \in \mathbb{N}^+$, then $H^+ = (x_{2i+1} = 1 \wedge x_{2i} = c)$ and we obtain:

$$\begin{array}{rcl} I^+(H^+) & = & I^+(x_{2i+1} = 1 \wedge x_{2i} = c) \\ & = & [I(x_i) \neq 0 \wedge I^+(x_{2i}) = c] \\ & = & [I(x_i) \neq 0 \wedge I(x_i) = c] \\ & = & I(x_i = c) \\ & = & I(H) \end{array}$$

(IS) If $H = \neg H_1$, then $H^+ = \neg H_1^+$ and $I^+(H^+) = I^+(\neg H_1^+) = 1 - I^+(H_1^+) = 1 - I(H_1) = I(\neg H_1) = I(H)$.

If $H = (H_1 \vee H_2)$, then $H^+ = (H_1^+ \vee H_2^+)$ and $I^+(H^+) = I^+(H_1^+ \vee H_2^+) = I^+(H_1^+) \vee I^+(H_2^+) = I(H_1) \vee I(H_2) = I(H_1 \vee H_2) = I(H)$.

If $H = \exists x_i H_1$, then $H^+ = \exists x_{2i} \exists x_{2i+1} (x_{2i+1} = 1 \vee x_{2i+1} = 2) \wedge (x_{2i+1} = 1 \vee x_{2i} = 1) \wedge H_1^+$ and we argue as follows:

1. If $I^+(H^+) = 1$, then there is some $I' \overset{x_{2i}, x_{2i+1}}{=} I^+$ such that $I'(x_{2i+1} = 1 \vee x_{2i+1} = 2) = I'(x_{2i+1} = 1 \vee x_{2i} = 1) = I'(H_1^+) = 1$. It follows that $I'(x_{2i+1}) \in \{1, 2\}$ and if $I'(x_{2i+1}) = 2$, then $I'(x_{2i}) = 1$. Let $I_0 \overset{x_i}{=} I$ such that

$$I_0(x_i) = \begin{cases} 0 & \text{if } I'(x_{2i+1}) = 2 \\ I'(x_{2i}) & \text{otherwise.} \end{cases}$$

Observe that $I_0^+ = I'$. Hence $I_0^+(H_1^+) = 1$ and from induction hypothesis it follows $I_0(H_1) = 1$. Together with $I_0 \overset{x_i}{=} I$ this implies $I(\exists x_i H_1) = 1$ and hence $I(H) = 1$.

2. If $I(H) = 1$, then there is some $I_0 \overset{x_i}{=} I$ such that $I_0(H_1) = 1$ and by induction hypothesis, $I_0^+(H_1^+) = 1$. From the definition of I_0^+ it follows that $I_0^+(x_{2i+1} = 1 \vee x_{2i+1} = 2) = I_0^+(x_{2i+1} = 1 \vee x_{2i} = 1) = 1$. Hence $I_0^+((x_{2i+1} = 1 \vee x_{2i+1} = 2) \wedge (x_{2i+1} = 1 \vee x_{2i} = 1) \wedge H_1^+) = 1$. From $I_0^+ \overset{x_{2i},x_{2i+1}}{=} I^+$ it follows that $I^+(\exists x_{2i} \exists x_{2i+1}(x_{2i+1} = 1 \vee x_{2i+1} = 2) \wedge (x_{2i+1} = 1 \vee x_{2i} = 1) \wedge H_1^+) = 1$. This shows $I^+(H^+) = 1$.

This completes the proof of Claim 25. □

If $H \in \mathrm{Th}(\mathbb{N}; \times, =, 1, 2, 3, 5, 7, \ldots)$, then for I with $I(x_i) := 0$ for all $i \in \mathbb{N}$ it holds that $I(H) = 1$ and by Claim 25, $I^+(H^+) = 1$, which shows $I'(H^+) = 1$ for all I' (as H is a sentence), and hence $H^+ \in \mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots)$.

Conversely, if $H^+ \in \mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots)$, then for I' with $I'(x_i) := 1$ for all $i \in \mathbb{N}$ we have $I'(H^+) = 1$. Note that for I with $I(x_i) := 1$ for all $i \in \mathbb{N}$ it holds that $I^+ = I'$. Therefore, $I^+(H^+) = 1$ and by Claim 25, $I(H) = 1$, which shows $H \in \mathrm{Th}(\mathbb{N}; \times, =, 1, 2, 3, 5, 7, \ldots)$ (as H is a sentence).

This shows the equivalence (1) and finishes the proof of Proposition 24. □

Now we sketch the idea of the reduction $\mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =, 1)$. Let H be a first-order sentence and let $C = \{q_1, \ldots, q_n\} \subseteq \mathbb{P}$ be the set of constants $\neq 1$ that appear in H. For $p \in C$ and $q \in \mathbb{P}$, let $H_{p,q}$ be the formula that is obtained from H if each occurrence of p is replaced with q and vice versa. It holds that H is true if and only if $H_{p,q}$ is true, since swapping prime factors p and q yields a one-one correspondence between assignments of variables in H and assignments of variables in $H_{p,q}$. Therefore, H is true if and only if H' is true, where H' is the formula obtained from H by replacing the occurrences of $q_1, \ldots, q_n$ with new variables $z_1, \ldots, z_n$ respectively and requiring that $z_1, \ldots, z_n$ are distinct primes. The latter is possible with the following formula:

$$\bigwedge_i \neg \exists a \exists b (a \neq 1 \wedge b \neq 1 \wedge a \cdot b = z_i) \;\wedge\; \bigwedge_{i \neq j} z_i \neq z_j.$$

This shows $\mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =, 1)$ via $H \mapsto H'$.

Proposition 26. $\mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =)$.

Proof. First we argue for $\mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \ldots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =, 1)$ via $H \mapsto H'$. Let p and q be distinct primes. Define $\pi_{p,q}(n) = np^b q^a / p^a q^b$, where $a = \max\{i \mid p^i \text{ divides } n\}$ and $b = \max\{i \mid q^i \text{ divides } n\}$. So $\pi_{p,q}$ swaps the factors p and q in the prime factorization of a given number. For a term T, let $T_{p,q}$ be the term that is obtained from T if each occurrence of p is replaced with q and vice versa. For a first-order formula H, let $H_{p,q}$ be the formula that is obtained from H if each occurrence of p is replaced with q and vice versa. For an interpretation I let $I_{p,q}$ be the interpretation defined by $I_{p,q}(x_i) = \pi_{p,q}(I(x_i))$ for all variables x_i.

Claim 27. *For all terms T and all interpretations I it holds that $I(T) = \pi_{p,q}(I_{p,q}(T_{p,q}))$.*

Proof. (IB) For variables $T = x_i$ we have

$$\pi_{p,q}(I_{p,q}(T_{p,q})) = \pi_{p,q}(I_{p,q}(T)) = \pi_{p,q}(\pi_{p,q}(I(T))) = I(T).$$

For constants $T = r \in \mathbb{P} \cup \{1\}$ we have

$$\pi_{p,q}(I_{p,q}(T_{p,q})) = \pi_{p,q}(I_{p,q}(\pi_{p,q}(r))) = \pi_{p,q}(\pi_{p,q}(r)) = r = I(T).$$

(IS) For products $T = T' \cdot T''$ we have

$$\begin{aligned}\pi_{p,q}(I_{p,q}(T_{p,q})) &= \pi_{p,q}(I_{p,q}(T'_{p,q} \cdot T''_{p,q}))\\ &= \pi_{p,q}(I_{p,q}(T'_{p,q}) \cdot I_{p,q}(T''_{p,q}))\\ &= \pi_{p,q}(I_{p,q}(T'_{p,q})) \cdot \pi_{p,q}(I_{p,q}(T''_{p,q}))\\ &= I(T') \cdot I(T'') = I(T' \cdot T'') = I(T),\end{aligned}$$

which proves the claim. □

Claim 28. *For all first-order formulas H and all interpretations I it holds that $I(H) = I_{p,q}(H_{p,q})$.*

Proof. (IB) For $H = (T' = T'')$ we have

$$\begin{aligned}I_{p,q}(H_{p,q}) &= I_{p,q}(T'_{p,q} = T''_{p,q})\\ &= [I_{p,q}(T'_{p,q}) = I_{p,q}(T''_{p,q})]\\ &= [\pi_{p,q}(I_{p,q}(T'_{p,q})) = \pi_{p,q}(I_{p,q}(T''_{p,q}))]\\ &= [I(T') = I(T'')] = I(T' = T'') = I(H).\end{aligned}$$

(IS) For $H = \neg H'$ we have

$$I_{p,q}(H_{p,q}) = I_{p,q}(\neg H'_{p,q}) = 1 - I_{p,q}(H'_{p,q}) = 1 - I(H') = I(\neg H') = I(H).$$

For $H = (H' \vee H'')$ we have

$$\begin{aligned}I_{p,q}(H_{p,q}) &= I_{p,q}(H'_{p,q} \vee H''_{p,q})\\ &= [I_{p,q}(H'_{p,q}) \vee I_{p,q}(H''_{p,q})]\\ &= [I(H') \vee I(H'')] = I(H' \vee H'') = I(H).\end{aligned}$$

For $H = \exists x H'$ we have

$$I_{p,q}(H_{p,q}) = I_{p,q}(\exists x H'_{p,q}) = \max_{I' \overset{x}{=} I_{p,q}} I'(H'_{p,q}) \overset{(*)}{=} \max_{I'' \overset{x}{=} I} I''_{p,q}(H'_{p,q}) = \max_{I'' \overset{x}{=} I} I''(H') = I(\exists x H') = I(H),$$

where $(*)$ holds, because (i) if $I' \overset{x}{=} I_{p,q}$, then for I'' such that $I'' \overset{x}{=} I$ and $I''(x) = \pi_{p,q}(I'(x))$ it holds that $I' = I''_{p,q}$ and (ii) if $I'' \overset{x}{=} I$, then for I' such that $I' \overset{x}{=} I_{p,q}$ and $I'(x) = \pi_{p,q}(I''(x))$ it holds that $I' = I''_{p,q}$. This proves the claim. □

Let H be a first-order sentence and let $C = \{q_1, \dots, q_n\} \subseteq \mathbb{P}$ be the set of constants $\neq 1$ that appear in H. By Claim 28, for all distinct primes p, q and all interpretations I it holds that $I(H) = I(H_{p,q})$. Therefore, H is true if and only if H' is true, which is the sentence obtained from H by replacing the occurrences of $q_1, \dots, q_n$ with new variables $z_1, \dots, z_n$ respectively and requiring that $z_1, \dots, z_n$ are distinct primes. The latter is possible with the following formula:

$$\bigwedge_i \neg \exists a \exists b (a \neq 1 \wedge b \neq 1 \wedge a \cdot b = z_i) \ \wedge \ \bigwedge_{i \neq j} z_i \neq z_j.$$

This shows $\mathrm{Th}(\mathbb{N}^+; \times, =, 1, 2, 3, 5, 7, \dots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =, 1)$ via $H \mapsto H'$.

Finally, $\mathrm{Th}(\mathbb{N}^+; \times, =, 1) \leq_{\mathrm{m}}^{\log} \mathrm{Th}(\mathbb{N}^+; \times, =)$, since $e = 1$ for a variable e can be expressed by $\forall x (x \cdot e = x)$. □

Corollary 29. $\mathrm{Th}(\mathbb{N}; \times, =, 0, 1, 2, 3, 5, 7, \dots) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Th}(\mathbb{N}^+; \times, =) \in \mathrm{3EXPSPACE}$.

Proof. The reduction follows from the Propositions 24 and 26. $\mathrm{Th}(\mathbb{N}^+; \times, =)$ is decidable by an alternating Turing machine in time $2^{2^{2^{O(n)}}}$ with n alternations [Grä89]. In particular it is decidable in space $2^{2^{2^{O(n)}}}$ [FR79]. □

5.2.2 Upper Bounds

The main results in this section are obtained by applying the decidability of Presburger and Skolem arithmetic. In contrast, the bounds in the following theorem are a consequence of results from [MW07].

Theorem 30. EC$(\cup,\cap,^-,+)$, EC$(\cup,\cap,^-,\times) \in$ PSPACE.

Proof. By Lemma 2 and MC$(\cup,\cap,^-,\times) \in$ PSPACE [MW07] it holds EC$(\cup,\cap,^-,\times) \in$ PSPACE.

Next, let C be a completely assigned $\{\cup,\cap,^-,+\}$-circuit, and $f(n) = n2^n$. An induction on the number of gates shows that $I(C)$ either completely contains the set $\{m \in \mathbb{N} \mid m \geq f(|C|)\}$, or is disjoint from it. Since MC$(\cup,\cap,^-,+) \in$ PSPACE [MW07], we can test in polynomial space, whether $(C,k) \in$ MC$(\cup,\cap,^-,+)$ for all $k \leq f(|C|)+1$. Hence EC$(\cup,\cap,^-,+) \in$ PSPACE. □

The proof of the following theorem closely follows [GJM15, Theorem 1], which deals with Σ_1-MC$(\cup,\cap,^-,\times)$ by reducing the problem to a formula in Skolem arithmetic. For the first part we modify that proof by replacing × with + and therefore argue via Presburger arithmetic.

Theorem 31. *1.* Σ_1-EC$(\cup,\cap,^-,+)$, Π_1-EC$(\cup,\cap,^-,+) \in$ 2EXPSPACE.

2. Σ_1-EC$(\cup,\cap,^-,\times)$, Π_1-EC$(\cup,\cap,^-,\times) \in$ 3EXPSPACE.

Proof. We start with part 1. By De Morgan's laws, it suffices to consider $\{\cup,^-,+\}$-circuits. Let C be a $\{\cup,^-,+\}$-circuit with gates $g_1 < \ldots < g_r$, where $g_1,\ldots,g_n$ $(n \leq r)$ are the input gates which are split into the assigned input gates $g_1,\ldots,g_m$ with labels $y_1,\ldots,y_m \in \mathbb{N}$ and the unassigned inputs $g_{m+1},\ldots,g_n$. We may assume g_r to be the output gate. For every gate g_k we shall construct in polynomial time in $|C|$ a formula $\varphi_k = \varphi_k(\boldsymbol{x_1},\ldots,\boldsymbol{x_n},\boldsymbol{i_k},\boldsymbol{v_k},\boldsymbol{b_k})$ over the structure $(\mathbb{N};+,=)$ such that for any assignment of variables $x_{m+1},\ldots,x_n,v_k \in \mathbb{N}$, $b_k \in \{0,1\}$ and $i_k = 1,\ldots,k$, the closed formula $\varphi_k(y_1,\ldots,y_m,x_{m+1},\ldots,x_n,i_k,v_k,b_k)$ is true if and only if $b_k = 1 \leftrightarrow v_k \in I(g_{i_k}; C(x_{m+1},\ldots,x_n))$ is true. The result follows from Theorem 22, since

$$\begin{aligned} C \in \Sigma_1\text{-EC}(\cup,^-,+) &\iff \exists \boldsymbol{x_{m+1}},\ldots,\boldsymbol{x_n}\, \forall \boldsymbol{v_r}\; v_r \notin C(\boldsymbol{x_{m+1}},\ldots,\boldsymbol{x_n}) \\ &\iff \exists \boldsymbol{x_{m+1}},\ldots,\boldsymbol{x_n}\, \forall \boldsymbol{v_r}\; \varphi_r(y_1,\ldots,y_m,\boldsymbol{x_{m+1}},\ldots,\boldsymbol{x_n},r,\boldsymbol{v_r},0) \end{aligned}$$

and

$$C \in \Sigma_1\text{-NEC}(\cup,^-,+) \iff \exists \boldsymbol{x_{m+1}},\ldots,\boldsymbol{x_n}\, \exists \boldsymbol{v_r}\; \varphi_r(y_1,\ldots,y_m,\boldsymbol{x_{m+1}},\ldots,\boldsymbol{x_n},r,\boldsymbol{v_r},1).$$

Note that part 2 of Theorem 22 is needed in order to ensure that the description of the constant $y_1,\ldots,y_m$ does not need too much space.

To construct φ_k, we proceed inductively. Let φ_0 be the tautology

$$\boldsymbol{b_0} \vee \neg\boldsymbol{b_0} \vee (\boldsymbol{x_1} + \ldots + \boldsymbol{x_n} + \boldsymbol{i_0} + \boldsymbol{v_0} = 0)$$

and $\psi_k = [\boldsymbol{i_k} \neq k \rightarrow (\boldsymbol{i_{k-1}} = \boldsymbol{i_k} \wedge \boldsymbol{v_{k-1}} = \boldsymbol{v_k} \wedge \boldsymbol{b_{k-1}} = \boldsymbol{b_k})]$. For the input gates g_k, i.e., $k = 1,\ldots,n$, we let

$$\begin{aligned} \varphi_k = \exists \boldsymbol{i_{k-1}},\boldsymbol{v_{k-1}},\boldsymbol{b_{k-1}} \Big(&\varphi_{k-1} \wedge \psi_k \wedge [(\boldsymbol{i_k} = k \wedge \boldsymbol{b_k} = 0) \rightarrow (\boldsymbol{x_k} \neq \boldsymbol{v_k} \wedge \boldsymbol{i_{k-1}} = 0)] \\ &\wedge [(\boldsymbol{i_k} = k \wedge \boldsymbol{b_k} = 1) \rightarrow (\boldsymbol{x_k} = \boldsymbol{v_k} \wedge \boldsymbol{i_{k-1}} = 0)]\Big). \end{aligned}$$

Observe that the free variables in φ_k are $\boldsymbol{x_1},\ldots,\boldsymbol{x_n},\boldsymbol{i_k},\boldsymbol{v_k},\boldsymbol{b_k}$ and that the φ_k thus defined satisfy the claim from above for all $k \leq n$.

Next, we define φ_k for $n < k \leq r$. If g_k is a complement gate with predecessor g_j then, in particular $j < k$ due to the topological ordering of $g_1, \ldots, g_r$. We let

$$\begin{aligned}\varphi_k = \exists \boldsymbol{i_{k-1}}, \boldsymbol{v_{k-1}}, \boldsymbol{b_{k-1}} \Big(\varphi_{k-1} \wedge \psi_k \wedge [\boldsymbol{i_k} = k \rightarrow (\boldsymbol{i_{k-1}} = j \wedge \boldsymbol{v_{k-1}} = \boldsymbol{v_k} \wedge \\ (\boldsymbol{b_k} = 1 \rightarrow \boldsymbol{b_{k-1}} = 0) \wedge (\boldsymbol{b_k} = 0 \rightarrow \boldsymbol{b_{k-1}} = 1))]\Big).\end{aligned}$$

If g_k is a $\cup$-gate with predecessors $g_j, g_{j'}$ then let

$$\begin{aligned}\varphi_k = \exists \boldsymbol{f_k}, \boldsymbol{f'_k} \, \forall \boldsymbol{e_k} \, \exists \boldsymbol{i_{k-1}}, \boldsymbol{v_{k-1}}, \boldsymbol{b_{k-1}} \Big(&\varphi_{k-1} \wedge \psi_k \\ &\wedge [(\boldsymbol{i_k} = k \wedge \boldsymbol{e_k} = 0) \rightarrow (\boldsymbol{i_{k-1}} = j \wedge \boldsymbol{v_{k-1}} = \boldsymbol{v_k} \wedge \boldsymbol{b_{k-1}} = \boldsymbol{f_k})] \\ &\wedge [(\boldsymbol{i_k} = k \wedge \boldsymbol{e_k} \neq 0) \rightarrow (\boldsymbol{i_{k-1}} = j' \wedge \boldsymbol{v_{k-1}} = \boldsymbol{v_k} \wedge \boldsymbol{b_{k-1}} = \boldsymbol{f'_k})] \\ &\wedge [(\boldsymbol{i_k} = k \wedge \boldsymbol{b_k} = 1) \rightarrow (\boldsymbol{f_k} = 1 \vee \boldsymbol{f'_k} = 1)] \\ &\wedge [(\boldsymbol{i_k} = k \wedge \boldsymbol{b_k} = 0) \rightarrow (\boldsymbol{f_k} = 0 \wedge \boldsymbol{f'_k} = 0)] \\ \Big).\end{aligned}$$

If g_k is a $+$-gate with predecessors $g_j, g_{j'}$ then let

$$\begin{aligned}\varphi_k = \exists \boldsymbol{f_k}, \boldsymbol{f'_k} \, \forall \boldsymbol{e_k} \, \forall \boldsymbol{h_k}, \boldsymbol{h'_k} \, \exists \boldsymbol{d_k} \, \exists \boldsymbol{i_{k-1}}, \boldsymbol{v_{k-1}}, \boldsymbol{b_{k-1}} \Big(&\varphi_{k-1} \wedge \psi_k \\ &\wedge [(\boldsymbol{i_k} = k \wedge \boldsymbol{b_k} = 1 \wedge \boldsymbol{e_k} = 0) \\ &\quad \rightarrow (\boldsymbol{f_k} + \boldsymbol{f'_k} = \boldsymbol{v_k} \wedge \boldsymbol{i_{k-1}} = j \wedge \boldsymbol{v_{k-1}} = \boldsymbol{f_k} \wedge \boldsymbol{b_{k-1}} = 1)] \\ &\wedge [(\boldsymbol{i_k} = k \wedge \boldsymbol{b_k} = 1 \wedge \boldsymbol{e_k} \neq 0) \\ &\quad \rightarrow (\boldsymbol{f_k} + \boldsymbol{f'_k} = \boldsymbol{v_k} \wedge \boldsymbol{i_{k-1}} = j' \wedge \boldsymbol{v_{k-1}} = \boldsymbol{f'_k} \wedge \boldsymbol{b_{k-1}} = 1)] \\ &\wedge [(\boldsymbol{i_k} = k \wedge \boldsymbol{b_k} = 0 \wedge \boldsymbol{h_k} + \boldsymbol{h'_k} = \boldsymbol{v_k} \wedge \boldsymbol{d_k} = 0) \\ &\quad \rightarrow (\boldsymbol{i_{k-1}} = j \wedge \boldsymbol{v_{k-1}} = \boldsymbol{h_k} \wedge \boldsymbol{b_{k-1}} = 0)] \\ &\wedge [(\boldsymbol{i_k} = k \wedge \boldsymbol{b_k} = 0 \wedge \boldsymbol{h_k} + \boldsymbol{h'_k} = \boldsymbol{v_k} \wedge \boldsymbol{d_k} \neq 0) \\ &\quad \rightarrow (\boldsymbol{i_{k-1}} = j' \wedge \boldsymbol{v_{k-1}} = \boldsymbol{h'_k} \wedge \boldsymbol{b_{k-1}} = 0)] \\ \Big).\end{aligned}$$

Again, it can be checked that the φ_k thus defined satisfies the claim from above. This concludes the proof of part 1. Part 2 can be proved analogously by using $\times$ instead of $+$ and $\mathrm{Th}(\mathbb{N}; \times, =, 0, 1, 2, 3, 5, 7, 11 \ldots)$ instead of Presburger arithmetic. The formulas φ_k for this part are thus the same as in [GJM15, Theorem 1]. □

5.2.3 Lower Bounds

We now move on to showing lower bounds. We prove that all problems covered by this section are $\leq_{\mathrm{m}}^{\log}$-hard for PSPACE. In particular, we prove the PSPACE-hardness for $\mathrm{EC}(^-, +)$ and $\mathrm{EC}(^-, \times)$.

Definition 32. *A $\{^-, +\}$-circuit over $\mathbb{N}^k$ ($k \in \mathbb{N}^+$) $C = ((V, E), g_C, \alpha)$ is a completely assigned $\{^-, +\}$-circuit where all constants are elements of $\mathbb{N}^k$. For a $\{^-, +\}$-circuit $C = ((V, E), g_C, \alpha)$ over $\mathbb{N}^k$ the set computed by a node g is defined as follows.*

$$I(g; C) = \begin{cases} \{\alpha(g)\} \subseteq \mathbb{N}^k & \textit{if } g \textit{ has indegree 0}, \\ \mathbb{N}^k \setminus I(g', C) & \textit{if } g = \overline{g'}, \\ I(g', C) + I(g'', C) & \textit{if } g = g' + g''. \end{cases}$$

Moreover, we define $I(C) = I(g_C; C)$ *and*

$$\begin{aligned}\mathrm{MC}^+(^-,+) = \{(C,b) \mid &C \textit{ is a } \{^-,+\}\textit{-circuit over } \mathbb{N}^k \textit{ for some } k \in \mathbb{N}^+\textit{, for every constant } c\\ &\textit{it holds } ||c||_\infty \leq 1,\ ||b||_\infty \leq 3, \textit{ and } b \in I(C)\}.\end{aligned}$$

For some fixed $k \in \mathbb{N}^+$ *we denote by* e_i *the* i*-th unit vector* $(0,\dots,0,1,0,\dots,0)$*, where the* i*-th component is* 1*. For an* $n \in \mathbb{N}^k$ *we denote the* i*-th component by* n_i*.*

In order to show the PSPACE-hardness of this problem we make use of the following problem which is known to be $\leq_{\mathrm{m}}^{\mathrm{log}}$-complete for PSPACE.

Definition 33. KNF-QBF $= \{F \mid F$ *is a closed quantified boolean formula in cnf with* $F \equiv 1\}$*.*

The proof of the following lemma is based on an unpublished proof by Reinhardt [Rei16] showing the PSPACE-hardness of MC$(^-,\times)$ (Corollary 36).

Lemma 34. $\mathrm{MC}^+(^-,+)$ *is* $\leq_{\mathrm{m}}^{\mathrm{log}}$*-hard for* PSPACE*.*

Proof. We show KNF-QBF $\leq_{\mathrm{m}}^{\mathrm{log}}$ $\mathrm{MC}^+(^-,+)$. Let $H = Q_1x_1 \dots Q_mx_m \bigwedge_{j=1}^n K_j$ with $Q_i \in \{\exists, \forall\}$ be an arbitrary quantified boolean formula with variables $x_1, \dots x_m$ and clauses K_j such that without loss of generality each positive literal appears exactly once in the formula (else generate H' by replacing all positive occurrences of x_i by $\neg y$ and replace H by $\exists y H'(x_1, \dots, x_m, y) \wedge (x_i \vee y) \wedge (\neg x_i \vee \neg y)$). Denote the unique clause in which the positive literal x_i occurs by $K_{j(i)}$. We assume that $\neg x_i$ does not appear in $K_{j(i)}$ (otherwise the clause can be deleted without changing the formula's truth value).

We now define circuits $C_m, \dots, C_0$ inductively. These circuits are $\{^-,+\}$-circuits over $\mathbb{N}^{m+n}$ such that all constants are unit vectors. For each of the circuits C_k and all $\alpha_1, \dots, \alpha_k \in \{0,1\}^{m+n}$ the following holds:

$$\begin{aligned}&Q_{k+1}x_{k+1} \dots Q_mx_mH(\alpha_1, \dots, \alpha_k, x_{k+1}, \dots, x_m) \;\Leftrightarrow\\ &\qquad\qquad \sum_{j=1}^n e_j + \sum_{i=1}^k (\alpha_i + 1) \cdot e_{n+i} + \sum_{i=k+1}^m 3e_{n+i} \in I(C_k) \qquad (*)\end{aligned}$$

Then, for $k = 0$, we obtain $Q_1x_1 \dots Q_mx_mH(x_1, \dots, x_m) \Leftrightarrow \sum_{j=1}^n e_j + \sum_{i=1}^m 3e_{n+i} \in I(C_0)$, the desired reduction.

We now consider the case $k = m$. Note that $\mathbb{N}^{m+n} = \overline{e_1} + \overline{e_2}$. We now define sets $F_i \subseteq \mathbb{N}^{n+m}$ for $i = 1, \dots, m$. The idea is that the vector $(k_1, \dots, k_n, 0, \dots, 0, z_i, 0, \dots, 0)$ with z_i as the $(n+i)$-th component is in F_i if and only if

1. $z_i = 1$ and for all clauses K_j that do not contain $\neg x_i$ it holds $k_j = 0$, or
2. $z_i = 2$ and for all clauses K_j that do not contain x_i it holds $k_j = 0$.

So if F_i contains a vector with $k_j = 1$ and $z_i = 1$, then K_j contains $\neg x_j$ and hence K_j is satisfied by $x_i := z_i - 1 = 0$. On the other hand, if F_i contains a vector with $k_j = 1$ and $z_i = 2$, then K_j contains x_j and hence K_j is satisfied by $x_i := z_i - 1 = 1$. Note that for the vectors in F_i we do not require $k_j = 1$ for all K_j satisfied by $x_i = z_i - 1$.

$$\begin{aligned}
\overline{F_i} = {} & \overline{\overline{\mathbb{N}^{m+n}+2e_{n+i}}+e_{n+i}}+ && (1)\\
& \sum_{i'\leq m, i'\neq i} \overline{\overline{\mathbb{N}^{m+n}+e_{n+i'}}+e_{n+i}}+ && (2)\\
& \sum_{j, \neg x_j \text{ is in } K_j} \overline{\overline{\mathbb{N}^{m+n}+e_j+e_{n+i}}+e_{n+i}}+ && (3)\\
& \overline{\overline{\overline{\overline{\mathbb{N}^{m+n}+e_{n+i}}+e_{n+i}}+e_{j(i)}}+e_{n+i}}+ && (4)\\
& \sum_{j\leq n, j\neq j(i), \neg x_i \text{ is not in } K_j} \overline{\overline{\mathbb{N}^{m+n}+e_j}+e_{n+i}}. && (5)
\end{aligned}$$

Each of the summands (1) - (5) of $\overline{F_i}$ contains 0. This excludes all vectors occurring in one of the summands from F_i.

- The summand (1) equals the set of all y with $y_{n+i} = 0$ or $y_{n+i} > 2$.
- The summand (2) consists of all y with $y_{n+i} = 0$ or $y_{n+i'} > 0$ for some $i' \neq i$. Hence the first two summands make sure that F_i contains only such vectors y for which $y_{n+i} \in \{1, 2\}$ (where 1 stands for false and 2 for true) and $y_{n+i'} = 0$ for $i' \neq i$.
- The summand (3) equals the set of all y with $y_{n+i} = 0$ or ($y_{n+i} > 1$ and $y_j > 0$ for some j such that K_j contains $\neg x_i$). This excludes from F_i those vectors that correspond to the situation that a clause K_j containing $\neg x_i$ is satisfied "by $x_i = 1$".
- The summand (4) consists of all y with $y_{n+i} = 0$ or ($y_{n+i} \neq 2$ and $y_{j(i)} > 0$). This excludes those vectors from F_i that correspond to the situation that the clause $K_{j(i)}$ is satisfied "by $x_i = 0$".
- The summand (5) consists of all y with $y_{n+i} = 0$ or $y_j > 0$ for some j such that $j \neq j(i)$ and K_j does not contain $\neg x_i$. This excludes those vectors from F_i which correspond to the situation that a clause K_j not containing the literals $\neg x_i$ and x_i is satisfied "by the variable x_i".

Let $C_m = F_1 + \cdots + F_m$. Observe that for all $\alpha_1, \ldots, \alpha_m$ it holds

$$H(\alpha_1, \ldots, \alpha_m) = 1 \Leftrightarrow \sum_{j=1}^{n} e_j + \sum_{i=1}^{m} (\alpha_i + 1)e_{n+i} \in I(C_m),$$

which means that $(*)$ holds for $k = m$. For the direction $\Leftarrow$ in the above equivalence, note that for all $y \in F_i$ it holds $y_{n+i'} = 0$ for $i' \neq i$.

Now, for the step from k to $k-1$, assume $(*)$. For further reasoning we need the following claim.

Claim 35. *It holds*

$$\overline{\overline{\overline{\mathbb{N}^{m+n}+2e_{n+k}}+e_{n+k}} + \sum_{1\leq i\leq m+n, i\neq n+k} \overline{\overline{\mathbb{N}^{m+n}+e_i}+e_{n+k}}} = \{e_{n+k}, 2e_{n+k}\}.$$

Proof of Claim 35. It holds $\overline{\overline{\mathbb{N}^{m+n} + 2e_{n+k}} + e_{n+k}} = \{x \in \mathbb{N}^{n+m} \mid x_{n+k} \notin \{1, 2\}\}$. For $1 \leq i \leq m + n$ with $i \neq n + k$ we have $\overline{\overline{\mathbb{N}^{m+n} + e_i} + e_{n+k}} = \{x \in \mathbb{N}^{n+m} \mid x_i \neq 0 \text{ oder } x_{n+k} = 0\}$. This yields

$$\sum_{1 \leq i \leq m+n, i \neq n+k} \overline{\overline{\mathbb{N}^{m+n} + e_i} + e_{n+k}} = \{x \in \mathbb{N}^{n+m} \mid x_{n+k} = 0 \vee \exists_{1 \leq i \leq n+m, i \neq n+k} x_i \neq 0\}.$$

Consequently,

$$\begin{aligned} \overline{\overline{\mathbb{N}^{m+n} + 2e_{n+k}} + e_{n+k}} + \sum_{1 \leq i \leq m+n, i \neq n+k} \overline{\overline{\mathbb{N}^{m+n} + e_i} + e_{n+k}} &= \\ = \{x \in \mathbb{N}^{n+m} \mid x_{n+k} \notin \{1, 2\} \vee \exists_{1 \leq i \leq n+m, i \neq n+k} x_i \neq 0\} \end{aligned}$$

and hence

$$\begin{aligned} \overline{\overline{\overline{\mathbb{N}^{m+n} + 2e_{n+k}} + e_{n+k}} + \sum_{1 \leq i \leq m+n, i \neq n+k} \overline{\overline{\mathbb{N}^{m+n} + e_i} + e_{n+k}}} &= \\ = \{x \in \mathbb{N}^{n+m} \mid x_{n+k} \in \{1, 2\} \wedge \forall_{1 \leq i \leq n+m, i \neq n+k} x_i = 0\} = \{e_{n+k}, 2e_{n+k}\}. \end{aligned}$$

□

In the case $Q_k = \exists$ we have:

$$\begin{aligned} &\exists x_k Q_{k+1} x_{k+1} \dots Q_m x_m \ H(\alpha_1, \dots, \alpha_{k-1}, x_k, \dots, x_m) \\ &\quad \Leftrightarrow Q_{k+1} x_{k+1} \dots Q_m x_m \ H(\alpha_1, \dots, \alpha_{k-1}, 0, x_{k+1}, \dots, x_m) \\ &\qquad\qquad \vee Q_{k+1} x_{k+1} \dots Q_m x_m \ H(\alpha_1, \dots, \alpha_{k-1}, 1, x_{k+1}, \dots, x_m) \\ &\quad \Leftrightarrow \sum_{j=1}^{n} e_j + \sum_{i=1}^{k-1} (\alpha_i + 1) \cdot e_{n+i} + e_{n+k} + \sum_{i=k+1}^{m} 3e_{n+i} \in I(C_k) \\ &\qquad\qquad \vee \sum_{j=1}^{n} e_j + \sum_{i=1}^{k-1} (\alpha_i + 1) \cdot e_{n+i} + 2e_{n+k} + \sum_{i=k+1}^{m} 3e_{n+i} \in I(C_k) \\ &\quad \Leftrightarrow \sum_{j=1}^{n} e_j + \sum_{i=1}^{k-1} (\alpha_i + 1) \cdot e_{n+i} + \sum_{i=k}^{m} 3e_{n+i} \in I(C_k + \{2e_{n+k}, e_{n+k}\}) = I(C_{k-1}) \end{aligned}$$

for $C_{k-1} := C_k + \overline{\overline{\overline{\mathbb{N}^{m+n} + 2e_{n+k}} + e_{n+k}} + \sum_{i \leq m+n, i \neq n+k} \overline{\overline{\mathbb{N}^{m+n} + e_i} + e_{n+k}}}$ according to Claim 35.

In the case $Q_k = \forall$ the reasoning becomes:

$$
\begin{aligned}
&\forall x_k Q_{k+1}x_{k+1}\dots Q_m x_m\ H(\alpha_1,\dots,\alpha_{k-1},x_k,\dots,x_m)\\
&\quad\Leftrightarrow Q_{k+1}x_{k+1}\dots Q_m x_m\ H(\alpha_1,\dots,\alpha_{k-1},0,x_{k+1},\dots,x_m)\\
&\qquad\qquad\qquad\qquad\qquad\qquad \wedge Q_{k+1}x_{k+1}\dots Q_m x_m\ H(\alpha_1,\dots,\alpha_{k-1},1,x_{k+1},\dots,x_m)\\
&\quad\Leftrightarrow \sum_{j=1}^{n} e_j + \sum_{i=1}^{k-1}(\alpha_i+1)\cdot e_{n+i} + e_{n+k} + \sum_{i=k+1}^{m} 3e_{n+i} \in I(C_k)\\
&\qquad\qquad\qquad\qquad\qquad \wedge \sum_{j=1}^{n} e_j + \sum_{i=1}^{k-1}(\alpha_i+1)\cdot e_{n+i} + 2e_{n+k} + \sum_{i=k+1}^{m} 3e_{n+i} \in I(C_k)\\
&\quad\Leftrightarrow \sum_{j=1}^{n} e_j + \sum_{i=1}^{k-1}(\alpha_i+1)\cdot e_{n+i} + \sum_{i=k}^{m} 3e_{n+i} \in I((C_k+2e_{n+k})\cap(C_k+e_{n+k}))\\
&\quad\Leftrightarrow \sum_{j=1}^{n} e_j + \sum_{i=1}^{k-1}(\alpha_i+1)\cdot e_{n+i} + \sum_{i=k}^{m} 3e_{n+i} \in I(\overline{\overline{C_k+2e_{n+k}}\cup\overline{C_k+e_{n+k}}})\\
&\quad\Leftrightarrow \sum_{j=1}^{n} e_j + \sum_{i=1}^{k-1}(\alpha_i+1)\cdot e_{n+i} + \sum_{i=k}^{m} 3e_{n+i} \in I(\overline{\overline{C_k}+2e_{n+k}\cup\overline{C_k}+e_{n+k}}) =\\
&\qquad = I(\overline{\overline{C_k}+\{2e_{n+k},e_{n+k}\}}) = I(C_{k-1})
\end{aligned}
$$

for $C_{k-1} := \overline{\overline{C_k} + \overline{\overline{\overline{\overline{\mathbb{N}^{m+n}+2e_{n+k}}+e_{n+k}} + \sum_{i\le m+n, i\ne n+k}\overline{\overline{\mathbb{N}^{m+n}+e_i}+e_{n+k}}}}}$ (cf. Claim 35).

Note that the circuits can be chosen such that all constants are unit vectors. Since the F_i and C_j can be constructed in logarithmic space, the proof is complete. □

The following corollary is not needed for our argumentation. We mention it, since it is a direct consequence of the proof above, which was originally developed by Reinhardt [Rei16] to show the PSPACE-hardness of MC$(^-,\times)$.

Corollary 36 ([Rei16])**.** MC$(^-,\times)$ *is* $\le_\mathrm{m}^\mathrm{p}$*-hard for* PSPACE.

Proof. According to Lemma 34 it suffices to show MC$^+(^-,+) \le_\mathrm{m}^\mathrm{p}$ MC$(^-,\times)$: Given a $\{^-,+\}$-circuit C over $\mathbb{N}^k$ for some $k\in\mathbb{N}^+$ and $b\in\mathbb{N}^k$, replace all $+$-gates with $\times$-gates and replace the input e_i with p_i, where p_i is the i-th prime ($1\le i\le k$). We denote the $\{^-,\times\}$-circuit obtained this way by C'. Moreover, replace $b=\sum_{i=1}^k b_i e_i$ with $\prod_{i=1}^k p_i^{b_i}$. As $b_i\le 3$ for all i and as — due to the prime number theorem — $p_1,\dots,p_k$ can be determined in time $p(k)$ for some polynomial p, the reduction can be computed in polynomial time.

It can be seen inductively that for every gate g of C and its corresponding gate g' in C' it holds $I(g';C')\cap\{n\in\mathbb{N}\mid\forall_{i>k}p_i\nmid n\} = \{\prod_{i=1}^k p_i^{x_i}\mid\sum_{i=1}^k x_i e_i\in I(g;C)\}$. Thus $b\in I(C)$ if and only if $b'\in I(C')$. □

Remark 37. *Note that Corollary 36 states* MC$(^-,\times)$ *only to be* $\le_\mathrm{m}^\mathrm{p}$*-hard for* PSPACE*. It is not clear whether the reduction described can also be computed in logarithmic space, since a product of polynomially many numbers of logarithmic length has to be computed.*
Nevertheless, from our results presented below it follows that MC$(^-,\times)$ *is even* $\le_\mathrm{m}^\mathrm{log}$*-hard for* PSPACE *(cf. Corollary 43).*

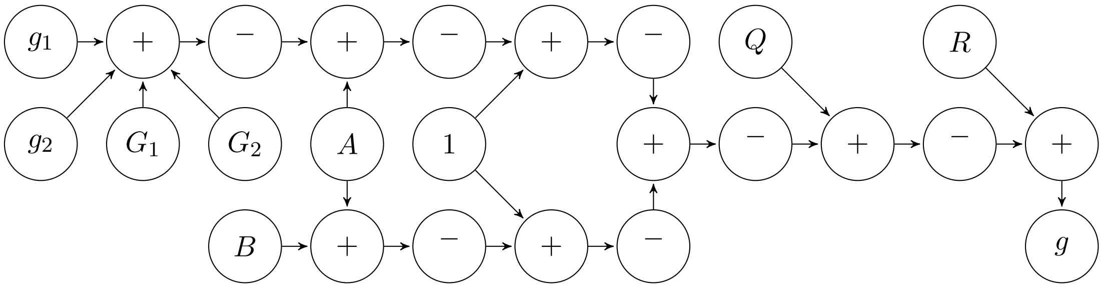
Theorem 38. MC$(^-,+)$ *is* $\le_\mathrm{m}^\mathrm{log}$*-hard for* PSPACE*.*

Proof. We show $\mathrm{MC}^+(^-,+) \leq_\mathrm{m}^\mathrm{log} \mathrm{MC}(^-,+)$. Let $C = ((V,E), g_C, \alpha)$ be a circuit over $\mathbb{N}^k$ for some $k \geq 2$ such that each input gate g satisfies $||\alpha(g)||_\infty \leq 1$. Furthermore, let $b = \sum_{i=1}^k b_i e_i \in \mathbb{N}^k$ with $b_i \leq 3$ for all i. Consider the variant of C where $+$-gates and complement-gates compute slightly modified addition and complement respectively, namely $A + B = \{x \in \{0,1,2,3\}^k \mid x = a + b \text{ for some } a \in A \text{ and some } b \in B\}$ and $\overline{A} = \{x \in \{0,1,2,3\}^k \mid x \notin A\}$ respectively ($A, B \subseteq \mathbb{N}^k$). Observe that this variant generates b if and only if the original circuit generates b. So it suffices to argue for circuits C with modified addition and modified complement.

We use the bijective mapping $f : \{0,1,\dots,7\}^k \to \{0,1,\dots,8^k-1\}$ with $f(x_1,\dots,x_k) = \sum_{i=0}^{k-1} x_{i+1} 8^i$ and describe how the pair (C,b) is transformed into an $\mathrm{MC}(^-,+)$-instance (C',b') with labeling function α' such that $(C,b) \in \mathrm{MC}^+(^-,+) \Leftrightarrow (C',b') \in \mathrm{MC}(^-,+)$.

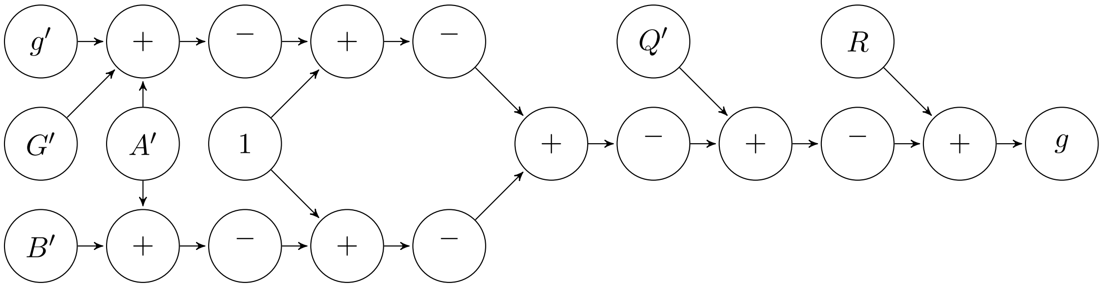
Let n be the length of the input pair (C,b). Recall that $V = \{1,2,\dots,r\}$ for some $r \in \mathbb{N}$. For the sake of simplicity, for a gate g in C we will denote the corresponding gate in C' with g as well, although this is formally not correct as for arbitrary two adjacent nodes in C there will be several new nodes between them in C', which changes the indices of the nodes.
For $m \in \mathbb{N}$ let $\widetilde{m} = 8^{n+m}$. Then let $b' = f(b) + \widetilde{g_C}$ and for each input node g of C let $\alpha'(g) = f(\alpha(g)) + \widetilde{g}$. For each inner node g in C do the following:

- If g is a $+$-node with predecessors g_1 and g_2, then delete the edges from g_1 and g_2 to g, let $\alpha'(g) = {}^-$, and add the following circuit C_g, where $G_i = \{\widetilde{g-1} - \widetilde{g_i}\}$, $A = \{2 \cdot \widetilde{g-1} - 1\}$, $B = \overline{\sum_{i=0}^{k-1} \left(\{0, 2^{3i}\} + \{0, 2^{3i+1}\}\right)} + \{2 \cdot \widetilde{g-1}\}$, $Q = \{4 \cdot \widetilde{g-1}, 6 \cdot \widetilde{g-1} - 1, 6 \cdot \widetilde{g-1}\}$, and $R = \{0, 4 \cdot \widetilde{g-1} - 1\}$:



Note that the $+$-gate with indegree 4 and all nodes computing sets with more than one element are used as an abbreviation. We denote the j-th node from the left in the i-th row by $N_{i,j}$.

- If g is a complement-node with g' in C, then remove the edge (g', g) and add the following circuit C_g, where $G' = \{\widetilde{g-1} - \widetilde{g'}\}$, $A' = \{3 \cdot \widetilde{g-1} - 1\}$, $B' = \overline{\sum_{i=0}^{k-1} \left(\{0, 2^{3i}\} + \{0, 2^{3i+1}\}\right) +} \{\widetilde{g-1}\}$, $Q' = \{4 \cdot \widetilde{g-1}\}$, and $R = \{0, 4 \cdot \widetilde{g-1} - 1\}$:



Again the $+$-gate with indegree 3 and all nodes computing sets with more than one element are used as an abbreviation. We denote the j-th gate from the left in the i-th row by $M_{i,j}$.

Claim 39. *The function $(C, b) \mapsto (C', b')$ is logspace computable.*

Proof of Claim 39. All numbers occurring in G_i, A, B, Q, R, G', A', B', and Q' can be computed in logarithmic space. Sets of natural numbers $\{a, b\}$ and $\{a, b, c\}$ for $a < b < c$ can be computed by a circuit via $\{a, b\} = \overline{\overline{\{b - a - 1\}} + \{1\}} + \{a\}$ and $\{a, b, c\} = \overline{\overline{\{b - a - 1, c - a - 1\}} + \{1\}} + \{a\}$ Consequently, there is a logspace computable circuit which computes the set $\sum_{i=0}^{k-1} \left(\{0, 2^{3i}\} + \{0, 2^{3i+1}\}\right)$. □

For $m \in \mathbb{N}^+$ let $D_m = \{0, \dots, \widetilde{m} - 1\}$, $E_m = \{\widetilde{m}, \dots, \widetilde{m} + 8^k - 1\}$, $D^2_m = \{0, \dots, 2 \cdot \widetilde{m} - 1\}$, $E^2_m = \{2 \cdot \widetilde{m}, \dots, 2 \cdot \widetilde{m} + 8^k - 1\}$, $D^4_m = \{0, \dots, 4 \cdot \widetilde{m} - 1\}$, and $E^4_m = \{4 \cdot \widetilde{m}, \dots, 4 \cdot \widetilde{m} + 8^k - 1\}$. Moreover, $F_m = D_m \cup E_m = \{0, \dots, \widetilde{m} + 8^k - 1\}$ and $F^i_m = D^i_m \cup E^i_m = \{0, \dots, i \cdot \widetilde{m} + 8^k - 1\}$ for $i \in \{2, 4\}$. Note that F_m, F^2_m, and F^4_m are intervals of $\mathbb{N}$ that start at 0.

Claim 40. *For each gate g of C it holds $I(g, C') \cap F_g = \{f(x) + \widetilde{g} \mid x \in I(g; C)\}$.*

Proof of Claim 40. Throughout this proof, x will denote an element of $\mathbb{N}^k$.
If g is an input node, the statement holds. Assume g is an inner node and the statement is true for all nodes $g' < g$.

We assume g is a $+$-gate in C with predecessors g_1 and g_2. First we argue that

$$B \cap F^2_{g-1} = \{f(x) + 2 \cdot \widetilde{g - 1} \mid 4 \leq ||x||_\infty \leq 7\} : \tag{2}$$

Let $y \in B \cap F^2_{g-1}$, hence $y = y' + 2 \cdot \widetilde{g-1}$ with $y' \notin \sum_{i=0}^{k-1} \left(\{0, 2^{3i}\} + \{0, 2^{3i+1}\}\right)$ and $y' < 8^k$. Because of this and as f is bijective, there is a unique $z \in \{0, 1, \dots, 7\}^k$ with $f(z) = y'$ and $||z||_\infty \in \{4, 5, 6, 7\}$, which shows $\subseteq$. Conversely, let $y = f(z) + 2 \cdot \widetilde{g-1}$ with $||z||_\infty \in \{4, 5, 6, 7\}$. Hence $f(z) \notin \sum_{i=0}^{k-1} \left(\{0, 2^{3i}\} + \{0, 2^{3i+1}\}\right)$, which proves (2).
Now, we argue for

$$\underbrace{\overline{\overline{A + B} + 1} \cap F^4_{g-1}}_{=:LHS} = \underbrace{\{0\} \cup \{f(x) + 4 \cdot \widetilde{g - 1} \mid x \in \mathbb{N}^k \wedge 4 \leq ||x||_\infty \leq 7\}}_{=:RHS} : \tag{3}$$

Let $y \in LHS$. Then $y = 0 \in RHS$ or it holds $y > 0$ and $y - 1 \notin \overline{A + B}$ and $y \in F^4_{g-1}$. Thus $y - 1 \in (A + B) \cap \{0, \dots, 4 \cdot \widetilde{g-1} + 8^k - 2\} = A + (B \cap F^2_{g-1}) \overset{(2)}{=} \{f(x) + 4 \cdot \widetilde{g-1} - 1 \mid 4 \leq ||x||_\infty \leq 7\}$ which implies $y \in RHS$.
Conversely, let $y \notin LHS$, hence $y \notin F^4_{g-1} \supseteq RHS$ and we are done or $y \in F^4_{g-1}$ and $y \in \overline{A + B} + 1$. Thus $y > 0$ and it holds $y - 1 \notin (A + B) \cap \{0, \dots, 4 \cdot \widetilde{g-1} + 8^k - 2\} = A + (B \cap F^2_{g-1}) \overset{(2)}{=} \{f(x) + 4 \cdot \widetilde{g-1} - 1 \mid 4 \leq ||x||_\infty \leq 7\}$. Hence $y \notin RHS$, which proves (3).

By induction hypothesis one has $I(g_i; C') \cap F_{g_i} = \{f(x) + \widetilde{g_i} \mid x \in I(g_i; C\}$ and hence

$$(I(g_i; C') + G_i) \cap F_{g-1} = \{f(x) + \widetilde{g - 1} \mid x \in I(g_i; C)\} \text{ for } i = 1, 2. \tag{4}$$

Let us observe that

$$\overline{I(g_1; C') + I(g_2; C') + G_1 + G_2} \subseteq \overline{\{f(x) + 2 \cdot \widetilde{g - 1} \mid x \in I(g; C)\}}. \tag{5}$$

Otherwise there exists an element y on the left-hand side such that $y = f(x) + 2 \cdot \widetilde{g-1}$ for some $x \in I(g; C)$ and hence $y = f(x_1) + \widetilde{g-1} + f(x_2) + \widetilde{g-1}$ for suitable $x_i \in I(g_i; C)$. By (4), $f(x_i) + \widetilde{g-1} \in I(g_i; C') + G_i$ and hence $y \in I(g_1; C') + I(g_2; C') + G_1 + G_2$. This is a contradiction and shows (5).

Next we argue for

$$\overline{I(g_1;C')+I(g_2;C')+G_1+G_2} \supseteq \overline{\{f(x)+2\cdot\widetilde{g-1} \mid x\in I(g;C)\vee 4\le \|x\|_\infty\le 7\}}\cap F^2_{g-1}. \tag{6}$$

It suffices to show that every $y\in(I(g_1;C')+I(g_2;C')+G_1+G_2)\cap F^2_{g-1}$ belongs to $\{f(x)+2\cdot\widetilde{g-1} \mid x\in I(g;C)\vee 4\le\|x\|_\infty\le 7\}$. By assumption, $y=y_1+y_2$ for suitable $y_i\in I(g_i;C')+G_i$. Together with (4) we obtain $y_1,y_2\ge\widetilde{g-1}$. If $y_i\notin F_{g-1}$ for some $i\in\{1,2\}$, then $y_i\ge\widetilde{g-1}+8^k$ and hence $y\ge 2\cdot\widetilde{g-1}+8^k\notin F^2_{g-1}$, a contradiction. So $y_1,y_2\in F_{g-1}$. By (4), for $i\in\{1,2\}$ there exists $x_i\in I(g_i;C)$ such that $y_i=f(x_i)+\widetilde{g-1}$. Hence $y=f(x_1+x_2)+2\cdot\widetilde{g-1}$. If $\|x_1+x_2\|_\infty\le 3$, then $y\in\{f(x)+2\cdot\widetilde{g-1}\mid x\in I(g;C)\}$, otherwise $y\in\{f(x)+2\cdot\widetilde{g-1}\mid x\in\mathbb{N}^k\wedge 4\le\|x\|_\infty\le 7\}$. This proves (6).

Consequently, due to

$$\begin{aligned}
I(N_{1,6};C')\cap F^4_{g-1} &= \big(\overline{\overline{I(g_1;C')+I(g_2;C')+G_1+G_2}+A}+\{1\}\big)\cap F^4_{g-1}\\
&= \big(\overline{(\overline{I(g_1;C')+I(g_2;C')+G_1+G_2}\cap F^2_{g-1})+A}+\{1\}\big)\cap F^4_{g-1}
\end{aligned}$$

it holds

$$\begin{aligned}
&I(N_{1,6};C')\cap F^4_{g-1} \overset{(5)}{\supseteq} \big(\overline{(\overline{\{f(x)+2\cdot\widetilde{g-1}\mid x\in I(g;C)\}}\cap F^2_{g-1})+A}+\{1\}\big)\cap F^4_{g-1}\\
&\quad= \big(\overline{(D^2_{g-1}\cup\{f(x)+2\cdot\widetilde{g-1}\mid x\in\{0,1,\dots,7\}^k-I(g;C)\})+A}+\{1\}\big)\cap F^4_{g-1}\\
&\quad= \big(\overline{\{2\cdot\widetilde{g-1}-1,\dots,4\cdot\widetilde{g-1}-2\}\cup\{f(x)+4\cdot\widetilde{g-1}-1\mid x\in\{0,1,\dots,7\}^k-I(g;C)\}}+\{1\}\big)\cap F^4_{g-1}\\
&\quad= \big((\{0,\dots,2\cdot\widetilde{g-1}-2\}\cup\{f(x)+4\cdot\widetilde{g-1}-1\mid x\in I(g;C)\})+\{1\}\big)\cap F^4_{g-1}\\
&\quad= \{1,\dots,2\cdot\widetilde{g-1}-1\}\cup\{f(x)+4\cdot\widetilde{g-1}\mid x\in I(g;C)\} \qquad (7)
\end{aligned}$$

and analogously

$$\begin{aligned}
&I(N_{1,6};C')\cap F^4_{g-1} \overset{(6)}{\subseteq} \big(\overline{(\overline{\{f(x)+2\cdot\widetilde{g-1}\mid x\in I(g;C)\vee 4\le\|x\|_\infty\le 7\}}\cap F^2_{g-1})+A}+\{1\}\big)\cap F^4_{g-1}\\
&\quad= \big(\overline{(D^2_{g-1}\cup\{f(x)+2\cdot\widetilde{g-1}\mid x\in\{0,1,2,3\}^k-I(g;C)\})+A}+\{1\}\big)\cap F^4_{g-1}\\
&\quad= \big(\overline{\{2\cdot\widetilde{g-1}-1,\dots,4\cdot\widetilde{g-1}-2\}\cup\{f(x)+4\cdot\widetilde{g-1}-1\mid x\in\{0,1,2,3\}^k-I(g;C)\}}+\{1\}\big)\cap F^4_{g-1}\\
&\quad= \big((\{0,\dots,2\cdot\widetilde{g-1}-2\}\cup\{f(x)+4\cdot\widetilde{g-1}-1\mid x\in I(g;C)\vee 4\le\|x\|_\infty\le 7\})+\{1\}\big)\cap F^4_{g-1}\\
&\quad= \{1,\dots,2\cdot\widetilde{g-1}-1\}\cup\{f(x)+4\cdot\widetilde{g-1}\mid x\in I(g;C)\vee 4\le\|x\|_\infty\le 7\}. \qquad (8)
\end{aligned}$$

Hence we obtain

$$\begin{aligned}
&\{0,2\cdot\widetilde{g-1},\dots,4\cdot\widetilde{g-1}-1\}\cup\{f(x)+4\cdot\widetilde{g-1}\mid x\in\{0,1,2,3\}^k-I(g;C)\}\\
&= \overline{\{1,\dots,2\cdot\widetilde{g-1}-1\}\cup\{f(x)+4\cdot\widetilde{g-1}\mid x\in I(g;C)\vee 4\le\|x\|_\infty\le 7\}}\cap F^4_{g-1}\\
&\overset{(8)}{\subseteq} \overline{I(N_{1,6};C')}\cap F^4_{g-1} = I(N_{1,7};C')\cap F^4_{g-1} \qquad (9)\\
&\overset{(7)}{\subseteq} \overline{\{1,\dots,2\cdot\widetilde{g-1}-1\}\cup\{f(x)+4\cdot\widetilde{g-1}\mid x\in I(g;C)\}}\cap F^4_{g-1}\\
&= \{0,2\cdot\widetilde{g-1},\dots,4\cdot\widetilde{g-1}-1\}\cup\{f(x)+4\cdot\widetilde{g-1}\mid x\in\{0,1,\dots,7\}^k-I(g;C)\}. \qquad (10)
\end{aligned}$$

By the definition of the circuit C_g, $I(N_{2,6};C')=I(N_{1,7};C')+\overline{\overline{A+B}+1}$. By (10), all positive elements in $I(N_{1,7},C')$ are $\ge 2\cdot\widetilde{g-1}$. By (3), all positive elements in $\overline{\overline{A+B}+1}$

are $\geq 4 \cdot \widetilde{g-1}$. As $\widetilde{g-1} > 8^n > 8^k$ (the latter holds since $b \in \mathbb{N}^k$ is part of the input) it holds that if $y \in I(N_{2,6}, C') \cap F^4_{g-1}$, then $y \in I(N_{1,7}, C')$ or $y \in \overline{\overline{A+B}+1}$. Therefore, $I(N_{2,6}; C') \cap F^4_{g-1} = \big(I(N_{1,7}; C') \cap F^4_{g-1}\big) \cup \big(\overline{\overline{A+B}+1} \cap F^4_{g-1}\big)$ and thus

$$\begin{aligned}
&I(N_{2,6};C') \cap F^4_{g-1}\\
&\qquad\overset{(10)}{\subseteq} \{0\} \cup \{2 \cdot \widetilde{g-1}, \dots, 4 \cdot \widetilde{g-1} - 1\} \cup\\
&\qquad\quad \{f(x) + 4 \cdot \widetilde{g-1} \mid x \in \{0,1,\dots,7\}^k - I(g;C)\} \cup \{f(x) + 4 \cdot \widetilde{g-1} \mid 4 \leq ||x||_\infty \leq 7\}\\
&\qquad= \{0\} \cup \{2 \cdot \widetilde{g-1}, \dots, 4 \cdot \widetilde{g-1} - 1\} \cup \{f(x) + 4 \cdot \widetilde{g-1} \mid x \in \{0,1,\dots,7\}^k - I(g;C)\}
\end{aligned}$$

and

$$\begin{aligned}
&I(N_{2,6};C') \cap F^4_{g-1}\\
&\qquad\overset{(3),(9)}{\supseteq} \{0\} \cup \{2 \cdot \widetilde{g-1}, \dots, 4 \cdot \widetilde{g-1} - 1\} \cup\\
&\qquad\quad \{f(x) + 4 \cdot \widetilde{g-1} \mid x \in \{0,1,2,3\}^k - I(g;C)\} \cup \{f(x) + 4 \cdot \widetilde{g-1} \mid 4 \leq ||x||_\infty \leq 7\}\\
&\qquad= \{0, 2 \cdot \widetilde{g-1}, \dots, 4 \cdot \widetilde{g-1} - 1\} \cup \{f(x) + 4 \cdot \widetilde{g-1} \mid x \in \{0,1,\dots,7\}^k - I(g;C)\}.
\end{aligned}$$

Thus

$$I(N_{2,6}; C') \cap F^4_{g-1} = \{0, 2 \cdot \widetilde{g-1}, \dots, 4 \cdot \widetilde{g-1} - 1\} \cup \{f(x) + 4 \cdot \widetilde{g-1} \mid x \in \{0,1,\dots,7\}^k - I(g;C)\}.$$

This yields $I(N_{2,7}; C') \cap F^4_{g-1} = \{1, \dots, 2 \cdot \widetilde{g-1} - 1\} \cup \{f(x) + 4 \cdot \widetilde{g-1} \mid x \in I(g;C)\}$. It follows from $\widetilde{g} > 8^n > 8^k$ that $10 \cdot \widetilde{g-1} - 1 \notin F_g$ and thus $(\{f(x) + 4 \cdot \widetilde{g-1} \mid x \in I(g;C)\} + \{6 \cdot \widetilde{g-1} - 1, 6 \cdot \widetilde{g-1}\}) \cap F_g = \emptyset$. Therefore, we obtain

$$\begin{aligned}
I(N_{2,8}; C') \cap F_g &= \big(\big(I(N_{2,7}; C') \cap F^4_{g-1}\big) + Q\big) \cap F_g\\
&= \big(\{1, \dots, 2 \cdot \widetilde{g-1} - 1\} + Q\big) \cup \big(\{f(x) + 4 \cdot \widetilde{g-1} \mid x \in I(g;C)\} + \{4 \cdot \widetilde{g-1}\}\big)\\
&= \{4 \cdot \widetilde{g-1} + 1, \dots, \widetilde{g} - 1\} \cup \{f(x) + \widetilde{g} \mid x \in I(g;C)\}
\end{aligned}$$

and for similar reasons

$$\begin{aligned}
&I(N_{2,10}; C') \cap F_g = \big(\overline{\{4 \cdot \widetilde{g-1} + 1, \dots, \widetilde{g} - 1\} \cup \{f(x) + \widetilde{g} \mid x \in I(g;C)\}} + R\big) \cap F_g\\
&\quad= \big((\{0, \dots, 4 \cdot \widetilde{g-1}\} + R) \cap F_g\big) \cup \big((\{f(x) + \widetilde{g} \mid x \in \{0,1,\dots,7\}^k - I(g;C)\} + R) \cap E_g\big)\\
&\quad= \{0, \dots, \widetilde{g} - 1\} \cup (\{f(x) + \widetilde{g} \mid x \in \{0,1,\dots,7\}^k - I(g;C)\}.
\end{aligned}$$

Consequently, $I(g; C') \cap F_g = \{f(x) + \widetilde{g} \mid x \in I(g;C)\}$.

Now we assume that g is a complement-gate with predecessor g' in C. Since $A+B = A'+B'$, from (3) we obtain

$$\overline{\overline{A' + B'} + 1} \cap F^4_{g-1} = \{0\} \cup \{f(x) + 4 \cdot \widetilde{g-1} \mid 4 \leq ||x||_\infty \leq 7\}. \tag{11}$$

From the induction hypothesis we obtain $(I(g'; C') + G') \cap F_{g-1} = \{f(x) + \widetilde{g-1} \mid x \in I(g'; C)\} = \{f(x) + \widetilde{g-1} \mid x \in \{0,1,2,3\}^k - I(g;C)\}$. This yields $\overline{I(g'; C') + G' + A'} \cap \{0, \dots, 4 \cdot \widetilde{g-1} + 8^k - 2\} = \{0, \dots, 4 \cdot \widetilde{g-1} - 2\} \cup \{f(x) + 4 \cdot \widetilde{g-1} - 1 \mid x \in I(g;C) \vee 4 \leq ||x||_\infty \leq 7\}$ and thus

$$I(M_{1,5}; C') \cap F^4_{g-1} = \{0\} \cup \{f(x) + 4 \cdot \widetilde{g-1} \mid x \in \{0,1,2,3\}^k - I(g;C)\}. \tag{12}$$

By (11) and (12) all positive elements of $\overline{\overline{A'+B'}+1}\cap F^4_{g-1}$ and $I(M_{1,5};C')\cap F^4_{g-1}$ are at least $4\cdot\widetilde{g-1}$. Since $8\cdot\widetilde{g-1}>8^n>8^k$ it holds

$$\begin{aligned}I(M_{2,4};C')\cap F^4_{g-1} &= (I(M_{1,5};C')\cap F^4_{g-1})+(\overline{\overline{A'+B'}+1}\cap F^4_{g-1})\\ &= (I(M_{1,5};C')\cap F^4_{g-1})\cup(\overline{\overline{A'+B'}+1}\cap F^4_{g-1})\\ &= \{0\}\cup\{f(x)+4\cdot\widetilde{g-1}\mid x\in\{0,1,2,3\}^k-I(g;C)\}\cup\{f(x)+4\cdot\widetilde{g-1}\mid 4\le\|x\|_\infty\le 7\}\\ &= \{0\}\cup\{f(x)+4\cdot\widetilde{g-1}\mid x\in\{0,1,\dots,7\}^k-I(g;C)\},\end{aligned}$$

which implies

$$\begin{aligned}I(M_{2,7};C')\cap F_g &= \overline{\overline{I(M_{2,4};C')\cap F^4_{g-1}}+Q'}\cap F_g\\ &= \overline{\Big(\{1,\dots,4\cdot\widetilde{g-1}-1\}\cup\{f(x)+4\cdot\widetilde{g-1}\mid x\in I(g;C)\}\Big)+Q'}\cap F_g\\ &= D^4_{g-1}\cup\{4\cdot\widetilde{g-1}\}\cup\{f(x)+\widetilde{g}\mid x\in\{0,1,\dots,7\}^k-I(g;C)\}.\end{aligned}$$

Consequently,

$$\begin{aligned}I(g,C')\cap F_g &= \overline{\big(I(M_{2,7};C')\cap F_g\big)+R}\cap F_g\\ &= \overline{\big((D^4_{g-1}\cup\{4\cdot\widetilde{g-1}\})+R\big)\cup\big((\{f(x)+\widetilde{g}\mid x\in\{0,1,\dots,7\}^k-I(g;C)\}+R)\cap F_g\big)}\cap F_g\\ &= \overline{D_g\cup\big(\{f(x)+\widetilde{g}\mid x\in\{0,1,\dots,7\}^k-I(g;C)\}+\{0\}\big)}\cap F_g\\ &= \overline{D_g\cup\{f(x)+\widetilde{g}\mid x\in\{0,1,\dots,7\}^k-I(g;C)\}}\cap F_g=\{f(x)+\widetilde{g}\mid x\in I(g;C)\}.\end{aligned}$$

□

It follows from the claim that $(C,b)\in\mathrm{MC}^+(^-,+)\Leftrightarrow(C',b')\in\mathrm{MC}(^-,+)$. This completes the proof. □

The following lemma is essentially due to Sigmund [Sig16]. He provided the proof of the second statement and the main idea of the proof of the first statement.

Lemma 41. *It holds*

1. $\mathrm{NMC}(^-,+)\le^{\log}_{\mathrm{m}}\mathrm{EC}(^-,+)$ *and*
2. $\mathrm{EC}(^-,+)\le^{\log}_{\mathrm{m}}\mathrm{EC}(^-,\times)$

Proof. 1. Let C be a completely assigned $\{^-,+\}$-circuit and $b\in\mathbb{N}$. It holds $\{1,\dots,b\}=\overline{\overline{\{0\}}+\{b-1\}}+\{1\}$ and $\{b+2,\dots,2b+2\}=\overline{\overline{0}+\{b\}}+\{b+2\}$. Let without loss of generality $0\in I(C)$ (else consider $(\overline{\overline{C}+\{1\}},b+1)$ instead of (C,b)).

1. Let $M=\overline{I(C)+\overline{\{1,\dots,b\}}+\{1\}}$. Because of $0\in I(C)$ and $\overline{\{1,\dots,b\}}=\{0\}\cup\{b+1,\dots\}$ we have $I(C)+\overline{\{1,\dots,b\}}=I(C)\cup\{b+1,\dots\}$. Hence $M=\overline{(I(C)\cup\{b+1,\dots\})+\{1\}}=\overline{(I(C)+\{1\})\cup\{b+2,\dots\}}=\overline{I(C)+\{1\}}\cap\{0,\dots,b+1\}=\{0\}\cup\{x+1\mid x\notin I(C)\wedge x\le b\}$.
2. Let $M':=\overline{M+\overline{\{b+2,\dots,2b+2\}}}$. Due to $0\in M$ and $\overline{\{b+2,\dots,2b+2\}}=\{0,\dots,b+1\}\cup\{2b+3,\dots\}$ we have $M+\overline{\{b+2,\dots,2b+2\}}=(M+\{0,\dots,b+1\})\cup(M+\{2b+3,\dots\})=\{0,\dots,b+1+\max M\}\cup\{2b+3,\dots\}$. Thus $M'=\{b+2+\max M,\dots,2b+2\}$. So we get $M'=\emptyset\Leftrightarrow\max M>b\Leftrightarrow\max M=b+1\Leftrightarrow b+1\in M\Leftrightarrow b\notin I(C)$.

Let C' the $\{^-,+\}$-circuit for M' and note that C' can be computed in logarithmic space. According to our argumentation above it holds $(C,b) \in \mathrm{NMC}(^-,+) \Leftrightarrow C' \in \mathrm{EC}(^-,+)$.

2. Let $f : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ with $f(A) = \{2^a \mid a \in A\} \times (2\mathbb{N}+1) = \{2^a \cdot (2n+1) \mid a \in A, n \in \mathbb{N}\}$, where $\mathcal{P}(\mathbb{N}) = \{A \mid A \subseteq \mathbb{N}\}$. Let C be a completely assigned $\{^-,+\}$-circuit. With the following modifications we receive a $\{^-,\times\}$-circuit C':

1. Replace each $+$-gate with a $\times$-gate.
2. Replace each input gate g with a $\{^-,\times\}$-circuit C_g such that the output node g_{C_g} of C_g is connected to all successors of g and g_{C_g} computes the set $f(I(g;C)) = \{2^{I(g;C)} \cdot (2n+1) \mid n \in \mathbb{N}\}$. Note that such a circuit can be computed in logarithmic space since $2^{I(g;C)}$ can be computed via the binary representation of $I(g;C)$, which is part of the input, and $2\mathbb{N}+1 = \overline{\{2\} \times \overline{2} \times \overline{3}}$.
3. For each complement-gate g and its predecessor g' add new nodes such that we have $g = \overline{g' \times ((2\mathbb{N}+1) \cup \{0\})}$, where $(2\mathbb{N}+1) \cup \{0\} = \overline{\{2\} \times \overline{\{0\}}}$.

To complete the proof we show the following statement inductively: For each gate g in C it holds $I(g;C') = f(I(g;C))$.

If g is an input gate of C, the statement is true. Let g be a $\times$-node with predecessors g_1 and g_2. By induction hypothesis it holds $I(g_i;C') = f(I(g_i;C))$ for $i = 1,2$. Hence

$$\begin{aligned} I(g;C') &= (\{2^x \mid x \in I(g_1;C)\} \times (2\mathbb{N}+1)) \times (\{2^x \mid x \in I(g_2;C)\} \times (2\mathbb{N}+1)) \\ &= \{2^{x+y} \mid x \in I(g_1;C), y \in I(g_2;C)\} \times (2\mathbb{N}+1) \\ &= f(I(g;C)). \end{aligned}$$

Now, assume g is a $^-$-gate with predecessor g'. By induction hypothesis it holds $I(g';C') = f(I(g';C))$. Thus

$$\begin{aligned} I(g;C') &= \overline{I(g';C') \times ((2\mathbb{N}+1) \cup \{0\})} = \overline{f(I(g';C)) \times ((2\mathbb{N}+1) \cup \{0\})} \\ &= \overline{\{2^x \mid x \in I(g';C)\} \times (2\mathbb{N}+1) \times ((2\mathbb{N}+1) \cup \{0\})} \\ &= \overline{(\{2^x \mid x \in I(g';C)\} \times ((2\mathbb{N}+1))) \cup \{0\}} \\ &= \{2^x \mid x \notin I(g';C)\} \times (2\mathbb{N}+1) \\ &= f(I(g;C)). \end{aligned}$$

□

Theorem 42. $\mathrm{EC}(^-,+)$ *and* $\mathrm{EC}(^-,\times)$ *are* $\leq_{\mathrm{m}}^{\log}$*-hard for* PSPACE.

Proof. Both statements follow from Lemma 41. □

With these results we can improve the lower bound for $\mathrm{MC}(^-,\times)$ stated in Corollary 36.

Corollary 43. $\mathrm{MC}(^-,\times)$ *is* $\leq_{\mathrm{m}}^{\log}$*-hard for* PSPACE.

Proof. The statement follows from Theorem 42 and Lemma 2. □

6 Circuits with both Arithmetic Operations

Besides proving bounds for emptiness problems with $+$ and $\times$, we improve the known lower and upper bounds for $\mathrm{MC}(\cup, \cap, ^-, +, \times)$ [MW07] and $\mathrm{EQ}(\cup, \cap, ^-, +, \times)$ [GHR+10]. 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 $\mathrm{MC}(\cap, +, \times)$ [MW07], $\mathrm{MC}_{\mathbb{Z}}(\cap, +, \times)$, $\mathrm{MC}_{\mathbb{Z}}(+, \times)$ [Tra06], and $\mathrm{EQ}(+, \times)$ [GHR+10] are reformulations of the well-studied, major open question for the complexity of PIT.

6.1 Upper and Lower Bounds for Undecidable Problems

We start by proving upper and lower bounds for certain undecidable emptiness problems.

Theorem 44.

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

Proof. 1. It suffices to show $\mathrm{EC}(\cup, \cap, ^-, +, \times) \leq_{\mathrm{tt}} K$. By [GHR+10, Lemma 5], there exists a Turing machine M with oracle K that on input of a completely assigned $\{\cup, \cap, ^-, +, \times\}$-circuit C computes a completely assigned $\{\cup, \cap, ^-, +, \times\}$-circuit D and a set $Z \subseteq \{0\}$ such that the label 0 does not appear in D and $I(C) = I_{\mathbb{N}^+}(D) \cup Z$. Here $I_{\mathbb{N}^+}(D)$ denotes the set computed by D when gates with label $^-$ compute the complement with respect to $\mathbb{N}^+$. The proof of [GHR+10, Lemma 5] shows that M on input C asks at most 3^n adaptive queries, where n is the number of gates in C. These queries can be replaced by $3^n \cdot 2^{3^n}$ nonadaptive queries (i.e., 3^n queries for each of the 2^{3^n} possible answer vectors). Moreover, Breunig [Bre07] shows that on input (D, x) where $x \in \mathbb{N}$ it is decidable in polynomial space whether $x \in I_{\mathbb{N}^+}(D)$. Hence with one additional query to K we can determine whether $I_{\mathbb{N}^+}(D)$ is empty, which in turn allows us to decide whether $I(C) = I_{\mathbb{N}^+}(D) \cup Z$ is empty. This shows $\mathrm{EC}(\cup, \cap, ^-, +, \times) \leq_{\mathrm{tt}} K$.

2. Σ_1-$\mathrm{EC}(\cup, \cap, ^-, +, \times)$ is computably enumerable in $\mathrm{EC}(\cup, \cap, ^-, +, \times)$. By statement 1 this shows Σ_1-$\mathrm{EC}(\cup, \cap, ^-, +, \times) \in \Sigma_2$. Similarly we obtain Π_1-$\mathrm{EC}(\cup, \cap, ^-, +, \times) \in \Pi_2$.

3. By Corollary 3, $\mathrm{EC}(\cup, \cap, +, \times)$ is decidable and hence Π_1-$\mathrm{EC}(\cup, \cap, +, \times) \in \Pi_1$. By the Matiyasevich-Robinson-Davis-Putnam theorem [Mat70, DPR61], there exists an $n \in \mathbb{N}$ and a multivariate polynomial p with integer coefficients such that for every $A \in \Sigma_1$ there exists an $a \in \mathbb{N}$ such that

$$x \in A \iff \exists y \in \mathbb{N}^n, p(a, x, y) = 0.$$

In the equation $p(a, x, y) = 0$ we can move negative monomials and negative constants to the right-hand side. This yields multivariate polynomials l and r with coefficients from $\mathbb{N}$ such that

$$x \in A \iff \exists y \in \mathbb{N}^n, l(a, x, y) = r(a, x, y).$$

Let C_l and C_r be $\{+, \times\}$-circuits computing the polynomials l and r, respectively. Hence

$$\begin{aligned} x \in \overline{A} &\iff \forall y \in \mathbb{N}^n, C_l(a, x, y) \neq C_r(a, x, y) \\ &\iff (C_l(a, x, \cdot) \cap C_r(a, x, \cdot)) \in \Pi_1\text{-}\mathrm{EC}(\cap, +, \times), \end{aligned}$$

where $C_l(a, x, \cdot)$ and $C_r(a, x, \cdot)$ denote the circuits obtained from C_l and C_r by assigning a and x to the first inputs, while leaving the remaining inputs unassigned. On input x, the $\{\cap, +, \times\}$-circuit $C_l(a, x, \cdot) \cap C_r(a, x, \cdot)$ can be constructed in logarithmic space, since C_l, C_r, and a do not depend on x. So $\overline{A} \leq_{\mathrm{m}}^{\log} \Pi_1\text{-EC}(\cap, +, \times)$, which proves the third statement of the theorem.

4+5. For $A \in \Sigma_1$ let a, C_l, and C_r be as above. So it holds that

$$x \in A \iff \exists y \in \mathbb{N}^n, C_l(a, x, y) = C_r(a, x, y). \tag{13}$$

It remains to formulate the equality on the right-hand side as a membership (resp., emptiness) problem. For this we define the following auxiliary circuits, where $x, y \in \mathbb{N}$, the set $\{0, 1\}$ is generated by $\overline{\overline{\{0\}} + \{1\}}$, and the set $\mathbb{N}$ is generated by $\overline{\{1\}} + \overline{\{2\}}$.

$$C_1(x,y) \overset{df}{=} \overline{\overline{\{y\} + \{1\}} + ((\{x\} + \{1\}) \times \{0,1\})} = \begin{cases} \{y+1\} & \text{if } x > y \\ \emptyset & \text{otherwise} \end{cases}$$

$$C_2(x,y) \overset{df}{=} \overline{\overline{\{0\} \times C_1(x,y)} + \{1\}} = \begin{cases} \{0,1\} & \text{if } x > y \\ \{0\} & \text{otherwise} \end{cases}$$

$$C_3(x,y) \overset{df}{=} C_2(x,y) + C_2(y,x) = \begin{cases} \{0,1\} & \text{if } x \neq y \\ \{0\} & \text{otherwise} \end{cases}$$

From (13) we obtain

$$\begin{aligned} x \in A &\iff \exists y \in \mathbb{N}^n, 1 \in \overline{C_3(C_l(a,x,y), C_r(a,x,y))} \\ &\iff (\overline{C_3(C_l(a,x,y), C_r(a,x,y))}, 1) \in \Sigma_1\text{-MC}({}^-, +, \times). \end{aligned}$$

This shows $A \leq_{\mathrm{m}}^{\log} \Sigma_1\text{-MC}({}^-, +, \times)$, since the circuits C_3, C_l, and C_r do not depend on x.

For $\Sigma_1\text{-EC}({}^-, +, \times)$ we define further auxiliary circuits.

$$C_4(x,y) \overset{df}{=} \{1\} + C_3(x,y) = \begin{cases} \{1,2\} & \text{if } x \neq y \\ \{1\} & \text{otherwise} \end{cases}$$

$$C_5(x,y) \overset{df}{=} \overline{C_4(x,y)} + \{0,1\} = \begin{cases} \overline{\{2\}} & \text{if } x \neq y \\ \mathbb{N} & \text{otherwise} \end{cases}$$

We obtain $A \leq_{\mathrm{m}}^{\log} \Sigma_1\text{-EC}({}^-, +, \times)$, since by (13) the following holds.

$$\begin{aligned} x \in A &\iff \exists y \in \mathbb{N}^n, \overline{C_5(C_l(a,x,y), C_r(a,x,y))} = \emptyset \\ &\iff \overline{C_5(C_l(a,x,y), C_r(a,x,y))} \in \Sigma_1\text{-EC}({}^-, +, \times) \end{aligned}$$

For $\Pi_1\text{-EC}({}^-, +, \times)$ let

$$C_6(x,y) \overset{df}{=} C_3(x,y) + (\{2\} \times \mathbb{N}) = \begin{cases} \mathbb{N} & \text{if } x \neq y \\ 2\mathbb{N} & \text{otherwise.} \end{cases}$$

We obtain $\overline{A} \leq_{\mathrm{m}}^{\log} \Pi_1\text{-EC}({}^-, +, \times)$, since by (13) the following holds.

$$\begin{aligned} x \in \overline{A} &\iff \forall y \in \mathbb{N}^n, \overline{C_6(C_l(a,x,y), C_r(a,x,y))} = \emptyset \\ &\iff \overline{C_6(C_l(a,x,y), C_r(a,x,y))} \in \Pi_1\text{-EC}({}^-, +, \times) \end{aligned}$$

□

6.2 Connecting Emptiness with Membership and Equivalence Problems

We show that with the operations $^-$, $+$, and $\times$ 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 $\mathrm{MC}(\cup, \cap, ^-, +, \times)$ [MW07] and $\mathrm{EQ}(\cup, \cap, ^-, +, \times)$ [GHR⁺10].

Lemma 45. *If $\{^-, +, \times\} \subseteq \mathcal{O}$ and $B \in \mathrm{P}$, then there exists an $f \in \mathrm{FL}$ such that for all $\mathcal{O}$-circuits $C_1, \dots, C_n$ it holds that $(c_{\mathrm{EC}(\mathcal{O})}(C_1), \dots, c_{\mathrm{EC}(\mathcal{O})}(C_n)) \in B \Leftrightarrow f(C_1, \dots, C_n) \in \mathrm{EC}(\mathcal{O})$.*

Proof. Ladner [Lad75] showed that the circuit value problem is $\leq_{\mathrm{m}}^{\log}$-complete for P. From the proof it follows that one can construct in logarithmic space in n a Boolean circuit C over $\{\vee, \neg\}$ such that for all $b_1, \dots, b_n \in \{0, 1\}$, $C(b_1, \dots, b_n) = c_B(b_1, \dots, b_n)$. We translate C into an $\mathcal{O}$-circuit C', where a Boolean value 1 (resp., 0) is represented by the empty (resp., a nonempty) set. First we replace C's inputs with $C_1, \dots, C_n$, which represent the Boolean values $c_{\mathrm{EC}(\mathcal{O})}(C_1), \dots, c_{\mathrm{EC}(\mathcal{O})}(C_n)$. Each $\vee$-gate can be replaced with a $+$-gate, since the sum of two $\mathcal{O}$-circuits is empty if and only if one of them generates the empty set. A $\neg$-gate with predecessor x can be replaced with the circuit $\overline{((x \times \{0\}) + \overline{\{1\}} + \overline{\{2\}}}\,)$, which is of constant size. This circuit generates the empty set if and only if x does not compute the empty set. Overall we obtain an $\mathcal{O}$-circuit C' in logarithmic space such that $(c_{\mathrm{EC}(\mathcal{O})}(C_1), \dots, c_{\mathrm{EC}(\mathcal{O})}(C_n)) \in B \Leftrightarrow C' \in \mathrm{EC}(\mathcal{O})$. □

Proposition 46. *The following holds if $\{^-, +, \times\} \subseteq \mathcal{O}$.*

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

Proof. If $A \leq_{\mathrm{tt}}^{\log} \mathrm{EC}(\mathcal{O})$, then there exists a nonadaptive logspace oracle Turing machine M that accepts A with $\mathrm{EC}(\mathcal{O})$ as oracle. Hence there exists a logspace computable function q and a logspace Turing machine M' such that

1. $q(x) = (C_1, \dots, C_n)$ is the sequence of queries of the computation $M(x)$ and
2. M' on input x together with the oracle answers computes $c_A(x)$, i.e.,
   $M'(x, c_{\mathrm{EC}(\mathcal{O})}(C_1), \dots, c_{\mathrm{EC}(\mathcal{O})}(C_n)) = c_A(x)$.

We may even assume that M' has no access to x, i.e., $M'(c_{\mathrm{EC}(\mathcal{O})}(C_1), \dots, c_{\mathrm{EC}(\mathcal{O})}(C_n)) = c_A(x)$, since we can use the oracle answers $c_{\mathrm{EC}(\mathcal{O})}(1) = 0$ and $c_{\mathrm{EC}(\mathcal{O})}(\overline{\overline{1} + \overline{2}}) = 1$ to encode the single bits of x (e.g., a bit 0 is encoded by two answer bits 00, a bit 1 is encoded by two answer bits 11, and the end of x is marked by two answer bits 10). In particular, the set $B = \{z \mid M'(z) = 1\}$ belongs to P. By Lemma 45, there exists an $f \in \mathrm{FL}$ such that for all $\mathcal{O}$-circuits $C_1, \dots, C_n$ it holds that $(c_{\mathrm{EC}(\mathcal{O})}(C_1), \dots, c_{\mathrm{EC}(\mathcal{O})}(C_n)) \in B \Leftrightarrow f(C_1, \dots, C_n) \in \mathrm{EC}(\mathcal{O})$. Hence for all x, where $q(x) = (C_1, \dots, C_n)$, it holds that

$$\begin{aligned} x \in A \quad &\Leftrightarrow \quad (c_{\mathrm{EC}(\mathcal{O})}(C_1), \dots, c_{\mathrm{EC}(\mathcal{O})}(C_n)) \in B \\ &\Leftrightarrow \quad f(C_1, \dots, C_n) \in \mathrm{EC}(\mathcal{O}). \end{aligned}$$

So $A \leq_{\mathrm{m}}^{\log} \mathrm{EC}(\mathcal{O})$, which proves the first statement. The second one is shown analogously.

From $A \leq_{\mathrm{tt}} \mathrm{EC}(\mathcal{O})$ it follows that there exists a total, computable function that on input x returns a list of queries $C_1, \dots, C_n$ and a Boolean circuit C over $\{\vee, \neg\}$ with n inputs such that

$$x \in A \quad \Leftrightarrow \quad C(c_{\mathrm{EC}(\mathcal{O})}(C_1), \dots, c_{\mathrm{EC}(\mathcal{O})}(C_n)) = 1.$$

The construction in the proof of Lemma 45 shows that from C we can compute an $\mathcal{O}$-circuit C' such that

$$C(c_{\mathrm{EC}(\mathcal{O})}(C_1), \dots, c_{\mathrm{EC}(\mathcal{O})}(C_n)) = 1 \quad \Leftrightarrow \quad C' \in \mathrm{EC}(\mathcal{O}).$$

Therefore, $A \leq_{\mathrm{m}} \mathrm{EC}(\mathcal{O})$, which proves the third statement.

Statement 4 follows from statement 3. Statement 5 holds, since $\mathrm{EC}(\mathcal{O}) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{EC}(\mathcal{O})}$ by the first statement. □

As a corollary we obtain that $\mathrm{EC}(\cup, \cap, ^-, +, \times)$, $\mathrm{MC}(\cup, \cap, ^-, +, \times)$, and $\mathrm{EQ}(\cup, \cap, ^-, +, \times)$ are equivalent and $\leq_{\mathrm{m}}^{\log}$-hard for $\mathrm{L}^{\mathrm{NEXP}}$.

Corollary 47.

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* $\mathcal{R}_{\mathrm{tt}}(\Sigma_1)$.

Proof. By [GHR+10], $\mathrm{MC}(\cup, \cap, ^-, +, \times) \equiv_{\mathrm{m}}^{\log} \mathrm{EQ}(\cup, \cap, ^-, +, \times)$. By Lemma 2, it holds that $\mathrm{MC}(\cup, \cap, ^-, +, \times) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{EC}(\cup, \cap, ^-, +, \times)}$ and $\Sigma_1\text{-}\mathrm{MC}(\cup, \cap, ^-, +, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{NEC}(\cup, \cap, ^-, +, \times)$. The reduction $C \mapsto \overline{((C \times \{0\}) + \overline{\{1\}} + \overline{\{2\}})}$ shows $\overline{\mathrm{EC}(\cup, \cap, ^-, +, \times)} \equiv_{\mathrm{m}}^{\log} \mathrm{EC}(\cup, \cap, ^-, +, \times)$ and $\Sigma_1\text{-}\mathrm{NEC}(\cup, \cap, ^-, +, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cup, \cap, ^-, +, \times)$, which proves 1 and 2.

In statement 3, the membership in $\mathcal{R}_{\mathrm{tt}}(\Sigma_1)$ follows from the first statement and Theorem 44. McKenzie and Wagner [MW07] show that $\mathrm{MC}(\cup, \cap, ^-, +, \times)$ is $\leq_{\mathrm{m}}^{\log}$-hard for NEXP. By Proposition 46.1 in conjunction with the first statement, it is $\leq_{\mathrm{m}}^{\log}$-hard for $\mathcal{R}_{\mathrm{tt}}^{\log}(\mathrm{NEXP})$. Ladner and Lynch [LL76] show that $A \leq_{\mathrm{T}}^{\log} B$ if and only if $A \leq_{\mathrm{tt}}^{\log} B$. Hence $\mathrm{MC}(\cup, \cap, ^-, +, \times)$ is $\leq_{\mathrm{m}}^{\log}$-hard for $\mathcal{R}_{\mathrm{T}}^{\log}(\mathrm{NEXP})$. The same holds for $\mathrm{EC}(\cup, \cap, ^-, +, \times)$ and $\mathrm{EQ}(\cup, \cap, ^-, +, \times)$, because of the first statement.

Statements 4 and 5 follow from Proposition 46 and Theorem 44. □

We prove further equivalences between membership and emptiness problems, this time for $\{^-, +, \times\}$-circuits.

Proposition 48. 1. $\mathrm{MC}(^-, +, \times) \equiv_{\mathrm{m}}^{\log} \mathrm{EC}(^-, +, \times) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{EC}(^-, +, \times)}$.

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

Proof. The reduction $C \mapsto \overline{((C \times \{0\}) + \overline{\{1\}} + \overline{\{2\}})}$ shows $\mathrm{EC}(^-, +, \times) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{EC}(^-, +, \times)}$ and $\Sigma_1\text{-}\mathrm{EC}(^-, +, \times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{NEC}(^-, +, \times)$. By Lemma 2, it holds $\overline{\mathrm{EC}(^-, +, \times)} \leq_{\mathrm{m}}^{\log} \mathrm{MC}(^-, +, \times)$ and $\Sigma_1\text{-}\mathrm{NEC}(^-, +, \times) \leq_{\mathrm{m}}^{\log} \mathrm{MC}(^-, +, \times)$.

The reduction $\mathrm{MC}(^-,+,\times) \leq_{\mathrm{m}}^{\log} \mathrm{EC}(^-,+,\times)$ is as follows. On input (C,b) it computes the numbers $d = \min\{2^n \mid n \geq 1 \text{ and } b < 2^n\}$ and $e = 2d - b - 1$, and returns the circuit C_2, where

$$\begin{array}{rcl} C_1 & \overset{df}{=} & (((C + \{e\}) \times \{0,1\}) + \{1\}) \times \{0,1\} \text{ and} \\ C_2 & \overset{df}{=} & \overline{C_1 \times \overline{\{2d\}}}. \end{array}$$

Note that the set $\{0,1\}$ is generated by $\overline{\overline{\{0\}} + \{1\}}$. Moreover, the reduction is computable in logarithmic space.

It remains to show $b \in C$ if and only if $C_2 = \emptyset$. Note that $C_1 = (C + \{2d - b\}) \cup \{0,1\}$. From $d > b$ it follows that $2d - b \geq d + 1$ and hence $0, 1 \in C_1$ and $2, \ldots, d \notin C_1$. If $b \in C$, then $2d = b + (2d - b) \in C_1$ and hence $C_2 = \emptyset$, since $1 \in C_1$ and $1 \in \overline{\{2d\}}$. If $C_2 = \emptyset$, then $C_1 \times \overline{\{2d\}} = \mathbb{N} \ni 2d$ and hence $2d \in C_1$, since $2d$ is a power of two and no proper divisor of $2d$ belongs to C_1. Note that $2d \in C_1$ implies $b \in C$.

The same reduction shows Σ_1-$\mathrm{MC}(^-,+,\times) \leq_{\mathrm{m}}^{\log} \Sigma_1$-$\mathrm{EC}(^-,+,\times)$. □

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

In Theorem 42 and Corollary 47 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 44, 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 such decision algorithms.

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).

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

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 $\overline{\overline{0} + 1}$.

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

We show the following equivalences.

(i) GC_1 is true if any only if $C_1 \in \mathrm{EC}(^-,+,\times)$.

(ii) GC is true if and only if $C \in \mathrm{EC}(\cup,\cap,^-,+,\times,)$.

If GC_1 is true, then $(\mathbb{P}_1 + \mathbb{P}_1) \times \{0,1\} \supseteq 2\mathbb{N}$ and hence $I(C_1) = \emptyset$. Assume that GC_1 is false and let $n \geq 2$ such that $2n \notin \mathbb{P}_1 + \mathbb{P}_1$. This implies $2n - 1 \notin \mathbb{P}_1 + \mathbb{P}_1$, since otherwise $2n - 1 = 2 + p$ for some odd $p \in \mathbb{P}$ and hence $2n = 3 + p \in \mathbb{P}_1 + \mathbb{P}_1$, which is a contradiction. So $2n - 1, 2n \notin \mathbb{P}_1 + \mathbb{P}_1$, which implies $2n - 1, 2n \notin (\mathbb{P}_1 + \mathbb{P}_1) \times \{0,1\}$ and hence $2n \notin ((\mathbb{P}_1 + \mathbb{P}_1) \times \{0,1\}) + \{0,1\}$. Therefore, $C_1 \notin \mathrm{EC}(^-,+,\times)$. This proves (i) and a similar argument shows (ii).

The equivalences (i) and (ii) tell us the following: If one finds decision algorithms for $\mathrm{EC}(^-,+,\times)$ and $\mathrm{EC}(\cup,\cap,^-,+,\times)$ and proves them to be correct, then this solves Goldbach's conjectures, since the computation of the algorithm is a proof/refutation. Hence finding such decision algorithms and proving their correctness is at least as difficult as solving Goldbach's conjecture.

Even more confusing, it is possible that $\mathrm{EC}(^{-},+,\times)$ and $\mathrm{EC}(\cup,\cap,^{-},+,\times)$ are decidable, but one cannot find and prove decision algorithms: Let us assume for the moment that GC and GC_1 are independent of Zermelo–Fraenkel set theory (ZFC) with the usual definition of $\mathbb{N}$ within ZFC, which is considered to be plausible by some researchers [Knu02]. This assumption implies that GC and GC_1 hold in elementary arithmetic (otherwise there are simple counterexamples refuting the sentences [Aar03]), but we cannot prove them in ZFC. Moreover, the assumption implies that no sentence of the form "the algorithm $\mathcal{A}$ decides $\mathrm{EC}(\cup,\cap,^{-},+,\times)$ (resp., $\mathrm{EC}(^{-},+,\times)$)" can be proved in ZFC, since otherwise the computation of $\mathcal{A}$ on input C is a proof/refutation of GC (resp., GC_1). Still it is possible that sentences of the form "$\mathrm{EC}(\cup,\cap,^{-},+,\times)$ is decidable" are provable in ZFC. So in such a situation, there exist decision algorithms, but one cannot find them and prove them to be correct.

The relationship to Goldbach's conjecture suggests the difficulty of proving the decidability of $\mathrm{EC}(^{-},+,\times)$ and $\mathrm{EC}(\cup,\cap,^{-},+,\times)$. It raises our main open question: Are these problems decidable? By Proposition 48, the decidability of $\mathrm{EC}(^{-},+,\times)$ is equivalent to the decidability of $\mathrm{MC}(^{-},+,\times)$. By Corollary 47, the decidability of $\mathrm{EC}(\cup,\cap,^{-},+,\times)$ is equivalent to the decidability of $\mathrm{MC}(\cup,\cap,^{-},+,\times)$ and $\mathrm{EQ}(\cup,\cap,^{-},+,\times)$.

6.4 Connection between Emptiness and Σ_1-Emptiness

We show that the emptiness and the Σ_1-emptiness problem are equivalent for the circuits over $\{\cap,+,\times\}$, $\{\cup,\cap,+,\times\}$, $\{\cap,\times\}$, and $\{\cup,\cap,\times\}$, respectively. 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 large argument only dependent on K and the total degree of the polynomial. To obtain the assertion for $\{\cup,\cap,+,\times\}$ and $\{\cup,\cap,\times\}$, one additionally has to observe that this argument depends only on the polynomial's degree, but not on the number of its monomials.

As a corollary we obtain the equivalence of the emptiness, the Σ_1-emptiness, and the nonmembership problem for $\{\cap,+,\times\}$-circuits. Moreover, we show $\Sigma_1\text{-}\mathrm{EC}(\cap,+,\times)\in\mathrm{RP}$ and the coNEXP-completeness of $\Sigma_1\text{-}\mathrm{EC}(\cup,\cap,+,\times)$.

Along the way we also prove the equivalence of emptiness and Σ_1-emptiness for circuits over $\mathbb{Z}$, which is important for the proof of Theorem 58 in Subsection 6.5. For this we define the integer variants of $\mathrm{MC}(+,\times)$, $\mathrm{MC}(\cap,+,\times)$, $\mathrm{EC}(\cap,+,\times)$, and $\Sigma_1\text{-}\mathrm{EC}(\cap,+,\times)$. Given $\mathcal{O}\subseteq\{\cap,\cup,^{-},+,\times\}$, let

$$\begin{aligned}
\mathrm{MC}_{\mathbb{Z}}(\mathcal{O}) &\overset{df}{=} \{(C,b)\mid C \text{ is a completely assigned } \mathcal{O}\text{-circuit such that the assigned inputs have labels from } \mathbb{Z} \text{ and } b\in I(C)\ \}\\
\mathrm{EC}_{\mathbb{Z}}(\mathcal{O}) &\overset{df}{=} \{C\mid C \text{ is a completely assigned } \mathcal{O}\text{-circuit such that the assigned inputs have labels from } \mathbb{Z} \text{ and } I(C)=\emptyset\ \}\\
\Sigma_1\text{-}\mathrm{EC}_{\mathbb{Z}}(\mathcal{O}) &\overset{df}{=} \{C\mid C \text{ is a partially assigned } \mathcal{O}\text{-circuit with unassigned inputs } u_1<\cdots<u_n \text{ such that the assigned inputs have labels from } \mathbb{Z} \text{ and there exist } x_1,\dots,x_n\in\mathbb{Z} \text{ such that } I(C(x_1,\dots,x_n))=\emptyset\ \}.
\end{aligned}$$

A systematic study of the membership problems $\mathrm{MC}_{\mathbb{Z}}(\mathcal{O})$ was done by Travers [Tra06].

Lemma 49 ([LV03]). *Given a polynomial $f(x_1,\dots,x_n)$ 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 $\mathbb{R}$ if and only if the new univariate polynomial is identically zero on $\mathbb{R}$.*

Theorem 50. *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. $\mathrm{EC}(\cup,\cap,+,\times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cup,\cap,+,\times)$.

4. $\mathrm{EC}(\cap,\times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cap,\times)$.

5. $\mathrm{EC}(\cup,\cap,\times) \equiv_{\mathrm{m}}^{\log} \Sigma_1\text{-}\mathrm{EC}(\cup,\cap,\times)$.

Proof. It suffices to show the reductions from the right-hand to the left-hand sides. We argue that these reductions are achieved by the same mapping described below.

Let C be a $\{\cup,\cap,+,\times\}$-circuit with unassigned input gates $g_1,\ldots,g_k$ and assigned input gates $g'_1,\ldots,g'_{k'}$. Let $n-1$ denote the depth of C, i.e., the maximum number of nodes on a path from an input node to the output node, which can be determined in logarithmic space by a depth first search. Let $\omega = \max(\{\mathrm{abs}(\alpha(g'_i))+2 \mid i=1,\ldots,k'\})$. The reduction is given by $C \mapsto C_{n,\omega}$, where $C_{n,\omega}$ is defined as follows: Let $v=(v_1,\ldots,v_k)$ where $v_i=\omega^{2^{ni}}$. Define $C_{n,\omega}$ as the circuit obtained from C by assigning $(v_1,\ldots,v_k)$ to $(g_1,\ldots,g_k)$ in such a way that the large number v_i is generated by the $\{\times\}$-circuit which squares the number ω precisely ni times. Observe that the mapping $C \mapsto C_{n,\omega}$ is computable in logarithmic space.

Claim 51. *1.* $C \in \Sigma_1\text{-}\mathrm{EC}(\cap,+,\times)$ *if and only if* $C_{n,\omega} \in \mathrm{EC}(\cap,+,\times)$.

2. $C \in \Sigma_1\text{-}\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)$ *if and only if* $C_{n,\omega} \in \mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)$.

Proof of Claim 51. We only show the second statement, as the first one can be deduced similarly. If $C_{n,\omega} \in \mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)$, then $C \in \Sigma_1\text{-}\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)$, as is witnessed by v. It remains to show the converse implication. So, suppose for the sake of contradiction that there is some $C \in \Sigma_1\text{-}\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)$ such that $I(C_{n,\omega}) \neq \emptyset$. By assumption, there exists $w=(w_1,\ldots,w_k)\in\mathbb{Z}^k$ such that $I(C(w))=\emptyset$. Let g be the first $\cap$-gate connected to the output gate that computes the empty set in $C(w)$, and let g_l (resp., g_r) be the left (resp., right) predecessor of g. Hence g_l and g_r compute singletons $\{a_l\}$ and $\{a_r\}$ in $C(w)$ such that $a_l \neq a_r$.

The number generated in g_l (resp., g_r) can be written as a multivariate polynomial p_l (resp., p_r) in $g_1,\ldots,g_k$. These polynomials are obtained inductively by assigning one polynomial to each gate: the univariate polynomial g_i to the unassigned input gate g_i, the constant polynomial c to assigned input gates with label $c\in\mathbb{Z}$, and the polynomial q_l+q_r (resp., $q_l\cdot q_r$, q_l) to a $+$-gate (resp., $\times$-gate, $\cap$-gate), where q_l (resp., q_r) is the polynomial of the left (resp., right) predecessor. Note that all gates above g compute non-empty sets. Hence the left and right predecessors of each $\cap$-gate above g compute the same number, which shows that it does not matter whether one chooses the polynomial of the left or right predecessor.

An induction shows that $p_l(w)=a_l$ and $p_r(w)=a_r$. Hence $p_l(w)\neq p_r(w)$. Another induction shows that p_l and p_r are of degree at most $d=2^n-1$. Let p'_l and p'_r be the polynomials obtained from p_l and p_r after the substitution $g_i \to x^{(d+1)^{i-1}}$. The application of Lemma 49 to the polynomial $p=p_l-p_r$ shows that p is identically zero on $\mathbb{R}$ if and only if $p' \overset{\mathrm{df}}{=} p'_l - p'_r$ is identically zero on $\mathbb{R}$. So by $p_l(w)\neq p_r(w)$, p' is not identically zero on $\mathbb{R}$.

In the expanded form of p_l and p_r, the absolute values of the coefficients of the monomials are less than $\omega^{2^{n-1}}$, which is shown by induction. Hence also the absolute values of the coefficients of the expanded forms of p'_l and p'_r are less than $\omega^{2^{n-1}}$, because different monomials $g_1^{e_1}\cdots g_k^{e_k}$ and $g_1^{e'_1}\cdots g_k^{e'_k}$ remain different after the substitution $g_i \to x^{(d+1)^{i-1}}$. So the absolute values of the coefficients of p' are less than $2\cdot\omega^{2^{n-1}} \leq \omega^{2^n}$. Observe that $p_l(v)=p'_l(\omega^{2^n})$ and $p_r(v)=p'_r(\omega^{2^n})$. Thus $p'(\omega^{2^n})=p_l(v)-p_r(v)=0$, since by assumption $I(C_{n,\omega})\neq\emptyset$ and hence $p_l(v)=p_r(v)$. Since p' is not identically zero on $\mathbb{R}$, it can be written as $p'=x^j\cdot\sum_{i=0}^r a_i x^i$ for suitable $j,r\in\mathbb{N}$ and $a_i\in\mathbb{Z}$ such that $-\omega^{2^n}<a_i<\omega^{2^n}$ and $a_0\neq 0$. From $p'(\omega^{2^n})=0$ we obtain $\sum_{i=0}^r a_i\omega^{i2^n}=0$. Hence $\omega^{2^n}\cdot\sum_{i=1}^r a_i\omega^{(i-1)2^n}=-a_0$, which implies that the absolute value of a_0 is $\geq \omega^{2^n}$. This contradicts the above observation on the coefficients of p'. □

The claim proves the statements 1 and 2 of the theorem. It basically remains to argue that the reduction Σ_1- $\mathrm{EC}(\cup,\cap,+,\times) \leq_{\mathrm{m}}^{\log} \mathrm{EC}(\cup,\cap,+,\times)$ is achieved by the same function.

Consider an arbitrary $\{\cup,\cap,+,\times\}$-circuit $C = (V, E, g_C, \alpha)$ with unassigned input gates $g_1, \dots, g_k$. We assume without loss of generality that the output gate of C is no $\cup$-gate (otherwise add a new output gate which multiplies the former output gate with 1). Let D be the circuit defined as follows: Fix $t = |V|$ and let $(h_1, \dots, h_t)$ be the elements of V such that for $i < j$ there is no edge from h_i to h_j. For $i = 1, \dots, t$ do the following: If h_i has outdegree ≥ 2, then determine the outdegree s of h_i and its successors $u_1, \dots, u_s$. Then, for $j = 2, \dots, s$, delete the edge from h_i to u_j, add a new node h with $\alpha(h) = \alpha(h_i)$ such that h has the same predecessors as h_i and there is an edge from h to u_k.

Thus it holds by construction:

Claim 52. *All nodes in D have outdegree 1, the depth of D is the same as the depth of C, and for all $x_1, \dots, x_k \in \mathbb{N}$ one has $I(C(x_1, \dots, x_k)) = I(D(x_1, \dots, x_k))$.*

Let $w_1, \dots, w_m$ be the $\cup$-gates of D such that for $i < j$ there is no edge from w_i to w_j. We fix this ordering of the $\cup$-gates. Let $\pi : \{1, \dots, m\} \to \{l, r\}$ be total and for any gate g in D, let the left (resp., right) predecessor of g be denoted by g_l (resp., g_r). By successively modifying D we define an $\{\cap,+,\times\}$-circuit D^π: for $i = 1, \dots, m$ add an edge from $(w_i)_{\pi(i)}$ to the unique successor of w_i and afterwards, delete w_i and all edges it is incident with. Thus, we obtain an $\{\cap,+,\times\}$-circuit D^π whose depth is not greater than the depth of D.

Claim 53. *Let $x_1, \dots, x_k \in \mathbb{N}$. Then $I(D(x_1, \dots, x_k)) = \emptyset$ if and only if for every total $\pi : \{1, \dots, m\} \to \{l, r\}$ it holds $I(D^\pi(x_1, \dots, x_k)) = \emptyset$.*

Proof of Claim 53. "⇒": Let $\pi : \{1, \dots, m\} \to \{l, r\}$. Note that D^π contains all the gates of D except for the $\cup$-gates. It can be shown inductively that for any gate g of D^π it holds $I(g; D^\pi(x_1, \dots, x_k)) \subseteq I(g; D(x_1, \dots, x_k))$. Since both circuits have the same output gate the proof of this direction is complete.

"⇐": We show the contraposition. Hence assume $I(D(x_1, \dots, x_k)) \neq \emptyset$. Choose some $x \in I(D(x_1, \dots, x_k))$. In the following we construct a map $\pi : \{1, \dots, m\} \to \{l, r\}$ such that $x \in I(D^\pi(x_1, \dots, x_k))$:

1. Let $U = \{g_D\}$ where g_D is D's output node. For every gate g we establish an initially undefined attribute $g.no$. Let $g_D.no = x$.

2. While U is not empty:

   (a) Extract a gate g from U and let $y = g.no$.

   (b) Let g_l (resp., g_r) be the left (resp., right) predecessor of g. If g has no predecessor, proceed with the next iteration of the loop.

   (c) If g is a $+$-gate (resp., $\times$-gate):

   - Choose $y_1 \in I(g_1; D(x_1, \dots, x_k))$ and $y_2 \in I(g_2; D(x_1, \dots, x_k))$ such that $y_1 + y_2 = y$ (resp., $y_1 \cdot y_2 = y$).
   - Let $g_l.no = y_1$ and $g_r.no = y_2$.
   - Add g_l and g_r to U.

   (d) If g is an $\cap$-gate:

   - Let $g_l.no = y$ and $g_r.no = y$.
   - Add g_l and g_r to U.

   (e) If g is a $\cup$-gate:

- $g = w_j$ for some $1 \leq j \leq m$.
- If $y \in I(g_l; I(D(x_1, \ldots, x_k))$, let $\pi(j) = l$, $g_l.no = y$, and add g_l to U. Otherwise let $\pi(j) = r$, $g_r.no = y$ and add g_r to U.

3. For all j for which $\pi(j)$ has not been defined yet let $\pi(j) = l$.

4. Return π.

As all gates have outdegree at most 1, each gate is considered at most once. The attribute $g.no$ is defined for g if and only if g and D^π's output gate are connected in D^π. Let g be such a gate. Then it can be seen inductively that $I(g; D^\pi(x_1, \ldots, x_k)) = \{g.no\}$ and hence $I(D^\pi(x_1, \ldots, x_k)) = \{x\}$. □

In the following we assume without loss of generality that the depths of all D^π and D are equal (otherwise multiply 1 to the output gate of D^π for correspondingly many times). Furthermore, for all circuits C, D, and D^π, the assigned input gates are mapped onto the same numbers respectively. Note that Claim 51 does not only hold for C but also for every $\{\cap, +, \times\}$-circuit with the same depth and the same assigned inputs, i.e., in particular it holds for all D^π. Hence it holds

$$\begin{aligned}
& C \in \Sigma_1\text{- EC}(\cup, \cap, +, \times) \\
\overset{\text{Claim 52}}{\Leftrightarrow}\ & D \in \Sigma_1\text{- EC}(\cup, \cap, +, \times) \\
\overset{\text{Claim 53}}{\Leftrightarrow}\ & \text{there are } x_1, \ldots, x_k \text{ such that for all } \pi : \{1, \ldots, m\} \to \{0, 1\}\text{: } D^\pi(x_1, \ldots, x_k) = \emptyset \\
\overset{\text{Claim 51}}{\Leftrightarrow}\ & \text{for all } \pi : \{1, \ldots, m\} \to \{0, 1\}\text{: } D^\pi_{n,\omega} \in \text{EC}(\cap, +, \times) \\
\Leftrightarrow\ & \text{for all } \pi : \{1, \ldots, m\} \to \{0, 1\}\text{: } D^\pi(\omega^{2^n}, \ldots, \omega^{2^{kn}}) \in \text{EC}(\cap, +, \times) \\
\overset{\text{Claim 53}}{\Leftrightarrow}\ & D(\omega^{2^n}, \ldots, \omega^{2^{kn}}) \in \text{EC}(\cup, \cap, +, \times) \\
\overset{\text{Claim 52}}{\Leftrightarrow}\ & C(\omega^{2^n}, \ldots, \omega^{2^{kn}}) \in \text{EC}(\cup, \cap, +, \times) \\
\Leftrightarrow\ & C_{n,\omega} \in \text{EC}(\cup, \cap, +, \times),
\end{aligned}$$

which proves the third statement.

We recall that the reduction presented at the beginning of the proof modifies an input circuit without adding gates of the type $\cup$ or $+$. Hence as $\{\cap, \times\}$- and $\{\cup, \cap, \times\}$-circuits are specific $\{\cup, \cap, +, \times\}$-circuits, the same reduction shows that the fourth and fifth statement hold as well. □

Corollary 54. $\text{EC}(\cap, +, \times) \equiv_{\text{m}}^{\log} \Sigma_1\text{- EC}(\cap, +, \times) \equiv_{\text{m}}^{\log} \overline{\text{MC}(\cap, +, \times)} \equiv_{\text{m}}^{\log} \overline{\text{EQ}(+, \times)}$.

Proof. $\text{MC}(\cap, +, \times) \equiv_{\text{m}}^{\log} \text{EQ}(+, \times)$ was shown by McKenzie and Wagner [MW07]. The remaining equivalences follow from Lemma 2 and Theorem 50. □

Corollary 55. *1.* $\Sigma_1\text{-EC}(\cap, +, \times) \in \text{RP}$.

2. $\Sigma_1\text{-EC}(\cup, \cap, +, \times)$ *is* $\leq_{\text{m}}^{\log}$*-complete for* coNEXP.

Proof. The first statement follows from Corollary 54 and $\text{MC}(\cap, +, \times) \in \text{coRP}$ [MW07]. The second one follows from Theorem 50 and Corollary 3. □

Theorem 50 directly implies some results which actually belong to Section 5.

Corollary 56. *1.* Σ_1-$\mathrm{EC}(\cap, \times) \in \mathrm{P}$.

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

Proof. Follows from Lemma 2 and $\mathrm{MC}(\cap, \times) \in \mathrm{P}$ [MW07]. □

Corollary 56 shows the equivalence of $\mathrm{EC}(\cap, \times)$, Σ_1- $\mathrm{EC}(\cap, \times)$, and $\overline{\mathrm{MC}(\cap, \times)}$. Therefore, 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 [MW07].

Corollary 57. Σ_1-$\mathrm{EC}(\cup, \cap, \times)$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* PSPACE*.*

Proof. Follows from Theorem 21 and Theorem 50. □

6.5 Connection to Polynomial Identity Testing

According to the previous section, the problems $\mathrm{EC}(\cap, +, \times)$, Σ_1- $\mathrm{EC}(\cap, +, \times)$, $\overline{\mathrm{EQ}(+, \times)}$, and $\overline{\mathrm{MC}(\cap, +, \times)}$ are equivalent. We extend this list by adding $\mathrm{EC}_{\mathbb{Z}}(\cap, +, \times)$, Σ_1- $\mathrm{EC}_{\mathbb{Z}}(\cap, +, \times)$, $\overline{\mathrm{MC}_{\mathbb{Z}}(\cap, +, \times)}$, $\overline{\mathrm{MC}_{\mathbb{Z}}(+, \times)}$, and $\overline{\mathrm{PIT}}$. This connection to PIT is especially interesting as it explains the difficulty of several open questions, namely the non-matching lower and upper bounds of $\mathrm{MC}(\cap, +, \times)$ in [MW07], $\mathrm{MC}_{\mathbb{Z}}(\cap, +, \times)$ and $\mathrm{MC}_{\mathbb{Z}}(+, \times)$ in [Tra06], and $\mathrm{EQ}(+, \times)$ in [GHR$^+$10]. In addition, this connection settles the question for the complexity of $\mathrm{EC}(\cap, +, \times)$ and Σ_1- $\mathrm{EC}(\cap, +, \times)$.

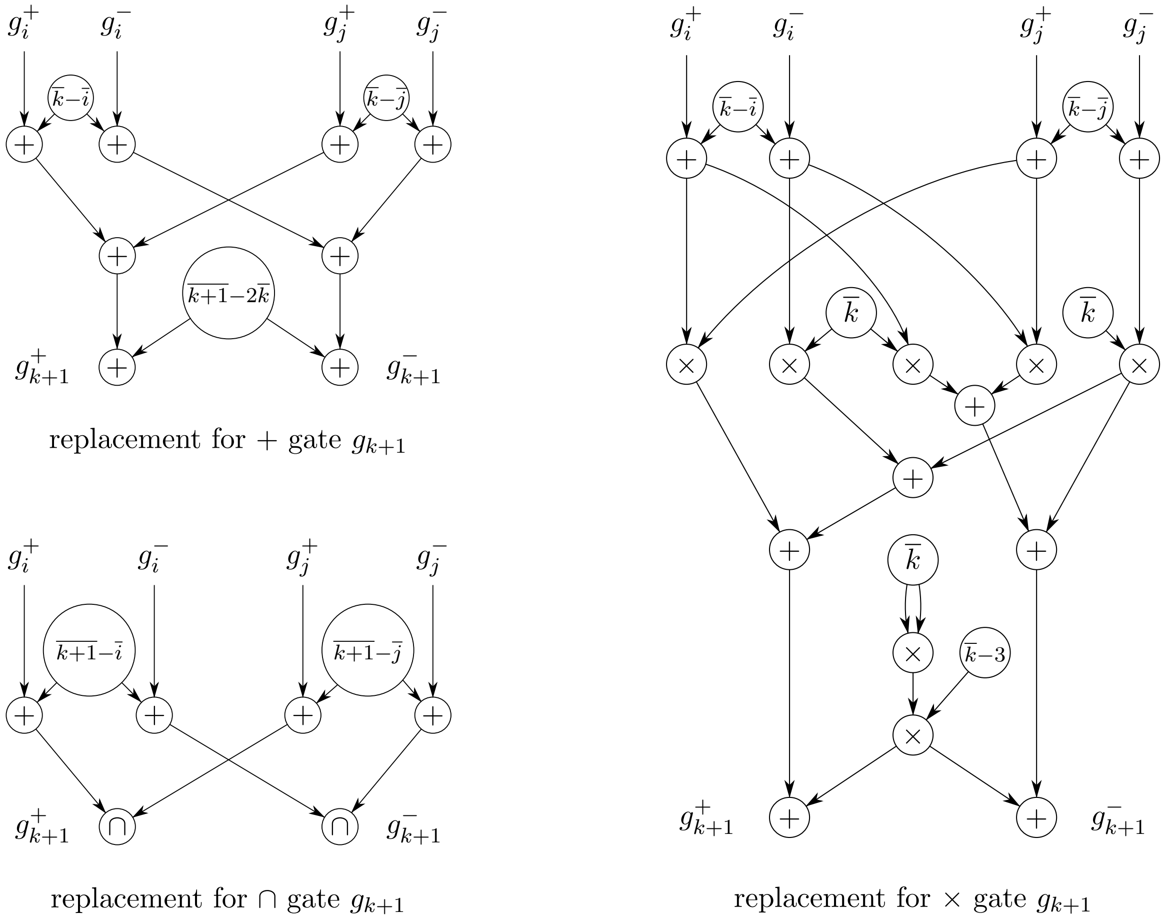
PIT (polynomial identity testing) is the following problem: For a given integer circuit consisting of input gates associated with variables/constants from $\mathbb{Z}$ and internal gates for addition/multiplication over $\mathbb{Z}$, one has to decide whether the polynomial described by the circuit is 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 $\mathbb{Z}$. (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 $\mathbb{Z}$.

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

It is known that $\mathrm{PIT} \in \mathrm{coRP}$ [IM83], but proving the exact complexity of PIT is considered as one of the greatest challenges in algebraic computing complexity [Sax09] and theoretical computer science in general [SY10]. This fundamental problem has many applications, e.g., a deterministic primality test [AKS04]. For further background on PIT we refer to the articles [Sax09, SY10, Sax13, KL15].

The equivalence to $\overline{\mathrm{PIT}}$ shows that $\mathrm{EC}(\cap, +, \times)$, Σ_1- $\mathrm{EC}(\cap, +, \times)$, and each of the open questions from [MW07, Tra06, GHR$^+$10] that were mentioned above is just a reformulation of a well-studied, major open question in algebraic computing complexity. Moreover, Kabanets and Impagliazzo [KI04] substantiate the hardness of obtaining subexponential or even polynomial-time algorithms for PIT by showing that it implies that $\mathrm{NEXP} \not\subset \mathrm{P/poly}$ 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.

Theorem 58. $\mathrm{EC}(\cap, +, \times) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{MC}(\cap, +, \times)} \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{EQ}(+, \times)} \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{PIT}} \equiv_{\mathrm{m}}^{\log} \mathrm{EC}_{\mathbb{Z}}(\cap, +, \times)$.


g_i^+
g_i^-
g_j^+
g_j^-
$\overline{k}-\overline{i}$
$\overline{k}-\overline{j}$
$\overline{k+1}-2\overline{k}$
$\overline{k+1}-\overline{i}$
$\overline{k+1}-\overline{j}$
$\overline{k}$
$\overline{k}-3$
$+$
$\times$
$\cap$
g_{k+1}^+
g_{k+1}^-

replacement for + gate g_{k+1}

replacement for $\cap$ gate g_{k+1}

replacement for $\times$ gate g_{k+1}

Figure 1: Subcircuits C_{k+1} that replace gates of the type $+$, $\cap$, or $\times$ in the proof of Theorem 58, where the direction of the edges is top-down. By Claim 59, the numbers $\overline{k}-3$, $\overline{k}$, $\overline{k}-\overline{i}$, $\overline{k}-\overline{j}$, $\overline{k+1}-\overline{i}$, and $\overline{k+1}-2\overline{k}$ are generated by subcircuits that can be constructed in logarithmic space.

Proof. By Corollary 54 it holds $\mathrm{EC}(\cap,+,\times) \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{MC}(\cap,+,\times)} \equiv_{\mathrm{m}}^{\log} \overline{\mathrm{EQ}(+,\times)}$. Moreover, $\mathrm{EQ}(+,\times) \leq_{\mathrm{m}}^{\log} \mathrm{PIT}$ via $(C_1,C_2) \mapsto (C_1+(C_2\times\{-1\}))$, since for $\{+,\times\}$-circuits C_1 and C_2 it holds $I(C_1)=I(C_2)$ if and only if $I((C_1+(C_2\times\{-1\}))) = \{0\}$. This shows $\overline{\mathrm{EQ}(+,\times)} \leq_{\mathrm{m}}^{\log} \overline{\mathrm{PIT}}$.

Note that $\overline{\mathrm{PIT}} \leq_{\mathrm{m}}^{\log} \Sigma_1\text{-}\,\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)$ via the reduction $C \mapsto C \cap \{0\}$. By Theorem 50, this implies $\overline{\mathrm{PIT}} \leq_{\mathrm{m}}^{\log} \mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)$.

It remains to show $\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times) \leq_{\mathrm{m}}^{\log} \mathrm{EC}(\cap,+,\times)$. Let C be an $\{\cap,+,\times\}$-circuit without unassigned inputs and with assigned inputs having labels from $\mathbb{Z}$. Without loss of generality, we may assume that there is exactly one input gate g_1 and that this gate has the label -1 (if not, we can construct an equivalent circuit with this property in logarithmic space). Moreover, for $i \in \mathbb{N}$ let $\overline{i} = 2^{3^i}$.

We convert C into a circuit C' over $\mathbb{N}$, which simulates the computation of C such that each value computed in C is represented by two positive numbers. More precisely, each gate g_i in C is simulated by a subcircuit C_i, which has two output gates g_i^+ and g_i^-. A value $v \in \mathbb{Z}$ computed in g_i is represented by the numbers $\overline{i}+v$ and $\overline{i}-v$ computed in g_i^+ and g_i^-. We will argue that both numbers are positive.

We will use the following claim to construct in logspace in the size of C certain terms involving $\overline{i}$.

Claim 59. *There exists a logspace machine that on input 2^i and 2^j, where $1 \leq i \leq j$, constructs $\{+,\times\}$-circuits over $\mathbb{N}$ that compute the numbers $\overline{i}-3$, $\overline{i}-1$, $\overline{i}$, $\overline{j}-\overline{i}$, and $\overline{i+1}-2\overline{i}$.*

Proof of Claim 59. Consider a $\{+,\times\}$-circuit computing the polynomial $p(x) = (x+3)^2(x+2)+(x+5)(x+1)+1$ and observe that $p(\overline{y}-3) = \overline{y+1}-3$ for all $y \in \mathbb{N}$. The repeated application of this circuit yields one for $\overline{i}-3$. By adding 2 and 3 we obtain circuits for $\overline{i}-1$ and $\overline{i}$ respectively.

Now consider a $\{+,\times\}$-circuit computing the polynomial $q(x) = (x+1)(x+2)x$ and observe that $q(\overline{y}-1) = \overline{y+1}-\overline{y}$ for all $y \in \mathbb{N}$. With this circuit we can build another one that first computes $\overline{i}-1, \overline{i+1}-1, \dots, \overline{j-1}-1$ as above, then $\overline{i+1}-\overline{i}, \overline{i+2}-\overline{i+1}, \dots, \overline{j}-\overline{j-1}$ by applying q, and finally $\sum_{k=i}^{j-1} \overline{k+1}-\overline{k} = \overline{j}-\overline{i}$.

Let $r(x) = (x+3)(x+5)(x+1)+2(x+3)$ and observe that $r(\overline{i}-3) = \overline{i+1}-2\overline{i}$. This yields a $\{+,\times\}$-circuit for $\overline{i+1}-2\overline{i}$ by first computing $\overline{i}-3$ as above and then applying r. □

We inductively convert C into C': The assigned input gate g_1 with label -1 is replaced by a subcircuit C_1 that consists of the gates g_1^+ and g_1^- with labels $\overline{1}+(-1)=7$ and $\overline{1}-(-1)=9$. Every $+$-gate, $\times$-gate, or $\cap$-gate g_{k+1} ($k \geq 1$) with predecessors g_i and g_j is replaced by the corresponding subcircuit C_{k+1} shown in Figure 1. Finally, if g_s is the output gate of C, then g_s^+ is the output gate of C'.

The construction of C' is possible in logarithmic space, since by Claim 59, the subcircuits C_k can be constructed in logarithmic space. Moreover, all numbers computed in C' are positive, since the two input gates have positive labels and we use only gates of the type $\cap$, $+$, or $\times$.

Claim 60. *For every gate g_k in C it holds that $I(g_k^+) = \overline{k}+I(g_k)$ and $I(g_k^-) = \overline{k}-I(g_k)$.*

Proof of Claim 60. The claim is proved by induction on the structure of the circuit. For the assigned input gate g_1 the claim holds by the definition of g_1^+ and g_1^-, which yields the induction base.

For a $+$-gate g_{k+1} with predecessors g_i and g_j we obtain

$$\begin{aligned} I(g_{k+1}^+) &= I(g_i^+)+I(g_j^+)+(\overline{k}-\overline{i})+(\overline{k}-\overline{j})+(\overline{k+1}-2\overline{k}) \\ &= I(g_i)+I(g_j)+\overline{i}+\overline{j}+\overline{k}-\overline{i}+\overline{k}-\overline{j}+\overline{k+1}-2\overline{k} \quad = \quad \overline{k+1}+I(g_{k+1}) \end{aligned}$$

and analogously $I(g_{k+1}^-) = \overline{k+1}-I(g_{k+1})$.

For a $\times$-gate g_{k+1} with predecessors g_i and g_j we obtain

$$\begin{aligned} I(g_{k+1}^+) &= (I(g_i^+)+\overline{k}-\overline{i})(I(g_j^+)+\overline{k}-\overline{j})+\overline{k}(I(g_i^-)+\overline{k}-\overline{i})+\overline{k}(I(g_j^-)+\overline{k}-\overline{j})+\overline{k}^2(\overline{k}-3) \\ &= (I(g_i)+\overline{k})(I(g_j)+\overline{k})+\overline{k}(2\overline{k}-I(g_i)-I(g_j))+\overline{k}^2(\overline{k}-3) \\ &= I(g_i)I(g_j)+\overline{k}(I(g_i)+I(g_j))+\overline{k}^2+2\overline{k}^2-\overline{k}(I(g_i)+I(g_j))+\overline{k}^3-3\overline{k}^2 \\ &= \overline{k}^3+I(g_i)I(g_j) \quad = \quad \overline{k+1}+I(g_{k+1}) \end{aligned}$$

and

$$\begin{aligned} I(g_{k+1}^-) &= (I(g_i^-)+\overline{k}-\overline{i})(I(g_j^+)+\overline{k}-\overline{j})+\overline{k}(I(g_i^+)+\overline{k}-\overline{i})+\overline{k}(I(g_j^-)+\overline{k}-\overline{j})+\overline{k}^2(\overline{k}-3) \\ &= (\overline{k}-I(g_i))(\overline{k}+I(g_j))+\overline{k}(2\overline{k}+I(g_i)-I(g_j))+\overline{k}^2(\overline{k}-3) \\ &= \overline{k}^2+\overline{k}(I(g_j)-I(g_i))-I(g_i)I(g_j)+2\overline{k}^2-\overline{k}(I(g_j)-I(g_i))+\overline{k}^3-3\overline{k}^2 \\ &= \overline{k}^3-I(g_i)I(g_j) \quad = \quad \overline{k+1}-I(g_{k+1}). \end{aligned}$$

For an $\cap$-gate g_{k+1} with predecessors g_i and g_j we obtain

$$\begin{aligned} I(g^+_{k+1}) &= (I(g^+_i) + (\overline{k+1-\bar{\imath}})) \cap (I(g^+_j) + (\overline{k+1-\bar{\jmath}})) \\ &= (I(g_i) + \overline{k+1}) \cap (I(g_j) + \overline{k+1}) \\ &= \overline{k+1} + (I(g_i) \cap I(g_j)) \quad = \quad \overline{k+1} + I(g_{k+1}) \end{aligned}$$

and analogously $I(g^-_{k+1}) = \overline{k+1} - I(g_{k+1})$. □

The claim implies $\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times) \leq^{\log}_{\mathrm{m}} \mathrm{EC}(\cap,+,\times)$ via $C \mapsto C'$. □

Corollary 61. $\mathrm{MC}_{\mathbb{Z}}(\cap,+,\times) \equiv^{\log}_{\mathrm{m}} \mathrm{MC}_{\mathbb{Z}}(+,\times) \equiv^{\log}_{\mathrm{m}} \mathrm{PIT}$.

Proof. We have $\mathrm{MC}_{\mathbb{Z}}(\cap,+,\times) \leq^{\log}_{\mathrm{m}} \overline{\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)}$ via $(C,b) \mapsto C \cap \{b\}$. By Theorem 58, $\overline{\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)} \leq^{\log}_{\mathrm{m}} \mathrm{EQ}(+,\times)$. Note that $\mathrm{EQ}(+,\times) \leq^{\log}_{\mathrm{m}} \mathrm{MC}_{\mathbb{Z}}(+,\times)$ via $(C_1,C_2) \mapsto (C_1 + (\{-1\} \times C_2), 0)$.

Hence $\mathrm{MC}_{\mathbb{Z}}(\cap,+,\times) \equiv^{\log}_{\mathrm{m}} \mathrm{MC}_{\mathbb{Z}}(+,\times) \equiv^{\log}_{\mathrm{m}} \overline{\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)}$. By Theorem 58, $\overline{\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times)} \equiv^{\log}_{\mathrm{m}}$ PIT. □

Corollary 62. $\mathrm{EC}(\cap,+,\times) \equiv^{\log}_{\mathrm{m}} \Sigma_1\text{-}\mathrm{EC}(\cap,+,\times) \equiv^{\log}_{\mathrm{m}} \mathrm{EC}_{\mathbb{Z}}(\cap,+,\times) \equiv^{\log}_{\mathrm{m}} \Sigma_1\text{-}\mathrm{EC}_{\mathbb{Z}}(\cap,+,\times) \equiv^{\log}_{\mathrm{m}} \overline{\mathrm{PIT}}$.

Proof. Follows from the Theorems 50 and 58. □

6.6 EQ$(\cap,+,\times)$ versus PIT

When looking at Theorem 58 one must ask the question of whether $\mathrm{EQ}(\cap,+,\times)$ can be added, i.e., whether $\mathrm{EQ}(\cap,+,\times)$ is equivalent to PIT. We show that this is unlikely. More precisely, we prove that $\mathrm{EQ}(\cap,+,\times)$ is $\leq^{\log}_{\mathrm{m}}$-complete for $\mathcal{PIT} \vee \mathrm{co}\mathcal{PIT}$, which is the complement of the second level of the difference hierarchy [KSW87] over $\mathcal{PIT}$. We already know that $\mathrm{EQ}(+,\times)$ is $\leq^{\log}_{\mathrm{m}}$-complete for $\mathcal{PIT}$. Therefore, if $\mathrm{EQ}(\cap,+,\times) \equiv^{\log}_{\mathrm{m}}$ PIT, then $\mathcal{PIT} = \mathcal{PIT} \vee \mathrm{co}\mathcal{PIT}$ and hence $\mathrm{PIT} \equiv^{\log}_{\mathrm{m}} \overline{\mathrm{PIT}} \in \mathrm{RP} \subseteq \mathrm{NP}$. Kabanets and Impagliazzo [KI04] show that PIT $\in$ NP is unlikely, since it implies NEXP $\cap$ coNEXP $\not\subset$ 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 [GHR+10] to coRP or even P (since this implies $\overline{\mathrm{PIT}} \leq^{\log}_{\mathrm{m}} \mathrm{EQ}(\cap,+,\times) \in \mathrm{coRP}$).

Definition 63. $\mathcal{PIT} \overset{df}{=} \mathcal{R}^{\log}_{\mathrm{m}}(\mathrm{PIT})$.

Lemma 64. *1. $\mathcal{PIT} \vee \mathcal{PIT} = \mathcal{PIT}$.*

2. $\mathrm{co}\mathcal{PIT} \wedge \mathrm{co}\mathcal{PIT} = \mathrm{co}\mathcal{PIT}$.

Proof. Note that in both cases $\supseteq$ holds by definition.

1. Let $A, B \in \mathcal{PIT}$. Thus there are $f, g \in$ FL such that $A \leq^{\log}_{\mathrm{m}}$ PIT via f and $B \leq^{\log}_{\mathrm{m}}$ PIT via g. Consider the FL-function $x \mapsto f(x) \cdot g(x)$. As $\mathbb{Z}[x_1, \ldots, x_n]$ for any n does not contain any zero divisors it holds that $f(x) \cdot g(x)$ computes the polynomial identically zero if and only if one of the polynomials computed by $f(x)$ and $g(x)$ is identically zero.

Thus $A \cup B \leq^{\log}_{\mathrm{m}} \mathrm{PIT} \in \mathcal{PIT}$.

2. Let $A, B \in \mathrm{co}\mathcal{PIT}$. Then $\overline{A}, \overline{B} \in \mathcal{PIT}$. According to 1. it holds $\overline{A} \cup \overline{B} \in \mathcal{PIT}$. Hence $\overline{\overline{A} \cup \overline{B}} = A \cap B \in \mathrm{co}\mathcal{PIT}$. This shows $\mathrm{co}\mathcal{PIT} \wedge \mathrm{co}\mathcal{PIT} \subseteq \mathrm{co}\mathcal{PIT}$. □

Lemma 65. $\{(C_1, C_2) \mid C_1 \in \mathrm{EC}(\cap, +, \times) \text{ or } C_2 \notin \mathrm{EC}(\cap, +, \times)\}$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* $\mathcal{PIT} \vee \mathrm{co}\mathcal{PIT}$.

Proof. Due to Theorem 58 it holds $\{(C_1, C_2) \mid C_1 \in \mathrm{EC}(\cap, +, \times) \text{ or } C_2 \notin \mathrm{EC}(\cap, +, \times)\} \equiv_{\mathrm{m}}^{\log} \{(x, y) \mid x \in \mathrm{PIT} \text{ or } y \notin \mathrm{PIT}\}$ and therefore, it suffices to show that $\{(x, y) \mid x \in \mathrm{PIT} \text{ or } y \notin \mathrm{PIT}\}$ is $\leq_{\mathrm{m}}^{\log}$-complete for $\mathcal{PIT} \vee \mathrm{co}\mathcal{PIT}$. Let $A \in \mathcal{PIT} \vee \mathrm{co}\mathcal{PIT}$. Then there are $B \in \mathcal{PIT}$ and $C \in \mathrm{co}\mathcal{PIT}$ such that $A = B \cup C$. Hence $B \leq_{\mathrm{m}}^{\log} \mathrm{PIT}$ via some FL-function f and $C \leq_{\mathrm{m}}^{\log} \overline{\mathrm{PIT}}$ via some FL-function g. Thus $x \mapsto (f(x), g(x))$ shows $A \leq_{\mathrm{m}}^{\log} \{(x, y) \mid x \in \mathrm{PIT} \text{ or } y \notin \mathrm{PIT}\}$.

Furthermore $\{(x, y) \mid x \in \mathrm{PIT} \text{ or } y \notin \mathrm{PIT}\} \in \mathcal{PIT} \vee \mathrm{co}\mathcal{PIT}$ because $\{(x, y) \mid x \in \mathrm{PIT} \text{ or } y \notin \mathrm{PIT}\} = \{(x, y) \mid x \in \mathrm{PIT}\} \cup \{(x, y) \mid y \notin \mathrm{PIT}\}$ where $\{(x, y) \mid x \in \mathrm{PIT}\} \in \mathcal{PIT}$ and $\{(x, y) \mid y \notin \mathrm{PIT}\} \in \mathrm{co}\mathcal{PIT}$. □

Proposition 66. $\mathrm{EQ}(\cap, +, \times)$ *is* $\leq_{\mathrm{m}}^{\log}$*-complete for* $\mathcal{PIT} \vee \mathrm{co}\mathcal{PIT}$.

Proof. We first show $\mathrm{EQ}(\cap, +, \times) \in \mathcal{PIT} \vee \mathrm{co}\mathcal{PIT}$. Since each $\{\cap, +, \times\}$-circuit computes either a singleton set or the empty set, a pair (C_1, C_2) of $\{\cap, +, \times\}$-circuits is in $\mathrm{EQ}(\cap, +, \times)$ if and only if one of the following two conditions holds:

- $C_1 \cap C_2 \notin \mathrm{EC}(\cap, +, \times)$
- $C_1, C_2 \in \mathrm{EC}(\cap, +, \times)$.

Hence

$$\mathrm{EQ}(\cap, +, \times) = \underbrace{\{(C_1, C_2) \mid C_1 \cap C_2 \notin \mathrm{EC}(\cap, +, \times)\}}_{=:A} \cup \underbrace{\{(C_1, C_2) \mid C_1, C_2 \in \mathrm{EC}(\cap, +, \times)\}}_{=:B},$$

where according to Theorem 58 $A \in \mathcal{PIT}$ and $B = \{(C, C') \mid C \in \mathrm{EC}(\cap, +, \times)\} \cap \{(C, C') \mid C' \in \mathrm{EC}(\cap, +, \times)\} \in \mathrm{co}\mathcal{PIT} \wedge \mathrm{co}\mathcal{PIT} \overset{\text{Lemma 64}}{=} \mathrm{co}\mathcal{PIT}$.

We show $\{(C_1, C_2) \mid C_1 \in \mathrm{EC}(\cap, +, \times) \text{ or } C_2 \notin \mathrm{EC}(\cap, +, \times)\} \leq_{\mathrm{m}}^{\log} \mathrm{EQ}(\cap, +, \times)$ via the FL-function $(C_1, C_2) \mapsto (0 \times C_1, 0 \times (C_1 + C_2))$. If $C_1 \in \mathrm{EC}(\cap, +, \times)$, then both $0 \times C_1$ and $0 \times (C_1 + C_2)$ compute $\emptyset$. If $C_1 \notin \mathrm{EC}(\cap, +, \times)$, then we distinguish two cases:

- $C_2 \in \mathrm{EC}(\cap, +, \times)$: then $0 \times C_1$ computes the set $\{0\}$ whereas $0 \times (C_1 + C_2)$ computes the empty set.
- $C_2 \notin \mathrm{EC}(\cap, +, \times)$: then $0 \times C_1$ and $0 \times (C_1 + C_2)$ both compute the set $\{0\}$.

□

7 Conclusions and Open Questions

The results of this paper are summarized in Figure 2. For most of the emptiness problems it was possible to precisely characterize their complexity, while in some cases the lower and upper bounds do not match.

Our results provide new insights and improved complexity bounds for the following problems: $\mathrm{MC}(\cup, \cap, ^-, +, \times), \mathrm{MC}(\cap, +, \times)$ studied in [MW07], $\mathrm{MC}_{\mathbb{Z}}(+, \times), \mathrm{MC}_{\mathbb{Z}}(\cap, +, \times)$ studied in [Tra06], and $\mathrm{EQ}(\cup, \cap, ^-, +, \times), \mathrm{EQ}(+, \times), \mathrm{EQ}(\cap, +, \times)$ studied in [GHR⁺10].

The main open problem is to improve the bounds for $\mathrm{EC}(^-, +, \times)$ and $\mathrm{EC}(\cup, \cap, ^-, +, \times)$. Here the state of knowledge is as follows:

$\mathcal{O}$	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, 7	NL	NL	NL, 7	NL	NL, 7
$\cup\cap$	P, 8	P	P	P, 8	P	P, 8
$\cap+$	coC$_=$L, 11	coC$_=$L	coC$_=$L	coC$_=$L, 11	coNP, 20	coNP, 20
$\cap\times$	coC$_=$L, 11	P	coC$_=$L	P, 56	coNP, 14	coNP, 14
$^-+$	PSPACE, 42	PSPACE	PSPACE	2EXPSPACE	PSPACE	2EXPSPACE
$^-\times$	PSPACE, 42	PSPACE	PSPACE	3EXPSPACE	PSPACE	3EXPSPACE
$\cup\cap^-$	P	P, 8	NP, 10	NP, 10	coNP, 10	coNP, 10
$\cup\cap+$	PSPACE, 21	PSPACE	PSPACE	PSPACE, 21	PSPACE	PSPACE, 21
$\cup\cap\times$	PSPACE, 21	PSPACE	PSPACE	PSPACE, 57	PSPACE	PSPACE, 21
$\cap+\times$	co$\mathcal{PIT}$, 58	co$\mathcal{PIT}$	co$\mathcal{PIT}$	co$\mathcal{PIT}$, 62	Π_1, 44	Π_1
$^-+\times$	PSPACE	$\mathcal{R}_{tt}(\Sigma_1)$	Σ_1, 44	Σ_2	Π_1, 44	Π_2
$\cup\cap^-+$	PSPACE	PSPACE, 30	PSPACE	2EXPSPACE, 31	PSPACE	2EXPSPACE, 31
$\cup\cap^-\times$	PSPACE	PSPACE, 30	PSPACE	3EXPSPACE, 31	PSPACE	3EXPSPACE, 31
$\cup\cap+\times$	coNEXP, 3	coNEXP	coNEXP	coNEXP, 55	Π_1	Π_1, 44
$\cup\cap^-+\times$	L$^{\mathrm{NEXP}}$, 47	$\mathcal{R}_{tt}(\Sigma_1)$, 44	Σ_1	Σ_2, 44	Π_1	Π_2, 44

Figure 2: 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 Proposition 6 these results are obtained from white cells. Subsets $\mathcal{O}$ that are missing in the first column either correspond to trivial problems (Proposition 4) or can be transformed by De Morgan's law to an equivalent subset (Proposition 5). $\mathcal{PIT}$ 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 P $\subseteq \mathcal{PIT} \subseteq$ coR and it is a major open problem to improve these bounds.

1. Both problems are equivalent to problems studied in [MW07, GHR$^+$10]. More precisely, $\mathrm{EC}(^-,+,\times) \equiv_m^{\log} \mathrm{MC}(^-,+,\times)$ and $\mathrm{EC}(\cup,\cap,^-,+,\times) \equiv_m^{\log} \mathrm{MC}(\cup,\cap,^-,+,\times) \equiv_m^{\log} \mathrm{EQ}(\cup,\cap,^-,+,\times)$. (Corollary 47, Proposition 48)

2. Finding a decision algorithm is at least as difficult as solving Goldbach's conjecture. (Subsection 6.3)

3. The problems are either decidable or outside $\Sigma_1 \cup \Pi_1$. (Proposition 46)

4. The problems are $\leq_m$-hard for Σ_1 if and only if they are $\leq_m$-complete for $\mathcal{R}_{tt}(\Sigma_1)$. (Corollary 47)

Another open problem is to improve the complexity bounds whenever we have 2EXPSPACE or 3EXPSPACE as upper bounds. 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-EC$(\cup,\cap,^-,\times)$ is equivalent to the complement of Σ_1-MC$(\cup,\cap,^-,\times)$, which has already been investigated in [GRTW10, GJM16].

A third open problem is to improve the bounds for EC$(\cap,\times)$ and Σ_1-EC$(\cap,\times)$. Both problems are equivalent to MC$(\cap,\times)$, which has already been studied in [MW07].

Acknowledgements: We thank Klaus Reinhardt for sharing an unpublished proof of the PSPACE-hardness of MC$(^-,\times)$ (Corollary 36), which we slightly adapted to show the PSPACE-hardness of MC$^+(^-,+)$ (Lemma 34), and for helpful discussions on the PSPACE-hardness of MC$(^-,+)$. Moreover, we thank Jakob Sigmund for helpful discussions and contributions to the proof of Lemma 41.

References

[Aar03] S. Aaronson. Is P versus NP formally independent? *Bulletin of the EATCS*, 81:109–136, 2003.

[AKS04] M. Agrawal, N. Kayal, and N. Saxena. Primes is in P. *Annals of Mathematics*, 160:781–793, 2004.

[All97] E. Allender. Making computation count: Arithmetic circuits in the nineties. *SIGACT NEWS*, 28(4):2–15, 1997.

[AO96] E. Allender and M. Ogihara. Relationships among PL, #L, and the determinant. *RAIRO – Theoretical Informatics and Applications*, 30:1–21, 1996.

[Bès02] A. Bès. A survey of arithmetical definability. *Soc. Math. Belgique*, pages 1–54, 2002.

[Bre07] 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.

[Dos16] 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 fuer Informatik, 2016.

[DPR61] M. Davis, H. Putnam, and J. Robinson. The decision problem for exponential Diophantine equations. *Annals of Mathematics*, 74(2):425–436, 1961.

[FR75] 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.

[FR79] J. Ferrante and C. W. Rackoff. The computational complexity of logical theories. volume 718 of *Lecture Notes in Mathematics*. Springer Verlag, 1979.

[GHR$^+$10] 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.

[GJM15] C. Glaßer, P. Jonsson, and B. Martin. Constraint satisfaction problems around skolem arithmetic. *CoRR*, abs/1504.04181, 2015.

[GJM16] 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.

[Gol77] L. M. Goldschlager. The monotone and planar circuit value problems are log space complete for p. *SIGACT News*, 9(2):25–29, July 1977.

[Grä89] E. Grädel. Dominoes and the complexity of subclasses of logical theories. *Annals of Pure and Applied Logic*, 43(1):1–30, 1989.

[GRTW10] 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.

[IM83] O. Ibarra and S. Moran. Probabilistic algorithms for deciding equivalence of straight-line programs. *Journal of the ACM*, 30(1):217–228, 1983.

[KI04] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1):1–46, 2004.

[KL15] D. König and M. Lohrey. Parallel identity testing for skew circuits with big powers and applications. *CoRR*, abs/1502.04545, 2015.

[Knu02] D. E. Knuth. All questions answered. *Notices of the AMS*, 49(3):318–324, 2002.

[KSW87] J. Köbler, U. Schöning, and K. W. Wagner. The difference and the truth-table hierarchies for NP. *RAIRO Inform. Théor.*, 21:419–435, 1987.

[Lad75] R. E. Ladner. The circuit value problem is log space complete for P. *SIGACT News*, 7(1):12–20, 1975.

[LL76] R. E. Ladner and N. A. Lynch. Relativization of questions about log space computability. *Mathematical Systems Theory*, 10:19–32, 1976.

[LV03] 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.

[Mat70] Y. V. Matiyasevich. Enumerable sets are diophantine. *Doklady Akad. Nauk SSSR*, 191:279–282, 1970. Translation in Soviet Math. Doklady, 11:354–357, 1970.

[MW07] 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.

[Opp78] D. C. Oppen. A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger arithmetic. *J. Comput. Syst. Sci.*, 16:323–332, 1978.

[Pap94] C. M. Papadimitriou. *Computational complexity.* Addison-Wesley, Reading, Massachusetts, 1994.

[PD09] 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.

[Rei16] K. Reinhardt, 2016. Personal communication.

[Sax09] N. Saxena. Progress on polynomial identity testing. *Electronic Colloquium on Computational Complexity (ECCC)*, 16:101, 2009.

[Sax13] N. Saxena. Progress on polynomial identity testing - II. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:186, 2013.

[Sch86] A. Schrijver. *Theory of Linear and Integer Programming.* John Wiley & Sons, Inc., New York, NY, USA, 1986.

[Sig16] J. Sigmund, 2016. Personal communication.

[SM73] 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.

[SY10] 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.

[Tra06] S. D. Travers. The complexity of membership problems for circuits over sets of integers. *Theoretical Computer Science*, 369(1-3):211–229, 2006.

[Wag84] 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.

[Yan01] 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.