# Decidable Membership Problems for Finite Recurrent Systems over Sets of Naturals

Daniel Meister

Bayerische Julius-Maximilians-Universitaet Wuerzburg,
97074 Wuerzburg, Germany
meister@informatik.uni-wuerzburg.de

**Abstract.** A finite recurrent system over the power set of the natural numbers of dimension $n$ is a pair composed of $n$ $n$-ary functions over the power set of the natural numbers and an $n$-tuple of singleton sets of naturals. Every function is applied to the components of the tuple and computes a set of natural numbers, that might also be empty. The results are composed into another tuple, and the process is restarted. Thus, a finite recurrent system generates an infinite sequence of $n$-tuples of sets of natural numbers. The last component of a generated $n$-tuple is the output of one step, and the union of all outputs is the set defined by the system. We will consider only special finite recurrent systems: functions are built from the set operations union ($\cup$), intersection ($\cap$) and complementation ($\overline{\ }$) and the arithmetic operations addition ($\oplus$) and multiplication ($\otimes$). Sum and product of two sets of natural numbers are defined elementwise. We will study two types of membership problems: given a finite recurrent system and a natural number, does the set defined by the system contain the queried number, and does the output of a specified step contain the queried number? We will determine upper and lower bounds for such problems where we restrict the allowed operations to subsets of $\{\cup, \cap, \overline{\ }, \oplus, \otimes\}$. We will show completeness results for the complexity classes NL, NP and PSPACE.

## 1 Introduction

Sets of natural numbers can be represented by a variety of mathematical objects. Finite sets or co-finite sets, the complements of finite sets, can be represented by words over $\{0, 1\}$, i.e., by natural numbers, with a canonical interpretation. However, large sets require large numbers in this model. If these sets possess regularities a more efficient representation would be desirable. In case of sets that are neither finite nor co-finite such a simple representation does not work at all. Stockmeyer and Meyer defined integer expressions, which are expressions built from naturals, the set operations union, intersection and complementation and an addition operation [7]. Wagner studied a hierarchical model of a similar flavour that can be understood as arithmetic circuits [9], [10]. Such concise representations however make it difficult to derive information about the set from its representation. The *membership problem* for natural numbers in general can

M. Liśkiewicz and R. Reischuk (Eds.): FCT 2005, LNCS 3623, pp. 80–91, 2005.

be understood as the problem, given a set $M$ of natural numbers represented in a certain model and a number $b$, to decide whether $b$ belongs to set $M$. The complexity of the membership problem heavily depends on the representation and can generally be described by the formula: the more concise the representation the more complex the membership problem.

McKenzie and Wagner recently studied a large number of membership problems [2]. Given an arithmetic circuit over sets of natural numbers involving the standard set operations union, intersection, complementation and the arithmetic operations addition and multiplication (both operations are defined on sets, and sum and product of two sets are defined elementwise) and a natural number $b$, does the circuit represent a set that contains $b$? It was shown that restricting the set of possible operations as well as restricting circuits to formulas cover a wide range of complexity classes. Here, a formula is an arithmetic circuit where every vertex has at most one successor. Their work extends past works by Stockmeyer and Meyer [7], Wagner [9] and Yang [11].

The standard approach to circuits is via functions, and circuits represent these functions efficiently. In this sense, all problems above concern such circuits but applied only to fixed inputs. Circuits of various types have been studied deeply, and they are an interesting model to obtain lower bounds complexity results. A lot of information on this subject can be found in the book by Vollmer [8]. In this paper, we combine ideas that have been sketched above to obtain set representations by special recurrent systems.

Recurrences are well-known. The sequence $1, 1, 2, 3, 5, 8, \ldots$ of numbers—the Fibonacci numbers—is generated by the simple formula $F(n{+}2) =_{\text{def}} F(n{+}1) + F(n)$ where $F(0) =_{\text{def}} F(1) =_{\text{def}} 1$. Numerical simulations of single-particle or multi-particle systems in physics use systems of recurrences instead of differential equations. Recurrences play an important role in mathematics, computer and other sciences. Though recurrences normally involve only basic arithmetic operations such as addition and multiplication over the natural or the real numbers, operations do not have to be limited to this small collection. A recurrent system over sets of natural numbers of dimension $n$ is a pair consisting of a set of $n$ $n$-ary functions $f_1, \ldots, f_n$ over sets of natural numbers and an $n$-tuple of naturals. Starting from singleton sets defined by the $n$-tuple the result of function $f_i$ in one step is used as the $i$-th input in the next step (the precise definition is provided in Section 3). So, a recurrent system iteratively generates an infinite sequence of tuples of sets of natural numbers. The last component of each tuple is the output of the system in the corresponding evaluation step. Then, the union of all outputs defines a set that may be finite or infinite. The existential membership problem $\mathrm{M}_{ex}$ for recurrent systems asks whether there is an evaluation step such that the corresponding output contains a given number, and the exact membership problem $\mathrm{M}_{tm}$ asks whether a given number is contained in the result of a specified evaluation step. Functions are represented by arithmetic circuits.

We examine membership problems for recurrent systems for a restricted set of operations. Functions are built from the three known set operations and addi-

tion and multiplication. The general problems in this restricted sense are denoted by $\mathrm{M}_{ex}(\cup, \cap, \overline{\ }, \oplus, \otimes)$ and $\mathrm{M}_{tm}(\cup, \cap, \overline{\ }, \oplus, \otimes)$. Reducing the set of allowed operations leads to problems like $\mathrm{M}_{ex}(\cup, \oplus)$, where functions are built only from $\cup$ and $\oplus$, or $\mathrm{M}_{tm}(\oplus, \otimes)$. We will study the complexity of such membership problems with respect to the set of allowed operations. We will see that such problems are complete for a number of complexity classes where we will focus on NP- and PSPACE-complete problems. The general existential membership problem over $\{\cup, \cap, \overline{\ }, \oplus, \otimes\}$ is undecidable [4]; however, the exact complexity is not known in that sense that the currently best known lower bound (RE-hardness) does not meet the upper bound $\Sigma_2$. It is a most interesting question whether $\mathrm{M}_{ex}(\cup, \cap, \overline{\ }, \oplus, \otimes)$ is coRE-hard. This would imply undecidability of the general problem considered by McKenzie and Wagner [2]. Some evidence for undecidability was given by showing that a decision algorithm would prove or disprove Goldbach's conjecture about sums of primes.

This presentation is composed as follows. In Section 3, finite recurrent systems are defined, an example is discussed and basic and supplementary results are mentioned. The following sections classify a range of membership problems for recurrent systems. Section 4 considers membership problems that are contained in P. These problems are related to number-of-paths problems in graphs, whose complexities were studied in [3]. In Section 5, NP-complete problems, such as $\mathrm{M}_{ex}(\cap)$ and $\mathrm{M}_{ex}(\cap, \oplus)$, are considered, Section 6 considers PSPACE-complete problems, e.g., $\mathrm{M}_{ex}(\cup, \cap)$ and $\mathrm{M}_{ex}(\cup, \oplus, \otimes)$, and in Section 7, problems without exact classification are delt with. The conclusions section contains a table summarising the best known upper and lower complexity bounds for all possible problems. In most cases, proofs are omitted or reduced to just the main ideas.

## 2 Preliminaries

We fix the alphabet $\Sigma =_{\mathrm{def}} \{0, 1\}$. The set of all words over $\Sigma$ is denoted by $\Sigma^*$. All inputs are assumed to be given as words over $\Sigma$. For definitions and notations of complexity classes we refer to the book by Papadimitriou [5]. If the computation mode is not mentioned we mean deterministic computations; nondeterminism is always indicated. The class FL contains all functions that can be computed deterministically by a Turing machine with output tape using logarithmic working space. A set $A$ is *log-space reducible* to set $B$, $A \leq_m^{\mathrm{L}} B$, if there is $f \in \mathrm{FL}$ such that, for all $x \in \Sigma^*$, $x \in A \leftrightarrow f(x) \in B$. We will also say that $A$ *reduces* to $B$. For complexity class $\mathcal{C}$, set $A$ is $\leq_m^{\mathrm{L}}$*-complete* for $\mathcal{C}$, if $A \in \mathcal{C}$ and $B \leq_m^{\mathrm{L}} A$ for all $B \in \mathcal{C}$. We will shortly say that $A$ is $\mathcal{C}$-complete.

**Numbers.** The set of the natural numbers is denoted by $\mathbb{N}$ and surely contains 0. If we talk about numbers, we always mean natural numbers. Unless otherwise stated numbers are represented in binary form. The power set of $\mathbb{N}$ is the set of all subsets of $\mathbb{N}$. For natural numbers $a, b$, $a \leq b$, $[a, b] =_{\mathrm{def}} \{a, a+1, \ldots, b\}$. Two numbers are *relatively prime*, if their greatest common devisor is 1.

**Theorem 1 (Chinese Remainder Theorem).** *Let $b_1, \ldots, b_k$ be pairwise relatively prime numbers, and let $n_1, n_2 \in \mathbb{N}$. Let $b =_{\text{def}} b_1 \cdots b_k$. Then, $n_1 \equiv n_2 \pmod{b}$ if and only if $n_1 \equiv n_2 \pmod{b_i}$ for every $i \in [1, k]$.*

For set $A$ and two binary operations $\diamond$ and $\circ$ over $A$, the triple $(A, \diamond, \circ)$ is a *semiring* if $(A, \diamond)$ and $(A, \circ)$ are commutative monoids and the two distributive laws hold. For $+$ and $\cdot$ denoting addition and multiplication over $\mathbb{N}$, $(\mathbb{N}, +, \cdot)$ is a semiring. By $\mathrm{SR}(b)$ we denote the semiring $([0, b{+}1], \mathrm{sum}_b, \mathrm{prod}_b)$ where the binary operations $\mathrm{sum}_b$ and $\mathrm{prod}_b$ are defined as follows. Let $a_1, a_2 \in \mathbb{N}$.

$$\mathrm{sum}_b(a_1, a_2) =_{\text{def}} \begin{cases} a_1 + a_2 & \text{, if } a_1 + a_2 \leq b \\ b{+}1 & \text{otherwise} \end{cases}$$

Similarly for $\mathrm{prod}_b$. So, matrix multiplication over $\mathrm{SR}(b)$ is well-defined.

**Graphs.** A simple, finite, directed graph is a pair $G = (V, A)$ where $V$ is a finite set and $A \subseteq V \times V$. For two vertices $u, v \in V$ there is a *$u, v$-path* in $G$, if there is a sequence $(x_0, \ldots, x_k)$ such that $x_0 = u$, $x_k = v$ and $(x_i, x_{i+1}) \in A$ for all $i \in [0, k{-}1]$. The *graph accessibility problem for directed graphs*, denoted by GAP, is the set of all triples $(G, u, v)$ where $G$ is a directed graph, $u$ and $v$ are vertices of $G$ and there is a $u, v$-path in $G$. The problem GAP is NL-complete [6]. $G$ is *acyclic*, if there is no sequence $P = (x_0, \ldots, x_n)$ for $n$ the number of vertices of $G$ such that $P$ is an $x_0, x_n$-path in $G$ for any pair of vertices $x_0, x_n$ of $G$. The problem ACYC is the set of all directed acyclic graphs. Since GAP restricted to acyclic graphs is NL-complete, ACYC is NL-complete. For vertices $u$ and $v$ of $G$, $u$ is a *predecessor* of $v$, if $(u, v) \in A$.

**Circuits.** Let $\mathcal{O}$ be a set of commutative operations over set $M$. $C = (G, g_c, \alpha)$ is an $n$-ary *arithmetic $\mathcal{O}$-circuit* over $M$ for $n \geq 0$, if $G = (V, A)$ is a (simple, finite) acyclic graph, $g_C \in V$ is a specified vertex of $G$, the *output vertex*, and $\alpha : V \to \mathcal{O} \cup [1, n]$ such that $\alpha$ establishes a 1-1 correspondence between $n$ vertices without predecessor and $[1, n]$ and all other vertices are assigned operations from $\mathcal{O}$ whose arities correspond with the numbers of predecessors of the vertices. Vertices assigned a number are called *input vertices* of $C$. The arithmetic $\mathcal{O}$-circuit $C$ over $M$ represents a function $f_C$ over $M$ in the following way. Let $(a_1, \ldots, a_n) \in M^n$. The value of the input vertex assigned number $i$ is $a_i$, the value of vertex $u$ where $u$ is assigned an operation from $\mathcal{O}$ is the result of $\alpha(u)$ applied to the values of the predecessors of $u$. Then, $f_C(a_1, \ldots, a_n)$ is the value of the output vertex $g_C$. Let $f_C$ be an $n$-ary function represented by circuit $C$, and let $f_{C_1}, \ldots, f_{C_n}$ be $n'$-ary functions represented by circuits $C_1, \ldots, C_n$. A circuit representation of function $f(x_1, \ldots, x_{n'}) = f_C(f_{C_1}(x_1, \ldots, x_{n'}), \ldots, f_{C_n}(x_1, \ldots, x_{n'}))$ is obtained from $C, C_1, \ldots, C_n$ by identifying the input vertices of $C_1, \ldots, C_n$ assigned the same numbers and identifying the vertices of $C$ assigned numbers with the output vertex of the corresponding circuit $C_i$.

## 3 Finite Recurrent Systems

A recurrence is a pair composed of a function and initial values. From recurrences one can generate infinite sequences of objects by applying the function to

certain of already generated objects. Usual recurrences are defined over natural, real or complex numbers and involve only basic arithmetical operations like addition and multiplication. We extend this notion to recurrent systems over sets of numbers.

**Definition 1.** *A* **finite recurrent system** *over sets of natural numbers of dimension $n \geq 1$ is a pair $S = (\mathcal{F}, A)$ where $\mathcal{F} =_{\text{def}} \langle f_1, \ldots, f_n \rangle$ for $f_1, \ldots, f_n$ $n$-ary functions over sets of natural numbers and $A \in \mathbb{N}^n$. The dimension $n$ of $S$ is denoted by* $\dim S$.

Let $S = (\mathcal{F}, A)$ be a finite recurrent system over sets of natural numbers where $\mathcal{F} = \langle f_1, \ldots, f_n \rangle$ and $A = (a_1, \ldots, a_n)$. We define for every $t \in \mathbb{N}$:

$$\begin{aligned} S_i(0) &=_{\text{def}} S[f_i](0) =_{\text{def}} \{a_i\}, \quad i \in [1,n] \\ S_i(t{+}1) &=_{\text{def}} S[f_i](t{+}1) =_{\text{def}} f_i(S_1(t), \ldots, S_n(t)), \quad i \in [1,n] \\ \mathcal{F}(t) &=_{\text{def}} (S_1(t), \ldots, S_n(t)) \\ S(t) &=_{\text{def}} S_n(t)\,. \end{aligned}$$

So, $S_i(t)$ denotes the result of $f_i$ in the $t$-th evaluation step. We can say that a finite recurrent system over sets of naturals defines or represents an infinite sequence of sets of naturals. By $[S]$ we denote the union of these sets, i.e., $[S] =_{\text{def}} \bigcup_{t \geq 0} S(t)$. We are interested in two problems that arise from our definitions. We ask whether a number $b$ is generated in step $t$ and whether $b$ is generated in some step at all, i.e., contained in $[S]$.

Several authors studied membership problems of sets of natural numbers that can be built from singleton sets of natural numbers by applying the set operations union, intersection, complementation and the two arithmetic set operations addition and multiplication, denoted by $\oplus$ and $\otimes$ [7], [9], [11], [2]. Addition and multiplication on sets are defined elementwise. Let $A, B \subseteq \mathbb{N}$. Then, $A \oplus B =_{\text{def}} \{r{+}s : r \in A \text{ and } s \in B\}$ and $A \otimes B =_{\text{def}} \{r{\cdot}s : r \in A \text{ and } s \in B\}$. Let $\mathcal{O} \subseteq \{\cup, \cap, \overline{\ }, \oplus, \otimes\}$. An $n$-ary $\mathcal{O}$-function $f = f(x_1, \ldots, x_n)$ is a function over the variables $x_1, \ldots, x_n$ defined by using only operations from $\mathcal{O}$. An $\mathcal{O}$-function is an $n$-ary $\mathcal{O}$-function for some $n \geq 1$.

**Definition 2.** *Let $\mathcal{O} \subseteq \{\cup, \cap, \overline{\ }, \oplus, \otimes\}$. A* **finite recurrent $\mathcal{O}$-system** *$S = (\mathcal{F}, A)$ over sets of natural numbers is a finite recurrent system over sets of natural numbers where every function in $\mathcal{F}$ is an $\mathcal{O}$-function.*

Our introductory sample sequence, the sequence of Fibonacci numbers, can be generated by a finite recurrent $\{\oplus\}$-system. Let

$$\begin{aligned} &\mathcal{F} =_{\text{def}} \langle f_1, f_2 \rangle \text{ where } f_1(x_1, x_2) =_{\text{def}} x_2 \text{ and } f_2(x_1, x_2) =_{\text{def}} x_1 \oplus x_2 \\ &A =_{\text{def}} (0, 1)\,. \end{aligned}$$

Let $S =_{\text{def}} (\mathcal{F}, A)$. Then,

$$\begin{aligned} S(0) &= S_2(0) = \{1\} \\ S(1) &= S_2(1) = f_2(S_1(0), S_2(0)) = f_2(\{0\}, \{1\}) = \{1\} \\ S(2) &= S_2(2) = f_2(S_1(1), S_2(1)) = f_2(\{1\}, \{1\}) = \{2\}\,, \end{aligned}$$

and so on. We will often speak of *recurrent systems* for short, which always means finite recurrent $\{\cup, \cap, \overline{\ }, \oplus, \otimes\}$-systems over sets of naturals. Every recurrent system $S$ defines a possibly infinite set $[S]$ of natural numbers. The *existential membership problem* $\mathrm{M}_{ex}$ for recurrent systems asks whether a given number is contained in the defined set, and the *exact membership problem* $\mathrm{M}_{tm}$ asks whether a given number is contained in the result of a specified evaluation step. We want to study the complexities of these membership problems with respect to the allowed operations. Let $\mathcal{O} \subseteq \{\cup, \cap, \overline{\ }, \oplus, \otimes\}$.

$$\mathrm{M}_{ex}(\mathcal{O}) =_{\mathrm{def}} \{(S, b) : S \text{ a recurrent } \mathcal{O}\text{-system and } b \in [S]\}$$
$$\mathrm{M}_{tm}(\mathcal{O}) =_{\mathrm{def}} \{(S, t, b) : S \text{ a recurrent } \mathcal{O}\text{-system and } b \in S(t)\}$$

Instead of writing $\mathrm{M}_{ex}(\{\cup, \cap, \oplus\})$ we will write $\mathrm{M}_{ex}(\cup, \cap, \oplus)$ for short; similarly for the other problems. The complexities of our problems strongly depend on the input representation. We assume that natural numbers are given in binary form and functions are represented by arithmetic circuits with appropriate labels. For circuits we require any (standard) encoding that permits adjacency tests of two vertices and detection of labels of vertices in logarithmic space. It can be verified in nondeterministic logarithmic space whether an input represents an $\mathcal{O}$-function for $\mathcal{O} \subseteq \{\cup, \cap, \overline{\ }, \oplus, \otimes\}$. Using our notations, McKenzie and Wagner studied the complexity of the question, for given recurrent $\mathcal{O}$-system $S$ and number $b \geq 0$, whether $(S, 1, b) \in \mathrm{M}_{tm}(\mathcal{O})$ [2]. Their input representation additionally required a topological ordering of the vertices of the circuits, but this is only of importance for problems that are contained in NL. We will denote the problems investigated by McKenzie and Wagner by $\mathrm{MC}(\mathcal{O})$. It follows for every $\mathcal{O} \subseteq \{\cup, \cap, \overline{\ }, \oplus, \otimes\}$ that $\mathrm{M}_{tm}(\mathcal{O})$ is decidable if and only if $\mathrm{MC}(\mathcal{O})$ is decidable. The only such problems that have not yet been proved decidable are $\mathrm{MC}(\cup, \cap, \overline{\ }, \oplus, \otimes)$ and $\mathrm{MC}(\overline{\ }, \oplus, \otimes)$ (see also [2]).

**Proposition 1.**

*(i)* $\mathrm{M}_{tm}(\cup, \cap, \overline{\ }, \oplus, \otimes)$ *is either decidable or not recursively enumerable.*
*(ii)* $\mathrm{M}_{ex}(\cup, \cap, \overline{\ }, \oplus, \otimes)$ *is recursively enumerable if and only if* $\mathrm{MC}(\cup, \cap, \overline{\ }, \oplus, \otimes)$ *is decidable.*
*(iii)* $\mathrm{M}_{ex}(\overline{\ }, \oplus, \otimes)$ *is recursively enumerable if and only if* $\mathrm{MC}(\overline{\ }, \oplus, \otimes)$ *is decidable.*

Glaßer showed that $\mathrm{MC}(\cup, \cap, \overline{\ }, \oplus, \otimes)$ is contained in $\Delta_2 = \Sigma_2 \cap \Pi_2$ [1].

**Theorem 2.** *[4]*

*(i)* $\mathrm{M}_{ex}(\cup, \cap, \oplus, \otimes)$ *is* $\Sigma_1$*-complete.*
*(ii)* $\mathrm{M}_{ex}(\overline{\ }, \oplus, \otimes)$ *is* $\Sigma_1$*-hard.*
*(iii)* $\mathrm{M}_{tm}(\cup, \cap, \overline{\ }, \oplus, \otimes) \in \Delta_2$.
*(iv)* $\mathrm{M}_{ex}(\cup, \cap, \overline{\ }, \oplus, \otimes) \in \Sigma_2$.

## 4 Easiest Membership Problems

In this section we consider membership problems that are contained in P. These problems have a strong connection to graph problems concerning the numbers of paths of certain lengths between two vertices. Such problems are investigated in [3]. In the same paper connections to matrix problems are established. This matrix interpretation is also of great advantage in the study of the problem $\mathrm{M}_{tm}(\cap, \oplus)$.

As a general model, proofs showing containment results for existential membership problems have a common structure. First, an upper bound for the complexity of deciding $\mathrm{M}_{tm}(\mathcal{O})$ for $\mathcal{O} \subseteq \{\cup, \cap, \overline{\ }, \oplus, \otimes\}$ is given. Second, the value of $t$ is bounded by some number $r$ for which holds that $(S, b) \in \mathrm{M}_{ex}(\mathcal{O})$ if and only if there is $t < r$ such that $(S, t, b) \in \mathrm{M}_{tm}(\mathcal{O})$. Bound $r$ normally depends on $b$ and the dimension of $S$.

**Lemma 1.** $\mathrm{M}_{tm}(\overline{\ })$ *is in* L.

The problem $\mathrm{NMDP}(2, \beta)$ for $\beta \geq 1$ is the set of all tuples $(G, M, k, \nu, u, v)$ where $G = (V, A)$ is a simple finite directed graph, $M \subseteq V$, $u, v \in V$, $k, \nu \in \mathbb{N}$, $k$ is represented in binary form, $\nu$ is represented in $\beta$-ary form, and there are $\nu$ $u, v$-paths in $G$ each of which containing exactly $k$ vertices from set $M$. Let $\mathrm{ExNMDP}(2, \beta)$ denote the problem corresponding to $\mathrm{NMDP}(2, \beta)$ where we ask for *exactly* $\nu$ paths.

**Theorem 3.** *[3]*

*(i)* $\mathrm{NMDP}(2, 1)$ *and* $\mathrm{ExNMDP}(2, 1)$ *are* NL*-complete.*
*(ii)* $\mathrm{ExNMDP}(2, 2)$ *is in* P *and* $\mathrm{C}_{=}$L*-hard.*

**Lemma 2.** $\mathrm{M}_{tm}(\cup)$ *and* $\mathrm{M}_{tm}(\cap)$ *are* NL*-complete.*

*Proof.* For showing $\mathrm{M}_{tm}(\cup) \in \mathrm{NL}$ and $\mathrm{M}_{tm}(\cap) \in \mathrm{NL}$, both problems are reduced to $\mathrm{NMDP}(2, 1)$. Hardness of $\mathrm{M}_{tm}(\cup)$ and $\mathrm{M}_{tm}(\cap)$ follows by the canonical reduction from the accessibility problem for acyclic graphs.

**Theorem 4.** *(i)* $\mathrm{M}_{ex}(\emptyset)$ *and* $\mathrm{M}_{ex}(\overline{\ })$ *are in* L.
*(ii)* $\mathrm{M}_{ex}(\cup)$ *is* NL*-complete.*

McKenzie and Wagner showed that $\mathrm{MC}(\otimes)$ is NL-complete and that $\mathrm{MC}(\oplus)$ is $\mathrm{C}_{=}$L-complete [2].

**Theorem 5.** $\mathrm{M}_{tm}(\otimes)$ *is* NL*-complete, and* $\mathrm{M}_{tm}(\oplus)$ *is in* P *and* $\mathrm{C}_{=}$L*-hard.*

*Proof.* Containment of both problems is shown by using $\mathrm{ExNMDP}(2, 1)$ or $\mathrm{ExNMDP}(2, 2)$ as oracle set. Hardness of both problems follows by the results of McKenzie and Wagner [2].

Let $\mathrm{M}^{+}_{tm}(\cap, \otimes)$ denote the set of tuples $(S, t, b) \in \mathrm{M}_{tm}(\cap, \otimes)$ where $b > 0$. By a construction that replaces numbers by a representation over a basis of relatively prime numbers we can show the following lemma. The same idea with a different construction was used by McKenzie and Wagner to obtain similar results [2].

**Lemma 3.** $\mathrm{M}^{+}_{tm}(\cap, \otimes) \leq^{\mathrm{P}}_{m} \mathrm{M}_{tm}(\cap, \oplus)$.

A thorough analysis of recurrent $\{\cap, \oplus\}$-systems and results from linear algebra yield the following theorem. The main part of its proof shows how to decide in polynomial time whether $S(t)$ for $S$ a recurrent $\{\cap, \oplus\}$-system is empty. This problem is not solved entirely. However, in the uncertain case the result of $S(t)$ is either empty or too large. A complete solution of the emptyness problem is of great importance for solving $\mathrm{M}_{tm}(\cap, \otimes)$.

**Theorem 6.** $\mathrm{M}_{tm}(\cap, \oplus)$ *is in* P.

**Corollary 1.** $\mathrm{M}^{+}_{tm}(\cap, \otimes)$ *is in* P.

## 5 NP-Complete Membership Problems

To show hardness of the problems considered in this section, we define a new problem. This problem can be considered a generalization of the Chinese Remainder Theorem. The Chinese Remainder Theorem shows that a system of congruence equations where the moduli are pairwise relatively prime numbers has a solution that is unique in a determined interval of natural numbers. We extend this problem with respect to two aspects. Moduli are arbitrary numbers, and for each modulus we find a set of congruence equations. A solution of this *Set-system of congruence equations* fulfills one equation from each set. Formally, we define the problem Set-SCE as follows.

**Solving a Set-System of Congruence Equations (Set-SCE).**
Instance. $((A_1, b_1), \ldots, (A_k, b_k))$ where $A_1, \ldots, A_k$ are finite sets of natural numbers, and $b_1, \ldots, b_k$ are natural numbers greater than 1 represented in unary form.
Question. Are there $n \in \mathbb{N}$ and $a_1 \in A_1, \ldots, a_k \in A_k$ such that $n \equiv a_i \pmod{b_i}$ for all $i \in [1, k]$?

Note that it is not important to require binary representation of the numbers in $A_1, \ldots, A_k$. However, we assume a binary representation of them to fix a system.

**Lemma 4.** Set-SCE *is* NP*-hard.*

**Theorem 7.** $\mathrm{M}_{ex}(\cap)$, $\mathrm{M}_{ex}(\oplus)$, $\mathrm{M}_{ex}(\otimes)$, $\mathrm{M}_{ex}(\cap, \oplus)$, $\mathrm{M}^{+}_{ex}(\cap, \otimes)$ *are* NP*-complete.*

*Proof.* We only show that $\mathrm{M}_{ex}(\cap)$ is NP-complete by reducing Set-SCE to $\mathrm{M}_{ex}(\cap)$. Let $\mathcal{S} =_{\mathrm{def}} ((A_1, b_1), \ldots, (A_k, b_k))$ be an instance of Set-SCE. We assume that $A_i$ only contains numbers that are smaller than $b_i$. We define a recurrent $\{\cap\}$-system $S = (\mathcal{F}, A)$ as follows. For every $i \in [1, k]$, for every $j \in [1, b_i - 1]$ we define

$$f^{(i)}_{j}(\mathsf{x}) =_{\mathrm{def}} x^{(i)}_{j-1} \quad \text{and} \quad f^{(i)}_{0}(\mathsf{x}) =_{\mathrm{def}} x^{(i)}_{b_i - 1}$$

where $\mathsf{x} =_{\text{def}} (x_0^{(1)}, \ldots, x_{b_1-1}^{(1)}, x_0^{(2)}, \ldots, x_{b_k-1}^{(k)}, x')$. Let $A =_{\text{def}} (c_0^{(1)}, \ldots, c_{b_k-1}^{(k)}, 0)$ where $c_j^{(i)} \in \{0,1\}$ and $c_j^{(i)} = 1$ if and only if $j \in A_i$. Furthermore, let $f'(\mathsf{x}) =_{\text{def}} x_0^{(1)} \cap \cdots \cap x_0^{(k)}$ and $\mathcal{F} =_{\text{def}} \langle f_0^{(1)}, \ldots, f_{b_k-1}^{(k)}, f' \rangle$. It holds that $S[f_j^{(i)}](t) = 1$ if and only if $c_r^{(i)} = 1$ for $r < b_i$ and $r \equiv t - j \pmod{b_i}$. Hence, $(S,1) \in \mathrm{M}_{ex}(\cap)$ if and only if $\mathcal{S} \in$ Set-SCE. By Lemma 4, $\mathrm{M}_{ex}(\cap)$ is NP-hard.

**Corollary 2.** Set-SCE *is* NP*-complete.*

It remains open not only whether $\mathrm{M}_{tm}(\cap, \otimes)$ is polynomial-time decidable but also whether $\mathrm{M}_{ex}(\cap, \otimes)$ is contained in NP. We do not know any upper bound $c$ for $t$ such that $0 \in [S]$ if and only if $0 \in S(t)$ for some $t < c$ where $S$ is a recurrent $\{\cap, \otimes\}$-system.

## 6 PSPACE-Complete Membership Problems

This section contains three interesting results. First, we will see that the existential membership problem for finite recurrent $\{\cup, \cap\}$-systems is PSPACE-complete. Containment is a mere observation. Hardness is shown by a reduction from QBF. Astoundingly at first glance, the corresponding exact membership problem is PSPACE-complete, too. Second, we will see that $\mathrm{M}_{tm}(\cup, \oplus, \otimes)$ can be decided in polynomial space. This result is surprising when we keep in mind that $\mathrm{MC}(\cup, \oplus, \otimes)$ is PSPACE-complete [11]. Third, we will see that a recurrent $\{\cup, \oplus, \otimes\}$-system $S$ needs at most $(b+1) \cdot 2^{n^3}$ evaluation steps to generate number $b$ where $n =_{\text{def}} \dim S$. This leads to a polynomial-space decision algorithm for $\mathrm{M}_{ex}(\cup, \oplus, \otimes)$.

**Theorem 8.** *[7]* QBF *is* PSPACE*-complete.*

**Theorem 9.** $\mathrm{QBF} \leq_m^{\mathrm{L}} \mathrm{M}_{ex}(\cup, \cap)$.

We turn to recurrent $\{\cup, \oplus, \otimes\}$-systems.

**Lemma 5.** *Let $S = (\mathcal{F}, A)$ be a recurrent $\{\cup, \oplus, \otimes\}$-system, $n =_{\text{def}} \dim S$. Let $b \in \mathbb{N}$. Then, $b \in [S]$ if and only if there is $t < (b+1) \cdot 2^{n^3}$ such that $b \in S(t)$.*

As we have already discussed the problems $\mathrm{M}_{tm}(\mathcal{O})$ for $\mathcal{O} \subseteq \{\cup, \cap, \overline{\ }, \oplus, \otimes\}$ can be considered similar to the problems $\mathrm{MC}(\mathcal{O})$ with succinct input representation. For most of our problems succinctness led to an increase of complexity. With this phenomenon in mind it is surprising that we can show that $\mathrm{M}_{tm}(\cup, \oplus, \otimes)$ is solvable in polynomial space. It is known that $\mathrm{MC}(\cup, \oplus, \otimes)$ is PSPACE-complete [11].

**Theorem 10.** $\mathrm{M}_{tm}(\cup, \oplus, \otimes)$ *is in* PSPACE.

**Theorem 11.** $\mathrm{M}_{ex}(\cup, \cap)$, $\mathrm{M}_{ex}(\cup, \cap, \overline{\ })$, $\mathrm{M}_{ex}(\oplus, \otimes)$, $\mathrm{M}_{ex}(\cup, \oplus)$, $\mathrm{M}_{ex}(\cup, \otimes)$ *and* $\mathrm{M}_{ex}(\cup, \oplus, \otimes)$ *are* PSPACE*-complete.*

**Corollary 3.** $\mathrm{M}_{tm}(\cup, \cap)$, $\mathrm{M}_{tm}(\cup, \cap, \overline{\ })$, $\mathrm{M}_{tm}(\oplus, \otimes)$, $\mathrm{M}_{tm}(\cup, \oplus)$, $\mathrm{M}_{tm}(\cup, \otimes)$ *and* $\mathrm{M}_{tm}(\cup, \oplus, \otimes)$ *are* PSPACE*-complete.*

## 7 More Complicated Problems

In this final section we consider those problems that are not yet solved entirely. These are most of the problems that allow $\cap$- and $\otimes$-operations. But also $\mathrm{M}_{tm}(\cup,\cap,^{-},\oplus)$ and $\mathrm{M}_{ex}(\cup,\cap,^{-},\oplus)$ are still open. We will not give tight upper and lower bounds. In most cases, we obtain upper bounds by adequately restating results by McKenzie and Wagner. However, the complexity of the mentioned problem $\mathrm{M}_{tm}(\cup,\cap,^{-},\oplus)$ can significantly be improved with respect to the corresponding result from [2]. Let us first recall some necessary results.

**Theorem 12.** *[2]*

*(i)* $\mathrm{MC}(\cap,\otimes)$ *is in* P.
*(ii)* $\mathrm{MC}(\cap,\oplus,\otimes)$ *is in* coNP.
*(iii)* $\mathrm{MC}(\cup,\cap,^{-},\oplus)$ *and* $\mathrm{MC}(\cup,\cap,^{-},\otimes)$ *are in* PSPACE.
*(iv)* $\mathrm{MC}(\cup,\cap,\oplus,\otimes)$ *is* NEXP*-complete.*

Given a recurrent system $S$ and some number $t$, we find a circuit representation of $S(t)$ by concatenating circuits. We obtain the following corollary.

**Corollary 4.** *(i)* $\mathrm{M}_{tm}(\cap,\otimes)$ *is in* EXP.
*(ii)* $\mathrm{M}_{tm}(\cap,\oplus,\otimes)$ *is in* coNEXP.
*(iii)* $\mathrm{M}_{tm}(\cup,\cap,^{-},\oplus)$ *and* $\mathrm{M}_{tm}(\cup,\cap,^{-},\otimes)$ *are in* EXPSPACE.
*(iv)* $\mathrm{M}_{tm}(\cup,\cap,\oplus,\otimes)$ *is in* $2-$NEXP.

In case of recurrent $\{\cup,\cap,^{-},\oplus\}$-systems, we can improve the trivial exponential-space upper bound.

**Lemma 6.** $\mathrm{M}_{tm}(\cup,\cap,^{-},\oplus)$ *is in* EXP.

Observe that $\mathrm{M}_{tm}(\cup,\cap)$ reduces to $\mathrm{M}_{tm}(\cup,\cap,\oplus)$ and $\mathrm{M}_{tm}(^{-},\oplus)$. The latter reduction is done by replacing $\cap$ by $\oplus$, $A\cup B$ by $\overline{\overline{A}\oplus\overline{B}}$, the queried number $b$ by 0 and every other number by 1. So, $\mathrm{M}_{tm}(\cup,\cap,\oplus)$, $\mathrm{M}_{tm}(^{-},\oplus)$ and $\mathrm{M}_{tm}(\cup,\cap,^{-},\oplus)$ are PSPACE-hard.

**Proposition 2.** $\mathrm{M}_{ex}(\cup,\cap,^{-},\oplus)$ *is in* EXPSPACE.

In a way similar to the reduction from $\mathrm{M}_{tm}(\cup,\cap)$ to $\mathrm{M}_{tm}(^{-},\oplus)$, the former problem reduces to $\mathrm{M}_{tm}(^{-},\otimes)$. Replace every $\cup$ by $\otimes$ and every $A\cap B$ by $\overline{\overline{A}\otimes\overline{B}}$, replace the queried number $b$ by 0 and every other number by 1. Note that no $\{^{-},\otimes\}$-function on inputs only $\{0\}$ or $\{1\}$ can compute $\emptyset$, since no such function can compute a set that contains 0 and 1. This shows PSPACE-hardness of $\mathrm{M}_{tm}(^{-},\otimes)$.

## 8 Concluding Remarks

In this extended abstract we introduced and studied two types of membership problems for recurrent $\{\cup,\cap,^{-},\oplus,\otimes\}$-systems. Table 1 summarises our results.

**Table 1.** Currently best known complexity bounds for the membership problems for finite recurrent systems. The question marks stand for $\Delta_2$ or $\Sigma_2$.

| **Operation set** | **Exact problem** $\mathrm{M}_{tm}$ | | **Existential problem** $\mathrm{M}_{ex}$ | |
|---|---|---|---|---|
| | Lower bound | Upper bound | Lower bound | Upper bound |
| $\cup\ \cap\ {}^{-}\ \oplus\ \otimes$ | NEXP | ? | RE | ? |
| $\cup\ \cap\ \oplus\ \otimes$ | NEXP | 2−NEXP | RE | |
| ${}^{-}\ \oplus\ \otimes$ | PSPACE | ? | RE | ? |
| $\cup\ \oplus\ \otimes$ | PSPACE | | | |
| $\cap\ \oplus\ \otimes$ | PSPACE | coNEXP | PSPACE | RE |
| $\oplus\ \otimes$ | PSPACE | | | |
| $\cup\ \cap\ {}^{-}\ \oplus$ | PSPACE | EXP | PSPACE | EXPSPACE |
| $\cup\ \cap\ \oplus$ | PSPACE | EXP | PSPACE | EXPSPACE |
| ${}^{-}\ \oplus$ | PSPACE | EXP | PSPACE | EXPSPACE |
| $\cup\ \oplus$ | PSPACE | | | |
| $\cap\ \oplus$ | $\mathrm{C}_{=}\mathrm{L}$ | P | NP | |
| $\oplus$ | $\mathrm{C}_{=}\mathrm{L}$ | P | NP | |
| $\cup\ \cap\ {}^{-}\ \otimes$ | PSPACE | EXPSPACE | PSPACE | RE |
| $\cup\ \cap\ \otimes$ | PSPACE | EXPSPACE | PSPACE | RE |
| ${}^{-}\ \otimes$ | PSPACE | EXPSPACE | PSPACE | RE |
| $\cup\ \otimes$ | PSPACE | | | |
| $\cap\ \otimes$ | NL | EXP | NP | RE |
| $\otimes$ | NL | | NP | |
| $\cup\ \cap\ {}^{-}$ | PSPACE | | | |
| $\cup\ \cap$ | PSPACE | | | |
| $\cap$ | NL | | NP | |
| $\cup$ | NL | | | |
| ${}^{-}$ | L | | | |
| | L | | | |

The question marks stand for complexity classes beyond the class of recursively enumerable sets. Future work should tighten upper and lower bounds. There are especially two open problems that the author finds worth being considered: undecidability of $\mathrm{M}_{tm}(\cup, \cap, {}^{-}, \oplus, \otimes)$ and an interesting upper—or lower—bound for $\mathrm{M}_{ex}(\cap, \otimes)$. McKenzie and Wagner studied the emptyness problem for some circuits as an auxiliary problem. It would be interesting to solve the emptyness problem for recurrent $\{\cap, \oplus\}$-systems.

**Acknowledgements.** The idea to study finite recurrent systems was the result of a discussion with Klaus Wagner when a lot of people at Würzburg were studying membership problems for arithmetic circuits. I thank Bernhard Schwarz for his help.

## References


[1] Chr. Glasser, *private communication*, 2003.

[2] P. McKenzie, K.W. Wagner, *The Complexity of Membership Problems for Circuits over Sets of Natural Numbers*, Proceedings of the 20th Annual Symposium on Theoretical Aspects of Computer Science, STACS 2003, Lecture Notes in Computer Science 2607, Springer, pp. 571–582, 2003.

[3] D. Meister, *The complexity of problems concerning matrix powers and the numbers of paths in a graph*, manuscript.

[4] D. Meister, *Membership problems for recurrent systems over the power set of the natural numbers*, Technical report 336, Institut für Informatik, Bayerische Julius-Maximilians-Universität Würzburg, 2004.

[5] Ch.H. Papadimitriou, *Computational Complexity*, Addison-Wesley, 1994.

[6] W.J. Savitch, *Relationships Between Nondeterministic and Deterministic Tape Complexities*, Journal of Computer and System Sciences 4, pp. 177–192, 1970.

[7] L.J. Stockmeyer, A.R. Meyer, *Word Problems Requiring Exponential Time*, Proceedings of the ACM Symposium on the Theory of Computation, pp. 1–9, 1973.

[8] H. Vollmer, *Introduction to Circuit Complexity*, Springer, 1999.

[9] K. Wagner, *The Complexity of Problems Concerning Graphs with Regularities*, Proceedings of the 11th International Symposium on Mathematical Fondations of Computer Science, MFCS 1984, Lecture Notes in Computer Science 176, Springer, pp. 544–552, 1984.

[10] K.W. Wagner, *The Complexity of Combinatorial Problems with Succinct Input Representation*, Acta Informatica 23, pp. 325–356, 1986.

[11] K. Yang, *Integer Circuit Evaluation Is* PSPACE-*Complete*, Journal of Computer and System Sciences 63, pp. 288–303, 2001.