Institut für Informationssysteme Universität Hannover

Diplomarbeit

The Complexity of Post's Classes

Henning Schnoor

7. Juli 2004

Prüfer:
Prof. Dr. Heribert Vollmer
Prof. Dr. Rainer Parchmann

Erklärung

Hiermit versichere ich, dass ich diese Diplomarbeit selbst verfasst und dabei keine außer den angegebenen Quellen und Hilfsmitteln verwendet habe.

Henning Schnoor, Hannover den 7. Juli 2004

Contents

1 Introduction **1**

1.1 Boolean functions and Circuits . . . 1

1.2 Known complexity results . . . 10

2 Upper bounds **11**

2.1 Subclasses of L . . . 12

2.2 Subclasses of M . . . 14

3 R_1-and R_2-formulas **15**

4 0-separating formulas **18**

4.1 Basic properties . . . 18

4.2 $\mathrm{S}_0, \mathrm{S}_{02}, \mathrm{S}_0^k$ and S_{02}^k-formulas . . . 20

4.3 S_{00}-, S_{00}^k-, S_{01}-, S_{01}^k-formulas and open problems . . . 22

5 Formulas representing monotonic functions **25**

6 Formulas representing self-dual functions **26**

7 Conclusions and generalizations **28**

8 Collection of results **29**

1 Introduction

The complexity of problems related to Boolean functions has been of special interest throughout the history of complexity theory. Many problems of this kind are standard examples for certain complexity classes - the first problem ever to be proven NP-complete was the satisfiability problem for Boolean formulas.

In the twenties of the last century, Emil Post studied sets B of Boolean functions closed under the closure operator *superposition*, which means the class of Boolean functions which can be expressed by formulas using only functions from B as connectives. He identified every set of Boolean functions closed under this operator, determined the complete inclusion structure of these sets and gave a finite base for every closed set. These sets of Boolean functions are now called Post's lattice.

The complexity of problems related to Boolean functions, like the satisfiability problem, is depending on the set of connectives used in the examined Boolean formulas. In 1979, Lewis showed that the satisfiability problem is either NP-complete or polynomial-time solvable, depending on which connectives are allowed in the formula ([Lew79]). Steffen Reith studied the complexity of many problems related to Post's lattice in [Rei01]. He proved coNP-completeness for many problems which we can use in this thesis to show completeness for our problems.

A more general problem than satisfiability is the question if a given Boolean formula describes a function from any of the closed classed Post identified. In this thesis we examine the computational complexity of the following problem: Given classes A and B from Post's lattice, how difficult is it to decide if a given formula using only connectives from B describes a function from A? For nearly every combination, we show this problem is polynomial-time solvable or coNP-complete. We will also see these results are identical for Boolean formulas and Boolean circuits.

We build up on the results presented in [Böh], in which the difficulty of deciding a similar problem was discussed, which serves as an upper complexity bound for our problem.

1.1 Boolean functions and Circuits

A standard way of representing Boolean functions is to write them as Boolean formulas. Most people working in computer science are familiar with formulas like $x \vee (y \wedge \overline{z})$. Usually, only $\vee, \wedge$ and negation are used in formulas, as in fact, every Boolean function can be represented using only these three connectives. In this thesis, we examine more general Boolean formulas, using arbitrary functions as connectives. Intuitively, it is clear what a Boolean formula over the base $\{\rightarrow, \neg\}$ is. Formally, Boolean formulas are defined as a special case of Boolean circuits. Our definition is based on the one in [Vol99].

Definition Let B be a finite set of Boolean functions. A *B-circuit with input-variables* $x_1, \dots, x_n$ is a tuple $C = (V, E, \alpha, \beta, o)$ where (V, E) is a finite directed acyclic graph, $\alpha\colon E \to \mathbb{N}$ is an injective function, $\beta\colon V \to B \cup \{x_1, \dots, x_n\}$ is a function, and $o \in V$, such that

- If $v \in V$ has in-degree 0, then $\beta(v) \in \{x_1, \dots, x_n\}$ or $\beta(v)$ is a 0-ary function (i.e. a constant) from B.

- If $v \in V$ has in-degree $k > 0$, then $\beta(v)$ is a k-ary function from B.

Nodes $v \in V$ are called *gates* in C, $\beta(v)$ is the gate-type of v. $o \in V$ is the *output-gate* of C. The function α is needed to define the order of arguments for non-commutative functions like $\to$. We will now define the function $f_C\colon \{0,1\}^n \to \{0,1\}$ calculated by the circuit C, by inductively defining a function $\mathrm{val}_v\colon \{0,1\}^n \to \{0,1\}$ for every gate v in C:

Let $\alpha_1, \dots, \alpha_n \in \{0,1\}$.

- If $v \in V$ has in-degree 0, and if $\beta(v) = x_i$ for $i \in \{1, \dots, n\}$, then $\mathrm{val}_v(\alpha_1, \dots, \alpha_n) := \alpha_i$.

- If $v \in V$ has in-degree 0, and if $\beta(v) = c$ for some 0-ary (constant) function c from B, then $\mathrm{val}_v(\alpha_1, \dots, \alpha_n) := c$.

- Let $v \in V$ have in-degree $k > 0$, and let $v_1, \dots, v_k$ be the predecessor gates of v such that $\alpha((v_1, v)) < \dots < \alpha((v_k, v))$. Let $\beta(v) =: f \in B$ a k-ary function. Then let $\mathrm{val}_v(\alpha_1, \dots, \alpha_n) := f(\mathrm{val}_{v_1}(\alpha_1, \dots, \alpha_n), \dots, \mathrm{val}_{v_k}(\alpha_1, \dots, \alpha_n))$.

Let $f_C := \mathrm{val}_o$. f_C is the function computed by the Boolean circuit C. A *Boolean formula* is a Boolean circuit where each gate has out-degree ≤ 1.

The *size* of a Boolean circuit C is the number of gates: $|C| := |V|$.

In this text, we will also use standard propositional formulas like $f_1 \to f_2$ to describe Boolean formulas. The construction of the corresponding circuit is obvious. We write $\leftrightarrow$ for equivalence in Boolean formulas, and $\Leftrightarrow$ for equivalence in the meta-language. We write $f \equiv g$, for Boolean formulas f and g, if the formulas are identical as a Boolean circuit. We write $f = g$, if for all input tuples, f and g evaluate to the same value, that is if $f_f = f_g$, e.g. we write $x_1 \vee (\overline{x_2} \wedge x_1) = x_1$ instead of $f_{x_1 \vee (\overline{x_2} \wedge x_1)} = f_{x_1}$.

As for a formula or circuit C with different input variables, it is not always obvious what we mean with $f_C(\alpha_1, \dots, \alpha_n)$ we introduce the following notation: For a circuit C with input variables $s_1, \dots, s_n$ for some symbols s_i, and for values $\alpha_1, \dots, \alpha_n$ from $\{0,1\}$, we write $C(s_1 = \alpha_1, s_2 = \alpha_2, \dots, s_n = \alpha_n)$ for the value of the function f_C when given the tuple $(\alpha_1, \ldots, \alpha_n)$ as argument in the order which assigns the binary value α_i to the input gate s_i. If the variables are the set $\{x_1, \ldots, x_n\}$, we simply write $C(v_1, \ldots, v_n)$ for $C(x_1 = v_1, \ldots, x_n = v_n)$, or, for a tuple $\overrightarrow{\alpha} = (\alpha_1, \ldots, \alpha_n), \in \{0,1\}^n$, we write $C(\overrightarrow{\alpha})$ for $C(x_1 = \alpha_1, \ldots, x_n = \alpha_n)$. If the input variables for C are the set $\{x_1, \ldots, x_n, s_1, \ldots, s_k\}$, then for a tuple $\overrightarrow{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$ and values $\beta_1, \ldots, \beta_k \in \{0,1\}$, we write $C(\overrightarrow{x} = \overrightarrow{\alpha}, s_1 = \beta_1, \ldots, s_k = \beta_k)$ for $C(x_1 = \alpha_1, \ldots, x_n = \alpha_n, s_1 = \beta_1, \ldots, s_k = \beta_k)$.

We say a set A of Boolean functions is a *closed class* if A contains the identity and is closed under the following operations(definition taken from [Rei01]):

- *Substitution*: Let f^n and g^m be Boolean functions. then we define h^{n+m-1} as $h(\alpha_1, \ldots, \alpha_{n-1}, \beta_1, \ldots, \beta_m) := f(\alpha_1, \ldots, \alpha_{n-1}, g(\beta_1, \ldots, \beta_m))$ for all $\alpha_1, \ldots, \alpha_{n-1}$, $\beta_1, \ldots, \beta_m \in \{0,1\}$.

- *Permutation of variables*: Let f^n be a Boolean function and $\Pi\colon \{1, \ldots, n\} \rightarrow \{1, \ldots, n\}$ be a permutation. Then we define $g(\alpha_1, \ldots, \alpha_n) := f(\alpha_{\Pi(1)}, \ldots, \alpha_{\Pi(n)})$ for all $\alpha_1, \ldots, \alpha_n \in \{0,1\}$.

- *Identification of the last variables:* Let f^n be a Boolean function. Then we define g^{n-1} as $g(\alpha_1, \ldots, \alpha_{n-1}) := f(\alpha_1, \ldots, \alpha_{n-1}, \alpha_{n-1})$ for all $\alpha_1, \ldots, \alpha_n \in \{0,1\}$. Identification of arbitrary variables can be achieved by combining this with permutation of variables.

- *Introduction of a fictive variable*: Let f^n be a Boolean function. Then we define g^{n+1} as $g(\alpha_1, \ldots, \alpha_{n+1}) := f(\alpha_1, \ldots, \alpha_n)$ for all $\alpha_1, \ldots, \alpha_{n+1} \in \{0,1\}$.

The set of these operations is called *superposition*. For a set B of Boolean functions, let $[B]$ denote the smallest set A of Boolean functions such that $B \subseteq A$ and A is a closed class. We say B is a *base* of $[B]$. Basically, $[B]$ is the set of all Boolean functions which can be calculated with B-circuits or B-formulas. The usual closure properties hold, i.e. $B \subseteq [B]$,$B_1 \subseteq B_2$ implies $[B_1] \subseteq [B_2]$ and $[[B]] = [B]$.

Emil Post showed in [Pos41] that the list of closed classes shown in Table 1 is complete, and the inclusion structure for these classes is shown in Figure 1. As any set of sets closed under a closure operator, Post's classes form a lattice. There are five maximal closed classes below BF: $\mathrm{R}_0, \mathrm{R}_1, \mathrm{M}, \mathrm{L}$ and D.

Definition Let $n \in \mathbb{N}$, f, g be Boolean functions of arity n, $A \subseteq \{0,1\}^n$, $\alpha \in \{0,1\}$, $m \in \mathbb{N}$, $m \geq 2$.

- $\mathrm{dual}(f)$ is the function $\mathrm{dual}(f)(\alpha_1, \ldots, \alpha_n) := \neg f(\overline{\alpha_1}, \ldots, \overline{\alpha_n})$.

- For a set B of Boolean functions, let $\text{dual}(B) := \{\text{dual}(f) | f \in B\}$.

A is called

- α-separating, if there exists an i such that for all $(\alpha_1, \ldots, \alpha_n) \in A$, $\alpha_i = \alpha$.

f is called

- *monotonic*, if for all $(\alpha_1, \ldots, \alpha_n)$ and $(\beta_1, \ldots, \beta_n)$ with $\alpha_i \leq \beta_i$ for all $1 \leq i \leq n$ holds $f(\alpha_1, \ldots, \alpha_n) \leq f(\beta_1, \ldots, \beta_n)$.
- *self-dual* if $\text{dual}(f) = f$
- *α-reproducing*, if $f(\alpha, \ldots, \alpha) = \alpha$).
- *α-separating*, if $f^{-1}(\{\alpha\})$ is α-separating
- *α-separating of degree m*, if every subset $S \subseteq f^{-1}(\{\alpha\})$ with $|S| = m$ is α-separating

We say

- $f \leq g$, if for all $(\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$, $f(\alpha_1, \ldots, \alpha_n) \leq g(\alpha_1, \ldots, \alpha_n)$ holds.
- For a tuple $\overrightarrow{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$, let $\overline{\overrightarrow{\alpha}} := (\overline{\alpha_1}, \ldots, \overline{\alpha_n})$.

Finally, let $h_m(x_1, \ldots, x_{m+1}) := \bigvee_{i=1}^{m+1} x_1 \wedge x_2 \wedge \cdots \wedge x_{i-1} \wedge x_{i+1} \wedge \cdots \wedge x_{m+1}$. This function is 1-separating of degree m, but not 1-separating of degree $m+1$.

Definition

- Let $\mathcal{P}$ denote the set of closed classes in Post's lattice.
- Let $B \in \mathcal{P}$ a class from Post's lattice. By $\text{base}(B)$ we denote the base for B given in table 1.
- For $B \in \mathcal{P}$, we often say B-circuit as an abbreviation for $\text{base}(B)$-circuit, and B-formula as a short form for $\text{base}(B)$-formula. So, a B-circuit is a circuit using only elements from the base of B as gates.
- For a class $A \in \mathcal{P}$, let $\mathcal{M}(A) := \{C | C \text{ is a Boolean circuit such that } f_C \in A\}$. Observe that for classes A_1, A_2, trivially $A_1 \subseteq A_2 \Leftrightarrow \mathcal{M}(A_1) \subseteq \mathcal{M}(A_2)$ holds.
- For a set A of Boolean functions and a class B from $\mathcal{P}$, let

$\mathcal{M}(A \twoheadleftarrow B) := \{f | f \text{ is a } B\text{-formula and } f \in \mathcal{M}(A)\}$

$\mathcal{M}_C(A \twoheadleftarrow B) := \{C | C \text{ is a } B\text{-circuit and } C \in \mathcal{M}(A)\}$

We will call $\mathcal{M}(A \twoheadleftarrow B)$ the A-membership problem for B-formulas and $\mathcal{M}_C(A \twoheadleftarrow B)$ the A-membership problem for B-circuits.

- For classes $A, B \in \mathcal{P}$, let $\mathcal{M}(A \wr_B) := \{C | C \text{ is a } \{\wedge, \vee, \neg\}\text{-circuit and } C \in \mathcal{M}(A)\}$ for circuits guaranteed to be in B. This means the decision algorithm only has to answer the question "Is f_C in A?" correctly for circuits with $f_C \in B$ (for a formal definition, see [Böh]). $\mathcal{M}(A \wr_B)$ is called the *membership problem for B-circuits with promise A.*

- For a circuit C, we say x_i is a *relevant variable* if there are $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n$ such that

$$C(x_1 = \alpha_1, \ldots, a_{i-1} = \alpha_{i-1}, x_i = 0, x_{i+1} = \alpha_{i+1}, \ldots, x_n = \alpha_n) \neq$$
$$C(x_1 = \alpha_1, \ldots, a_{i-1} = \alpha_{i-1}, x_i = 1, x_{i+1} = \alpha_{i+1}, \ldots, x_n = \alpha_n).$$

For a B-formula f, $f \in \mathcal{M}(A \twoheadleftarrow B)$ holds if and only if there is a A-formula g with $f = g$. In this thesis, we will examine the computational complexity of deciding the A-membership problem for B-formulas for all combinations $A, B \in \mathcal{P}$. We will not try to find an actual A-formula describing a given function, we just determine if such a formula exists. For the demonstrated algorithms, we will make some assumptions about the input of the algorithm for convenience. For once, we will always assume the input formula is a correct B-formula. To check this can obviously be done in polynomial time before starting the actual algorithm. We will also assume the variables in a given input formula are $x_1, \ldots, x_n$ for some $n \in \mathbb{N}$. If other variables are used, we can simply rename the occurring variables.

Since a formula is just a special case of a Boolean circuit, it is obvious that $\mathcal{M}(A \twoheadleftarrow B) \leq_m^p \mathcal{M}_C(A \twoheadleftarrow B)$ holds for all classes A, B. Thus, we will show polynomial-time results for the circuit problem, and coNP-completeness for the formula problem. With this, it follows $\mathcal{M}(A \twoheadleftarrow B) \equiv_m^p \mathcal{M}_C(A \twoheadleftarrow B)$ for all classes $A, B \in \mathcal{P}$ for which we can decide the complexity. If we look closer at the complexity than just the difference between polynomial-time solvable and coNP-complete, there most likely will be a difference between circuits and formulas for our membership problems, as in [Rei01], it was shown the complexity of the circuit value problem is different from the formula value problem - in this thesis, we only use the fact that both are solvable in polynomial time.

Proposition 1 *Let $A, B \in \mathcal{P}$. Then*

1. $\mathcal{M}(A \twoheadleftarrow B) = \mathcal{M}(A \cap B \twoheadleftarrow B)$
2. $\mathcal{M}_C(A \twoheadleftarrow B) = \mathcal{M}_C(A \cap B \twoheadleftarrow B)$
3. $\mathcal{M}(B \twoheadleftarrow B)$ *is in* P

The consequence of Proposition 1 is that we only have to consider $\mathcal{M}(A \twoheadleftarrow B)$ for classes A, B such that $A \subsetneqq B$ holds.

In [Böh], Böhler examined the complexity of $\mathcal{M}(A \wr_B)$ for classes A, B from $\mathcal{P}$. Our problem $\mathcal{M}_C(A \twoheadleftarrow B)$ seems easier than that one on first sight, since we do not only have the information a certain formula or circuit describes a function from a class B, but we also have the representation as a B-circuit. However, we must consider that the expansion of a given B-circuit into a $\{\vee, \wedge, \neg\}$-circuit describing the same function cannot always easily be done in polynomial time - for example, a circuit calculating the function $x_1 \oplus x_2 \oplus \cdots \oplus x_n$ cannot be expressed as $\{\vee, \wedge. \neg\}$-formula in a straightforward way without the result growing exponentially in size with regard to n. Thus, we cannot take $\mathcal{M}(A \wr_B)$ for granted as an upper bound for our problem. However, in the proofs for polynomial-time results, Böhler used only the fact that the value of a Boolean circuit can be calculated in polynomial time, and this holds for our case as well. Therefore, at least for the polynomial-time results, $\mathcal{M}_C(A \twoheadleftarrow B) \leq_m^p \mathcal{M}(A \wr_B)$ holds.

The membership problem for BF-formulas, meaning formulas containing $\vee, \wedge$ and $\neg$ as connectives, is coNP-complete in nearly every case, as the following theorem shows. The theorem was proven by Klaus Wagner, the proof can be found in [Böh].

Theorem 2 $\mathcal{M}(A \twoheadleftarrow \mathrm{BF})$ *is coNP-complete for every closed class of Boolean functions A such that $A \notin \{\emptyset, \mathrm{R}_0, \mathrm{R}_1, \mathrm{R}_2, \mathrm{BF}\}$. $\mathcal{M}(A \twoheadleftarrow \mathrm{BF}) \in \mathrm{P}$ for $A \in \{\emptyset, \mathrm{R}_0, \mathrm{R}_1, \mathrm{R}_2, \mathrm{BF}\}$.*

Since there are a lot of combinations A, B for which $\mathcal{M}(A \twoheadleftarrow B)$ can be examined, we need methods for reducing the number of combinations we actually have to look at. With help of the lattice structure Post proved for his classes, it is easy to see we only have to examine a subset of the possible combinations. In the following paragraphs we present definitions and elementary, yet useful results.

Name	Definition	Base
BF	All Boolean functions	$\{\vee, \wedge, \neg\}$
R_0	$\{f \in BF \mid f$ is 0-reproducing $\}$	$\{\wedge, \oplus\}$
R_1	$\{f \in BF \mid f$ is 1-reproducing $\}$	$\{\vee, \leftrightarrow\}$
R_2	$R_1 \cap R_0$	$\{\vee, x \wedge (y \leftrightarrow z)\}$
M	$\{f \in BF \mid f$ is monotonic $\}$	$\{\vee, \wedge, 0, 1\}$
M_1	$M \cap R_1$	$\{\vee, \wedge, 1\}$
M_0	$M \cap R_0$	$\{\vee, \wedge, 0\}$
M_2	$M \cap R_2$	$\{\vee, \wedge\}$
S_0^n	$\{f \in BF \mid f$ is 0-separating of degree $n\}$	$\{\rightarrow, \text{dual}(h_n)\}$
S_0	$\{f \in BF \mid f$ is 0-separating $\}$	$\{\rightarrow\}$
S_1^n	$\{f \in BF \mid f$ is 1-separating of degree $n\}$	$\{x \wedge \overline{y}, h_n\}$
S_1	$\{f \in BF \mid f$ is 1-separating $\}$	$\{x \wedge \overline{y}\}$
S_{02}^n	$S_0^n \cap R_2$	$\{x \vee (y \wedge \overline{z}), \text{dual}(h_n)\}$
S_{02}	$S_0 \cap R_2$	$\{x \vee (y \wedge \overline{z})\}$
S_{01}^n	$S_0^n \cap M$	$\{\text{dual}(h_n), 1\}$
S_{01}	$S_0 \cap M$	$\{x \vee (y \wedge z), 1\}$
S_{00}^n	$S_0^n \cap R_2 \cap M$	$\{x \vee (y \wedge z), \text{dual}(h_n)\}$
S_{00}	$S_0 \cap R_2 \cap M$	$\{x \vee (y \wedge z)\}$
S_{12}^n	$S_1^n \cap R_2$	$\{x \wedge (y \vee \overline{z}), h_n\}$
S_{12}	$S_1 \cap R_2$	$\{x \wedge (y \vee \overline{z})\}$
S_{11}^n	$S_1^n \cap M$	$\{h_n, 0\}$
S_{11}	$S_1 \cap M$	$\{x \wedge (y \vee z), 0\}$
S_{10}^n	$S_1^n \cap R_2 \cap M$	$\{x \wedge (y \vee z), h_n\}$
S_{10}	$S_1 \cap R_2 \cap M$	$\{x \wedge (y \vee z)\}$
D	$\{f \mid f$is self-dual$\}$	$\{x\overline{y} \vee x\overline{z} \vee (\overline{y} \wedge \overline{z})\}$
D_1	$D \cap R_2$	$\{xy \vee x\overline{z} \vee y\overline{z}\}$
D_2	$D \cap M$	$\{xy \vee yz \vee xz\}$
L	$\{f \mid f$is linear$\}$	$\{\oplus, 1\}$
L_0	$L \cap R_0$	$\{\oplus\}$
L_1	$L \cap R_1$	$\{\leftrightarrow\}$
L_2	$L \cap R$	$\{x \oplus y \oplus z\}$
L_3	$L \cap D$	$\{x \oplus y \oplus z \oplus 1\}$
V	$\{f \mid$ There is a formula of the form $c_0 \vee c_1x_1 \vee \cdots \vee c_nx_n$ such that c_i are constants for $1 \leq i \leq n$ that describes $f\}$	$\{\vee, 1, 0\}$
V_0	$[\{\vee\}] \cup \{0\}$	$\{\vee, 0\}$
V_1	$[\{\vee\}] \cup \{1\}$	$\{\vee, 1\}$
V_2	$[\{\vee\}]$	$\{\vee\}$
E	$\{f \mid$ There is a formula of the form $c_0 \wedge (c_1 \vee x_1) \wedge \cdots \wedge (c_n \vee x_n)$ such that c_i are constants for $1 \leq i \leq n$ that describes $f\}$	$\{\wedge, 1, 0\}$
E_0	$[\{\wedge\}] \cup \{0\}$	$\{\wedge, 0\}$
E_1	$[\{\wedge\}] \cup \{1\}$	$\{\wedge, 1\}$
E_2	$[\{\wedge\}]$	$\{\wedge\}$
N	$[\{\neg\}] \cup \{0\} \cup \{1\}$	$\{\neg, 1\}$
N_2	$[\{\neg\}]$	$\{\neg\}$
I	$[\{\text{id}\}] \cup \{0\} \cup \{1\}$	$\{\text{id}, 0, 1\}$
I_0	$[\{\text{id}\}] \cup \{0\}$	$\{\text{id}, 0\}$
I_1	$[\{\text{id}\}] \cup \{1\}$	$\{\text{id}, 1\}$
I_2	$[\{\text{id}\}]$	$\{\text{id}\}$

Table 1: List of all closed classes of Boolean functions with bases

$$(h_n(x_1, \ldots, x_{n+1}) := \bigvee_{i=1}^{n+1} x_1 \wedge x_2 \wedge \cdots \wedge x_{i-1} \wedge x_{i+1} \wedge \cdots \wedge x_{n+1})$$

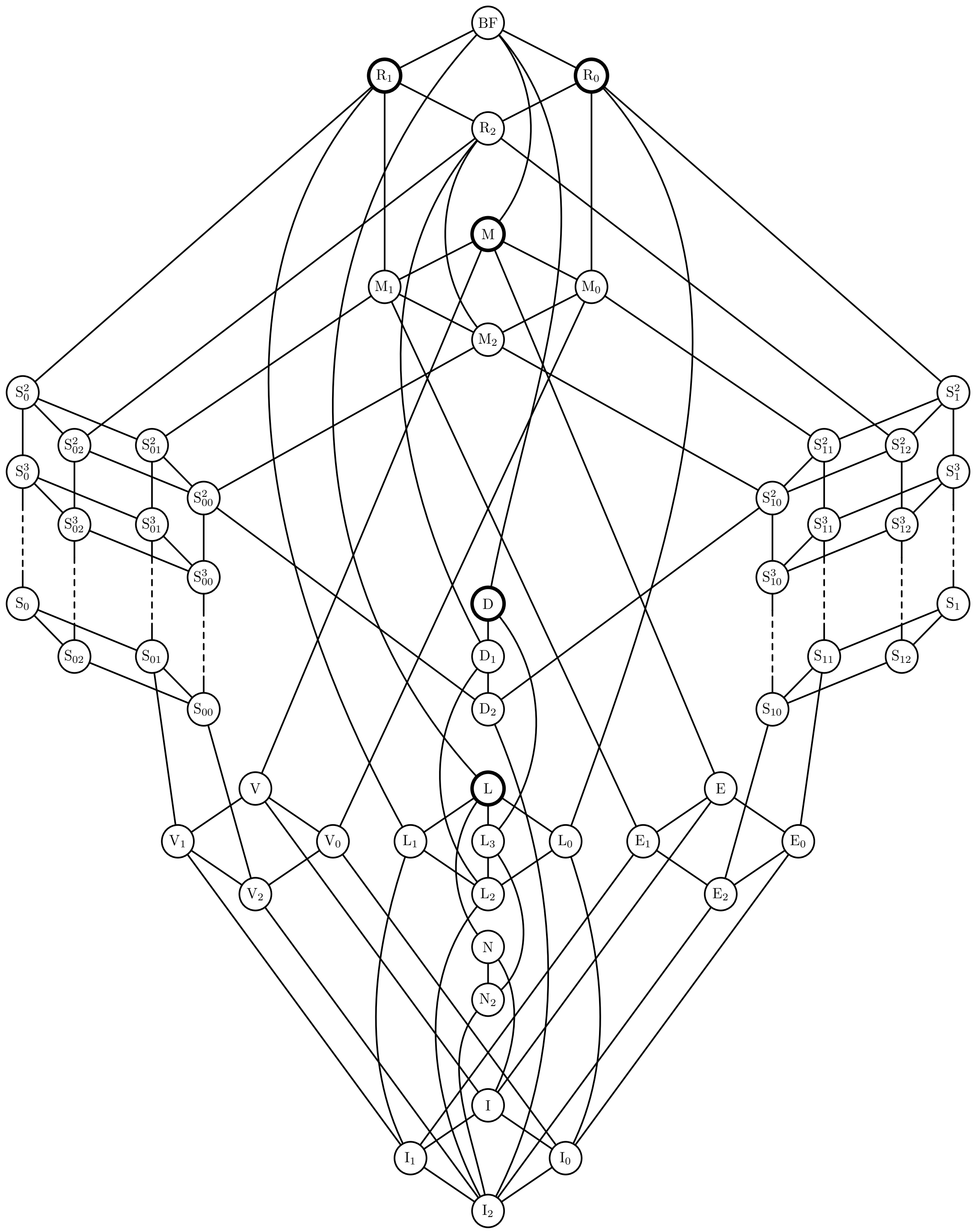

Figure 1: Graph of all closed classes of Boolean functions

The following lemma is taken from [Rei01]:

Lemma 3

1. *Let g be a Boolean function such that* $g(x_1, \ldots, x_n) = f(f_1(x_1^1, \ldots, x_{m_1}^1), \ldots, f_l(x_1^l, \ldots, x_{m_l}^l))$*, For the dual function of g it holds that* $\mathrm{dual}(g) = \mathrm{dual}(f)(\mathrm{dual}(f_1), \ldots, \mathrm{dual}(f_l))$.

2. *If B is a finite set of Boolean functions, then* $[\mathrm{dual}(B)] = \mathrm{dual}([B])$.

3. *Every closed class is dual to its mirror class (via the symmetry axis in the lattice).*

4. *Let A be a closed class. Then* $\mathrm{dual}(A)$ *is a closed class, too.*

Lemma 4 *(Duality principle) Let $A, B \in \mathcal{P}$ such that* $\mathrm{dual}(\mathrm{base}(B)) = \mathrm{base}(\mathrm{dual}(B))$. *Then* $\mathcal{M}(A \twoheadleftarrow B) \equiv_m^p \mathcal{M}(\mathrm{dual}(A) \twoheadleftarrow \mathrm{dual}(B))$.

Proof Let f be a B-formula. Let $g :\equiv \mathrm{dual}(f)$. g can be computed easily in polynomial time, since with Lemma 3 we know we just have to exchange every gate in the formula f with a gate for the dual function. Since $\mathrm{dual}(\mathrm{base}(B)) = \mathrm{base}(\mathrm{dual}(B))$, the result is a $\mathrm{dual}(B)$-formula.

Now we see $f \in \mathcal{M}(A) \Leftrightarrow \mathrm{dual}(g) \in \mathcal{M}(A) \Leftrightarrow g \in \mathcal{M}(\mathrm{dual}(A))$ holds. Thus, $\mathcal{M}(A \twoheadleftarrow B) \leq_m^p \mathcal{M}(\mathrm{dual}(A) \twoheadleftarrow \mathrm{dual}(B))$. For symmetry reasons, $\mathcal{M}(\mathrm{dual}(A) \twoheadleftarrow \mathrm{dual}(B)) \leq_m^p \mathcal{M}(A \twoheadleftarrow B)$ holds as well (since with $\mathrm{dual}(\mathrm{dual}(f)) = f$, we have $\mathrm{dual}(\mathrm{base}(B)) = \mathrm{base}(B)$). □

This lemma reduces the number of combinations A, B for which we have to examine $\mathcal{M}(A \twoheadleftarrow B)$: Since for any class from Post's lattice which is not self-dual (that means a class B such that $\mathrm{dual}(B) \neq B$), the premise of Lemma 4 is met, the lemma implies that we only have to consider membership problems for B-formulas, where B is on one fixed side of the lattice. In this thesis, we will analyse formulas from classes of the left side of Post's lattice. Moreover, for a self-dual class B on the symmetry axis of the lattice for which $\mathrm{base}(B) = \mathrm{dual}(\mathrm{base}(B))$ holds, we only have to consider $\mathcal{M}(A \twoheadleftarrow B)$ for classes A on the left side of the lattice as well. This holds for any of the self-dual classes except for R_2 (the dual function of $\vee$ is $\wedge$, and $\wedge$ is not an element of $\mathrm{base}(\mathrm{R}_2)$).

Proposition 5 *Let B, A_1, A_2 be classes from $\mathcal{P}$, $\mathcal{K} \in \{\mathrm{P}, \mathrm{coNP}\}$ (or any complexity class closed under intersection and unification) such that $\mathcal{M}(A_1 \twoheadleftarrow B), \mathcal{M}(A_2 \twoheadleftarrow B) \in \mathcal{K}$. Then $\mathcal{M}(A_1 \cap A_2 \twoheadleftarrow B), \mathcal{M}(A_1 \cup A_2 \twoheadleftarrow B) \in \mathcal{K}$ (Note $A_1 \cup A_2$ is not necessarily a class from Post's lattice, but $A_1 \cap A_2$ is).*

To show some membership problem $\mathcal{M}(A \twoheadleftarrow B)$ is coNP-complete, formally we have to construct some B-formula in many cases. The following lemma enables us to express the reduction function over any base, as long as the function can be expressed with a formula of a certain class. This also helps us to give a single reduction for membership problems $\mathcal{M}(A \twoheadleftarrow B_1)$ and $\mathcal{M}(A \twoheadleftarrow B_2)$ with $B_1 \subseteq B_2$. We cannot convert any given B_1-formula into an equivalent B_2-formula easily, but with this lemma we can do this in the most important cases.

Lemma 6 *Let B be some class from Post's lattice, f a fixed function from B, $g_1, \dots, g_n$ B-formulas. Then there exists a B-formula h such that $h = f(g_1, \dots, g_n)$, and there is a polynomial-time algorithm that calculates h when given $g_1, \dots, g_n$. h is of polynomial length in $|g_1| + \dots + |g_n|$.*

Proof Since $f \in B$, there exists a fixed B-formula f' such that $f'(\alpha_1, \dots, \alpha_n) = f(\alpha_1, \dots, \alpha_n)$ for all $\alpha_1, \dots, \alpha_n \in \{0, 1\}$. The algorithm only needs to replace every x_i-gate with the formula g_i to obtain the formula h. Since f' is a B-formula, and all g_i are B-formulas, the result h is a B-formula as well. Obviously, $|h| \leq |f'| \cdot max(|g_1|, \dots, |g_n|)$ holds, and the algorithm runs in polynomial time. □

1.2 Known complexity results

Here we will list problems known to be coNP-complete from [ReiWag99] and [Rei01]. These will be used in our reductions.

Definition Let B be a set of Boolean functions. Then

$$\mathrm{EQ}^F(B) := \{(g, h) \mid g \text{ and } h \text{ are } B\text{-formulas and } g = h\}$$

is the equivalence problem for B-formulas.

Definition Let B be a set of Boolean functions. Then

$$\mathrm{TAUT}^F(B) := \{f \mid f \text{ is a } B\text{-formula and } f = 1 \text{ holds}\}$$

is the tautology problem for B-formulas.

The following theorems are from [Rei01] and [ReiWag99]:

Theorem 7 *Let B be a finite set of Boolean functions,* $\mathrm{S}_{10} \subseteq [B]$ *or* $\mathrm{S}_{00} \subseteq [B]$ *or* $\mathrm{D}_2 \subseteq [B]$*. Then $EQ^F(B)$ is coNP-complete.*

Theorem 8 *Let B be a finite set of Boolean functions,* $\mathrm{S}_0 \subseteq [B]$*. Then* $\mathrm{TAUT}^F(B)$ *is coNP-complete.*

2 Upper bounds

In this section, we will show upper bounds for our membership problems. In general, $\mathcal{M}(A \twoheadleftarrow B)$ is always in coNP, as we will see in the next theorem. We will also show most membership problems for M-formulas are easy to solve, and all membership problems for L-formulas are solvable in polynomial time.

Theorem 9 *Let $A, B \in \mathcal{P}$. Then* $\mathcal{M}_C(A \twoheadleftarrow B) \in \mathrm{coNP}$.

Proof We show the complement of $\mathcal{M}(A \twoheadleftarrow B)$ is in NP: To show $C \notin \mathcal{M}(A \twoheadleftarrow B)$, for a given circuit C, it is sufficient to give a counter-example of small size (note that for any class B and any B-circuit C, the value of $f_C(\alpha_1, \ldots, \alpha_n)$ can be computed in polynomial time):

I_2 For each $i \in \{1, \ldots, n\}$, give a tuples $(\alpha_1^i, \ldots, \alpha_n^i)$ such that $C(\alpha_1^i, \ldots, \alpha_n^i) \neq \alpha_i^i$

S_0^k Give k input tuples which evaluate to 0 but do not have a common 0

S_0 Observe it is enough to give n input tuples to show $C \notin \mathcal{M}(\mathrm{S}_0)$: If $C \notin \mathcal{M}(\mathrm{S}_0)$, then there exists some finite set $A \subseteq \{0,1\}^n$ such that for all $\overrightarrow{x} \in A$, $C(\overrightarrow{x}) = 0$ but the elements of A do not have a common 0. Thus it is sufficient to choose a n-element subset A' of A such that for every position $i \in \{1, \ldots, n\}$ there is some $\overrightarrow{x} \in A'$ such that the i-th component of $\overrightarrow{x}$ is 1.

M A counter-example of two input tuples exists if the function is not monotonic: In this case we have $\overrightarrow{x_1}$ and $\overrightarrow{x_2}$ such that $\overrightarrow{x_1} \leq \overrightarrow{x_2}$ and $C(\overrightarrow{x_1}) > C(\overrightarrow{x_2})$.

$\mathrm{R}_0, \mathrm{R}_1$ This problem even is in P: To test whether C is in R_0, just verify that $C(0, \ldots, 0) = 0$ holds. For R_1, check whether $C(1, \ldots, 1) = 1$.

D It is sufficient to give one tuple $\overrightarrow{\alpha}$ such that $C(\overrightarrow{\alpha}) \neq \mathrm{dual}(C)(\overrightarrow{\alpha})$.

L For one variable x_i, give a proof that it is a relevant variable (this can be achieved with two tuples), then give two tuples which show changing the assignment of x_i does not change the value of C.

N_2 For each $i \in \{1, \ldots, n\}$, give a tuple $(\alpha_1^i, \ldots, \alpha_n^i)$ such that $C(\alpha_1^i, \ldots, \alpha_n^i) = \alpha_i^i$. Further, give counter-examples to prove $C \notin I_2 \subseteq N_2$.

V_2 Let $W := \{i \mid 1 \leq i \leq n \; C(x_1 = 0, \ldots, x_{i-1} = 0, x_i = 1, x_{i+1} = 0, \ldots, x_n = 0) = 1\}$. Observe we have $C \in \mathcal{M}(V_2)$ if and only if $C = \bigvee_{i \in W} x_i$: Obviously, if $C = \bigvee_{i \in W} x_i$, then C can be written over the basis $\{\vee\}$, and thus $C \in \mathcal{M}(V_2)$. Now assume $C \in \mathcal{M}(V_2)$. Then $C = \bigvee_{i \in W'} x_i$ for some set $W' \subseteq \{1, \ldots, n\}$ holds. Obviously, $W \subseteq W'$, since for any $i \in W$, $x_i \to C$ holds. On the other hand, for any $i \in W'$, we have $C(x_1 = 0, \ldots, x_{i-1} = 0, x_1 = 1, x_{i+1} = 0, \ldots, x_n = 0) = 1$ holds, and therefore $i \in W$. Thus, $W = W'$ holds, and so it is sufficient to give one counter-example for the equivalence $C = \bigvee_{i \in W} x_i$ to show that $C \notin V_2$.

Obviously, these counter-examples can be verified in polynomial time by an algorithm. For classes of the form $A_1 \cap A_2$ or $A_1 \cup A_2$, the theorem follows with proposition 5. For the class I_1, we give a tuple for which C does not evaluate to the constant 1 in addition to the examples for proving C is not an identify. For the classes on the right side of Post's lattice, the theorem follows with Lemma 4. □

2.1 Subclasses of L

In this section we show that for a circuit describing a linear function, all membership problems in Post's lattice are easy to solve. The reason for this is that it is easy to determine the set of relevant variables for a linear function - knowing these, we have all the information we need, since this leaves only 2 possibilities for the linear function in question. Note we only need to show $\mathcal{M}_C(A \twoheadleftarrow L') \in \mathrm{P}$ for all pairs A, L' such that $A \subseteq L' \subsetneq \mathrm{L}$, due to Proposition 1.

Proposition 10 *Let C be a Boolean circuit, $C \in \mathcal{M}(\mathrm{L})$. Then there exists a* L*-formula f, such that $f_C = f_f$, $|f|$ is linear with regard to $|C|$. There exists an algorithm which, given C, calculates f in time $O(|C|^{O(1)})$.*

Proof It is easy to see x_i is a relevant variable for C if and only if

$$C(x_1 = 0, \ldots, x_{i-1} = 0, x_i = 0, x_{i+1} = 0, \ldots, x_n = 0) \neq$$

$$(x_1 = 0, \ldots, x_{i-1} = 0, x_i = 1, x_{i+1} = 0, \ldots, x_n = 0).$$

So it is easy to determine the set of relevant variables for C. Now, the formula f' is of the form $c \oplus x_{i_1} \oplus \cdots \oplus x_{i_k}$ with $x_{i_1}, \ldots, x_{i_k}$ being the pairwise different relevant variables for C, and $c = C(0, \ldots, 0)$. □

Theorem 11 *Let $A \subseteq L' \subseteq \mathrm{L}$ be classes from $\mathcal{P}$. Then $\mathcal{M}_C(A \twoheadleftarrow L') \in \mathrm{P}$.*

Proof Let C be a L'-circuit, and f the corresponding L-formula constructed in Proposition 10. Obviously, $f \in \mathcal{M}(A) \Leftrightarrow C \in \mathcal{M}_C(A \twoheadleftarrow L')$ holds, since they describe the same function.

To test if $f \in \mathcal{M}(\mathrm{L}_0), \mathcal{M}(\mathrm{L}_1)$ or $\mathcal{M}(\mathrm{L}_2)$, we just have to calculate $f(0, \ldots, 0)$ and $f(1, \ldots, 1)$. We show $f \in \mathcal{M}(\mathrm{L}_3)$ if and only if the number of relevant variables in f is odd:

Let $f \in \mathcal{M}(L_3)$. Assume the number of relevant variables is even, let the variables be $x_1, \ldots, x_{2k}$. Then we have

$$\begin{array}{rcccl} f(x_1 = 0, \ldots, x_{2k} = 0) & = & c \oplus 0 \oplus \cdots \oplus 0 & = & c \\ \neg f(x_1 = 1, \ldots, x_{2k} = 1) & = & \neg(c \oplus \underbrace{1 \oplus 1 \oplus \cdots \oplus 1}_{=0,\text{since } 2k \text{ even.}}) & = & \neg c. \end{array}$$

Thus, f is not self-dual, and so $f \notin \mathcal{M}(\mathrm{L}_3)$.

Now, let the relevant variables for f be $x_1, \ldots, x_{2k+1}$ for some $k \in \mathbb{N}$. Let $\alpha_1, \ldots, \alpha_{2k+1} \in \{0, 1\}$. Then we have

$$\begin{aligned} f(x_1 = \alpha_1, \ldots, x_{2k+1} = \alpha_{2k+1}) &= c \oplus \overline{\alpha_1} \oplus 1 \oplus \overline{\alpha_2} \oplus 1 \oplus \cdots \oplus \overline{\alpha_{2k+1}} \oplus 1 \\ &= c \oplus \overline{\alpha_1} \oplus \overline{\alpha_2} \oplus \cdots \oplus \overline{\alpha_{2k+1}} \oplus \underbrace{1 \oplus 1 \cdots \oplus 1}_{=1(2k+1 \text{ odd})} \\ &= \neg(c \oplus \overline{\alpha_1} \oplus \overline{\alpha_2} \oplus \cdots \oplus \overline{\alpha_{2k+1}} \\ &= \neg f(x_1 = \overline{\alpha_1}, \ldots, x_{2k+1} = \overline{\alpha_{2k+1}}). \end{aligned}$$

Thus, $f = \mathrm{dual}(f)$, and since $f \in \mathcal{M}(\mathrm{L})$, we have $f \in \mathcal{M}(\mathrm{L}_3)$. Since counting the relevant variables in f can be done in polynomial time, we have $\mathcal{M}_C(\mathrm{L}_3 \twoheadleftarrow L') \in P$.

To see whether $f \in \mathcal{M}(\mathrm{N})$ or $f \in \mathcal{M}(\mathrm{I})$, observe this is true if and only if $f \equiv 1 \oplus x_i$ or $f \equiv 0 \oplus x_i$ for some i, which is trivial to verify. Thus, $\mathcal{M}_C(\mathrm{N} \twoheadleftarrow L'), \mathcal{M}_C(\mathrm{I} \twoheadleftarrow L') \in P$. With proposition 5, this implies $\mathcal{M}_C(A \twoheadleftarrow L') \in P$ for $A \in \{\mathrm{N}_2, \mathrm{I}_0, \mathrm{I}_1, \mathrm{I}_2\}$. Thus, we have $\mathcal{M}_C(A \twoheadleftarrow L') \in \mathrm{P}$ for all cases. □

2.2 Subclasses of M

For circuits describing monotonic functions, a lot of membership problems are easy to solve as well, since with calculating function values for two input tuples, we can get a lot of information about other input tuples without the need to calculate them directly. The proof to the following theorem is based on the proof for a similar proposition in [Böh].

Theorem 12 *Let $M' \subseteq \mathrm{M}$ and A from $\mathcal{P}$ such that $A \subseteq \mathrm{S}_{01}$, $A \subseteq \mathrm{S}_{11}$, $A \subseteq \mathrm{V}$ or $A \subseteq \mathrm{E}$. Then $\mathcal{M}_C(A \twoheadleftarrow M') \in \mathrm{P}$.*

Proof Let C be a M'-circuit. Note the only properties we use in this proof are that C describes a monotonic function, and that f_C is computable in polynomial time.

Case 1 $A = \mathrm{I}_2$. Observe for an input variable x_i, $C = x_i$ holds if and only if

$$\begin{aligned} 0 &= C(x_1 = 0, \ldots, x_{i-1} = 0, x_i = 0, x_{i+1} = 0, \ldots, x_n = 0) \\ &= C(x_1 = 1, \ldots, x_{i-1} = 1, x_i = 0, x_{i+1} = 1, \ldots, x_n = 1) \text{ and} \\ 1 &= C(x_1 = 0, \ldots, x_{i-1} = 0, x_i = 1, x_{i+1} = 0, \ldots, x_n = 0) \\ &= C(x_1 = 1, \ldots, x_{i-1} = 1, x_i = 1, x_{i+1} = 1, \ldots, x_n = 1). \end{aligned}$$

Thus, for every input variable, at most 4 values of f_C must be calculated.

Case 2 $A = \mathrm{V}_2$. Let $W := \{i | 1 \leq i \leq n, C(x_i = 0, \ldots, x_{i-1} = 0, x_i = 1, x_{i+1} = 0, \ldots, x_n = 0) = 1\}$. Since f_C is monotonic, $x_i \rightarrow C$ holds for all $i \in W$. If $W = \emptyset$, we know $C \notin \mathcal{M}(V_2)$. If $W \neq \emptyset$, we know $C \in \mathcal{M}(V_2)$ if and only if $C = \bigvee_{i \in W} x_i$. Without loss of generality, let $W = \{1, \ldots, k\}$ (rename variables if necessary). Observe we have $C \in \mathcal{M}(\mathrm{V}_2)$ if and only if $C(x_1 = 0, \ldots, x_k = 0, x_{k+1} = 1, \ldots, x_n = 1) = 0$, since in this case we have $C \rightarrow x_1 \vee \cdots \vee x_k$.

Case 3 $A = \mathrm{S}_{01}$. For $C \in \mathcal{M}(\mathrm{M})$, we have

$$\begin{aligned} C \in \mathcal{M}(\mathrm{S}_{01}) \quad &\Leftrightarrow \quad C \in \mathcal{M}(\mathrm{S}_0) \\ &\Leftrightarrow \quad \exists i \text{ such that } C(\alpha_1, \ldots, \alpha_n) = 0 \Rightarrow \alpha_i = 0 \\ &\Leftrightarrow \quad \exists i \text{ such that } \alpha_i = 1 \Rightarrow C(\alpha_1, \ldots, \alpha_n) = 1 \\ &\Leftrightarrow \quad \exists i \text{ such that} \\ &\qquad C(x_1 = 0, \ldots, x_{i-1} = 0, x_i = 1, x_{i+1} = 0, \ldots, x_n = 0) = 1 \\ &\qquad \text{(since } f_C \text{ is monotonic)} \end{aligned}$$

To verify this last condition, we just need to compute n values of f_C, which can be done in polynomial time.

Case 4 $A = \mathrm{E}_2$ or $A = \mathrm{S}_{11}$: This follows from the cases V_2 and S_{01}: We have $C \in \mathcal{M}(\mathrm{E}_2) \Leftrightarrow \mathrm{dual}(C) \in \mathcal{M}(\mathrm{V}_2)$ and $C \in \mathcal{M}(\mathrm{S}_{11}) \Leftrightarrow \mathrm{dual}(C) \in \mathcal{M}(\mathrm{S}_{01})$, both cases can be tested in polynomial time, since $\mathrm{dual}(C)$ is a monotonic circuit as well.

The remaining classes $\mathrm{I}_0, \mathrm{I}_1, \mathrm{I}, \mathrm{V}_0, \mathrm{V}_1, \mathrm{E}_0, \mathrm{E}_1, \mathrm{V}, \mathrm{S}_{00}$ and S_{10} follow from the above with Proposition 5 and Theorem 2. □

3 R_1-and R_2-formulas

We will now examine R_1-and R_2-formulas. The information a certain Boolean function is from one of these classes does not give us much information - we just know the value of the function for one or two input tuples. We will show in this section the knowledge of the representation of a Boolean function as a R_1- or R_2-formula does not give us a significant advantage either, membership problems for these formulas are not easier than those for general Boolean formulas. Note the results for R_0 formulas follow with Lemma 4.

For R_2-formulas, we can basically prove coNP-completeness for all relevant membership problems using only one reduction. However, since the base for R_2 does not meet the condition for Lemma 4, this is the one case where we actually have to look at both sides of Post's lattice.

Lemma 13 *Let $A \in \mathcal{P}$ such that $A \subseteq \mathrm{S}_0^2$ or $A \subseteq \mathrm{M}$ or $A \subseteq \mathrm{D}$, $B \in \{\mathrm{R}_1, \mathrm{R}_2\}$. Then $\mathcal{M}(A \twoheadleftarrow B)$ is coNP-complete.*

Proof We show $EQ^F(B) \leq_m^p \mathcal{M}(A \twoheadleftarrow B)$. The proposition follows with Theorem 7. Let f_1, f_2 be B-formulas, and h a B-formula such that $h \notin \mathcal{M}(A)$. Let y be a new variable, and

$$g :\equiv \begin{cases} y \wedge (f_1 \leftrightarrow f_2), & \text{if } f_1(0,\ldots,0) = f_2(0,\ldots,0) \\ h, & \text{otherwise.} \end{cases}$$

For $B = \mathrm{R}_2$, g is a B-formula, with help of Lemma 6, we can construct an equivalent R_1-formula, since $x \wedge (y \leftrightarrow z) \in \mathcal{M}(R_2)$. We claim $f_1 = f_2 \Leftrightarrow g \in \mathcal{M}(A)$.

Let $f_1 = f_2$. Then $g = y \wedge (1) = y \in \mathcal{M}(\mathrm{I}_2) \subseteq \mathcal{M}(A)$.

Let $f_1 \neq f_2$.

Case 1 Let $f_1(0,\ldots,0) \neq f_2(0,\ldots,0)$. Then $g \equiv h \notin \mathcal{M}(A)$.

Case 2 Let $f_1(0,\dots,0) = f_2(0,\dots,0)$. Let $\alpha_1,\dots,\alpha_n \in \{0,1\}$ such that, without loss of generality,

$$f_1(\alpha_1,\dots,\alpha_n) = 0$$
$$f_2(\alpha_1,\dots,\alpha_n) = 1.$$

Since $f_1, f_2 \in \mathcal{M}(\mathrm{R}_1)$, we know $f_1(1,\dots,1) = f_2(1,\dots,1) = 1$. Thus,

$$g(x_1 = 1,\dots,x_n = 1, y = 0) = 0 \wedge (1 \leftrightarrow 1) = 0$$
$$g(x_1 = \alpha_1,\dots,x_n = \alpha_n, y = 1) = 1 \wedge (0 \leftrightarrow 1) = 0$$

but the two input tuples do not have a common 0. Thus, g is not 0-separating of degree 2, $g \notin \mathcal{M}(\mathrm{S}_0^2)$. Further, we see, since $f_1(0,\dots,0) = f_2(0,\dots,0)$:

$$g(x_1 = 0,\dots,x_n = 0, y = 1) = 1 \wedge (0 \leftrightarrow 0) = 1$$
$$g(x_1 = \alpha_1,\dots,x_n = \alpha_n, y = 1) = 1 \wedge (0 \leftrightarrow 1) = 0$$

and so, $g \notin \mathcal{M}(\mathrm{M})$. Last, we know

$$\neg g(x_1 = \overline{\alpha_1},\dots,x_n = \overline{\alpha_n}, y = 0) = \neg(0 \wedge (g_1 \leftrightarrow g_2)) = \neg 0 = 1$$

so g is not self-dual, $g \notin \mathcal{M}(\mathrm{D})$. Thus, we know $g \notin \mathcal{M}(A)$.

□

To show the coNP-completeness for A-membership problems with $A \subseteq \mathrm{S}_1^2$, we can just "dualize" the proof of the first part of the preceding lemma to handle the right side of the lattice as well:

Lemma 14 *Let $A \in \mathcal{P}$ such that $A \subseteq \mathrm{S}_1^2$, $B \in \{\mathrm{R}_2, \mathrm{R}_1\}$ Then $\mathcal{M}(A \twoheadleftarrow B)$ is coNP-complete.*

Proof We show $EQ^F(B) \leq_m^p \mathcal{M}(A \twoheadleftarrow B)$. The proposition follows with Theorem 7. Let f_1, f_2 be B-formulas. With Lemma 6, construct a B-formula $g := y \vee (f_1 \neq f_2)$ (note $y \vee (x \neq z \in \mathcal{M}(\mathrm{R}_2) \subseteq \mathcal{M}(B))$. We claim $f_1 = f_2 \Leftrightarrow g \in \mathcal{M}(A)$.

Let $f_1 = f_2$. Then $g = y \vee (f_1 \neq f_2) = y \vee 0 = y \in \mathcal{M}(I_2) \subseteq \mathcal{M}(A)$.

Let $f_1 \neq f_2$. Let $\alpha_1, \dots, \alpha_n \in \{0, 1\}$ such that, without loss of generality,

$$f_1(\alpha_1, \dots, \alpha_n) = 0$$

$$f_2(\alpha_1, \dots, \alpha_n) = 1.$$

We see

$$g(x_1 = 0, \dots, x_n = 0, y = 1) = 1 \vee (f_1 \neq f_2) = 1$$

$$g(x_1 = \alpha_1, \dots, x_n = \alpha_n, y = 0) = 0 \vee (0 \neq 1) = 1$$

but the two input tuples do not have a common 1. Thus, g is not 1-separating of degree 2, $g \notin \mathcal{M}(\mathrm{S}_1^2) \supseteq \mathcal{M}(A)$. □

The only cases left are membership problems for classes below L. Since $\mathrm{R}_2 \cap \mathrm{L} = \mathrm{I}_2$, and this case was shown to be coNP-complete in the previous lemma, we only have to look at R_1-formulas here:

Lemma 15 *Let $A \in \mathcal{P}$ such that $A \subseteq \mathrm{L}$. Then $\mathcal{M}(A \twoheadleftarrow \mathrm{R}_1)$ is coNP-complete.*

Proof We show $\mathrm{TAUT}^F(\mathrm{R}_1) \leq_m^p \mathcal{M}(A \twoheadleftarrow \mathrm{R}_1)$. The proposition follows with Theorem 8. Let f be any R_1-formula. Let $g :\equiv y \vee (f \leftrightarrow y)$ for some new variable y. We claim $f \in \mathrm{TAUT} \Leftrightarrow g \in \mathcal{M}(A)$.

Let $f \in \mathrm{TAUT}$. Then $g = y \vee (1 \leftrightarrow y) = y \in \mathcal{M}(\mathrm{I}_2) \subseteq \mathcal{M}(A)$.

Let $f \notin \mathrm{TAUT}$. Let $\alpha_1, \dots, \alpha_n$ such that $f(\alpha_1, \dots, \alpha_n) = 0$. Since $f \in \mathcal{M}(\mathrm{R}_1)$, we know $f(1, \dots, 1) = 1$. Thus,

$$g(x_1 = 1, \dots, x_n = 1, y = 0) = 0 \vee (1 \leftrightarrow 0) = 0$$

$$g(x_1 = 1, \dots, x_n = 1, y = 1) = 1 \vee (1 \leftrightarrow 1) = 1$$

therefore we know y is a relevant variable for g. We see

$$g(x_1 = \alpha_1, \dots, x_n = \alpha_n, y = 0) = 0 \vee (0 \leftrightarrow 0) = 1$$

$g(x_1 = \alpha_1, \ldots, x_n = \alpha_n, y = 1) = 1 \vee (1 \leftrightarrow 0) = 1$

Thus, the changing of the value for y does not change the value of the formula g, although y is a relevant variable for g. Therefore, $g \notin \mathcal{M}(\mathrm{L})$. □

4 0-separating formulas

4.1 Basic properties

In this section, we examine classes of formulas which are 0-separating of some degree $k \in \mathbb{N}$. The bases for these classes contain the dual(h_k) function, so we will start our discussion of these formulas with a look at this function.

Lemma 16 *Let $k \in \mathbb{N}$ and $\alpha_1, \ldots, \alpha_{k+1} \in \{0, 1\}$. Then $(\mathrm{dual}(h_k))(\alpha_1, \ldots, \alpha_{k+1}) = 1$ if and only if there exist i, j such that $1 \leq i, j \leq k+1$, $i \neq j$ and $\alpha_i = \alpha_j = 1$.*

Proof

$(\mathrm{dual}(h_k))(\alpha_1, \ldots, \alpha_{k+1}) = 1$

$\Leftrightarrow \neg h_k(\overline{\alpha_1}, \ldots, \overline{\alpha_{k+1}}) = 1$

$\Leftrightarrow h_k(\overline{\alpha_1}, \ldots, \overline{\alpha_{k+1}}) = 0$

$$\Leftrightarrow \bigvee_{i=1}^{k+1} \overline{\alpha_1} \cdot \cdots \cdot \overline{\alpha_{i-1}} \cdot \overline{\alpha_{i+1}} \ldots \overline{\alpha_{k+1}} = 0$$

$\Leftrightarrow$ For any subset A of $\{1, \ldots, k+1\}$ with $|A| = k$ holds: $\exists j \in A$ with $\overline{\alpha_j} = 0$

$\Leftrightarrow$ For any subset A of $\{1, \ldots, k+1\}$ with $|A| = k$ holds: $\exists j \in A$ with $\alpha_j = 1$

Let $(\mathrm{dual}(h_k))(\alpha_1, \ldots, \alpha_{k+1}) = 1$. Obviously, from the above follows there is some $i \in \{1, \ldots, k+1\}$ such that $\alpha_i = 1$. Assume $\alpha_j = 0$ for all $j \neq i$. Then let $A := \{1, \ldots, k+1\} \setminus \{i\}$. $|A| = k$, but for all $j \in A$, $\alpha_j = 0$ holds, which is a contradiction to the above.

Now, let $i \neq j$ such that $\alpha_i = \alpha_j = 1$. Then obviously, every subset A of $\{1, \ldots, k+1\}$ with $|A| = k$ contains i or j. Thus, $(\mathrm{dual}(h_k))(\alpha_1, \ldots, \alpha_n) = 1$. □

Remark: A set $A \subseteq \{0,1\}^n$ is 0-separating if and only if $\bigvee\limits_{\overrightarrow{\alpha} \in A} \overrightarrow{\alpha} \neq \overrightarrow{1}$.

The following lemma is trivial, but useful:

Lemma 17 *Let f, g Boolean functions, $m \in \mathbb{N}$ such that $f \leq g$. Then*

1. $f \in \mathrm{S}_0^m \Rightarrow g \in \mathrm{S}_0^m$.
2. $f \in \mathrm{S}_0 \Rightarrow g \in \mathrm{S}_0$.

Proof

1. Let $\overrightarrow{x_1}, \ldots, \overrightarrow{x_m} \in \{0,1\}^n$ such that $g(\overrightarrow{x_i}) = 0$ for all $i \in \{1, \ldots, m\}$. Then $f(\overrightarrow{x_i}) = 0$, since $f \leq g$. Thus, $\overrightarrow{x_1} \vee \cdots \vee \overrightarrow{x_m} \neq \overrightarrow{1}$, and $g \in \mathrm{S}_0^m$ holds.
2. This follows directly from part 1, since $\mathrm{S}_0 = \bigcap\limits_{m \geq 2} \mathrm{S}_0^m$.

□

The following proposition is needed in some reductions:

Lemma 18 *Let $f'(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \wedge (x_1 \vee \cdots \vee x_n)$ and $k \in \mathbb{N}, k \geq 2$.*

1. $f \in \mathrm{S}_0^k \Leftrightarrow f' \in \mathrm{S}_0^k$.
2. $f \in \mathrm{S}_0 \Leftrightarrow f' \in \mathrm{S}_0$.

Proof

1. Let $f' \in \mathrm{S}_0^k$. Since $f' \leq f$, the proposition follows with Lemma 17.
   Let $f' \notin \mathrm{S}_0^k$. Let $\overrightarrow{\alpha_1}, \ldots, \overrightarrow{\alpha_k}$ such that $f'(\overrightarrow{\alpha_1}) = f'(\overrightarrow{\alpha_2}) = \ldots = f'(\overrightarrow{\alpha_k}) = 0$ and $\overrightarrow{\alpha_1} \vee \cdots \vee \overrightarrow{\alpha_k} = \overrightarrow{1}$.
   Let $B := \{\overrightarrow{\alpha_1}, \ldots, \overrightarrow{\alpha_k}\} \backslash \{(0, \ldots, 0)\}$. Note $1 \leq |B| \leq k$ and $\bigvee_{\overrightarrow{\alpha} \in B} \overrightarrow{\alpha} = \overrightarrow{\alpha_1} \vee \cdots \vee \overrightarrow{\alpha_k} = \overrightarrow{1}$. For all $\overrightarrow{\beta} \in B$ holds $0 = f'(\overrightarrow{\beta}) = f(\beta_1, \ldots, \beta_n) \wedge (\beta_1 \vee \cdots \vee \beta_n) = f(\beta_1, \ldots, \beta_n)$. Thus, $f \notin \mathrm{S}_0^{|B|} \supseteq S_0^k$.
2. This follows directly from part 1, since $\mathrm{S}_0 = \bigcap\limits_{m \geq 2} S_0^m$.

□

4.2 $\mathrm{S}_0, \mathrm{S}_{02}, \mathrm{S}_0^k$ and S_{02}^k-formulas

In this section we will discuss membership problems for formulas representing 0-separating functions which are not necessarily monotonic.

Lemma 19 *Let $B \in \mathcal{P}$, $\mathrm{S}_{02} \subseteq B \subseteq \mathrm{R}_1$ and $A \subseteq \mathrm{M}$. Then $\mathcal{M}(A \twoheadleftarrow B)$ is coNP-complete.*

Proof We show $EQ^F(B) \leq_m^p \mathcal{M}(A \twoheadleftarrow B)$. The result follows from Theorem 7. Let f_1, f_2 be B-formulas. Let $g :\equiv (y \vee (f_1 \oplus f_2))$. Note $y \vee (x_1 \oplus x_2)$ is a function from $S_{02} \subseteq B$, and therefore, a B-formula equivalent to g exists and is polynomial-time constructable due to Lemma 6.

We claim $f_1 = f_2 \Leftrightarrow g \in \mathcal{M}(A)$.

Let $f_1 = f_2$. Then $g = (y \vee (f_1 \oplus f_1)) = y \in \mathcal{M}(\mathrm{I}_2) \subseteq \mathcal{M}(A)$.

Let $(\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$ such that $\beta := f_1(\alpha_1, \ldots, \alpha_n) \neq f_2(\alpha_1, \ldots, \alpha_n) =: \gamma$. Then we have (since $f_1, f_2 \in \mathcal{M}(B) \subseteq \mathcal{M}(\mathrm{R}_1)$):

$$g(x_1 = \alpha_1, \ldots, x_n = \alpha_n, y = 0) = 0 \vee (\beta \oplus \gamma) = 1$$

$$g(x_1 = 1, \ldots, x_n = 1, y = 0) = 0 \vee (1 \oplus 1) = 0$$

thus, $g \notin \mathcal{M}(\mathrm{M}) \supseteq \mathcal{M}(A)$. □

Lemma 20 *Let $A \in \mathcal{P}$ such that $\mathrm{V}_2 \subseteq A \subseteq \mathrm{S}_0^k$. Then $\mathcal{M}(A \twoheadleftarrow \mathrm{S}_0^m)$ is* coNP*-complete for $k > m \geq 2$.*

Proof We show $\mathrm{TAUT}^F(\mathrm{S}_0^m) \leq_m^p \mathcal{M}(A \twoheadleftarrow \mathrm{S}_0^m)$. The lemma follows with Theorem 8. Let f any S_0^m-formula. Let $g :\equiv \mathrm{dual}(h_m)(f, y_1, \ldots, y_m)$ for new variables $y_1, \ldots, y_m$. We claim $f \in \mathrm{TAUT} \Leftrightarrow g \in \mathcal{M}(A)$.

Let $f \in \mathrm{TAUT}$. Then $g \equiv (\mathrm{dual}(h_n))(1, y_1, \ldots, y_m) = y_1 \vee \cdots \vee y_m \in \mathcal{M}(V_2) \subseteq \mathcal{M}(A)$.

Let $f \notin \mathrm{TAUT}$. Let $\alpha_1, \ldots, \alpha_n$ such that $f(\alpha_1, \ldots, \alpha_n) = 0$. Then we have (with $g_n := \mathrm{dual}(h_n)$):

$$g(\overrightarrow{x}{=}\overrightarrow{\alpha}, y_1{=}1, y_2{=}0, y_3{=}0, \ldots, y_{m-1}{=}0, y_m{=}0) = g_n(0, 1, 0, 0, \ldots, 0, 0) = 0$$

$$g(\overrightarrow{x}{=}\overrightarrow{\alpha}, y_1{=}0, y_2{=}1, y_3{=}0, \ldots, y_{m-1}{=}0, y_m{=}0) = g_n(0, 0, 1, 0, \ldots, 0, 0) = 0$$

...

$g(\overrightarrow{x}{=}\overrightarrow{\alpha}, y_1{=}0, y_2{=}0, y_3{=}0, \ldots, y_{m-1}{=}0, y_m{=}1) = g_n(0,0,0,0,\ldots,0,1) = 0$

$g(\overrightarrow{x} = \overrightarrow{1}, y_1 = 0, y_2 = 0, y_3 = 0, \ldots, y_{m-1} = 0, y_m = 0) = g_n(1,0,0,0,\ldots,0,0) = 0$ (since $g \in \mathcal{M}(R_1)$.

These are $m+1$ input tuples for which g' evaluates to 0, but the input tuples do not have a common 0. Thus, $g \notin \mathcal{M}(\mathrm{S}_0^{m+1}) \supseteq \mathcal{M}(\mathrm{S}_0^k) \supseteq \mathcal{M}(A)$. □

The classes S_0^k and S_{02}^k are very similar, since the only condition a function from S_0^k has to fulfill to be in S_{02}^k is just the behaviour for one input tuple. So, deciding membership problems for these two classes should not differ much in complexity. In the following lemma, we construct a S_{02}^k-formula which describes "nearly the same function" as a given S_0^k formula.

Lemma 21 *Let* $m \geq 2, \mathrm{S}_{02} \subseteq A \subseteq \mathrm{S}_{02}^{m+1}$. *Then* $\mathcal{M}(A \twoheadleftarrow \mathrm{S}_{02}^m)$ *is* coNP*-complete.* $\mathcal{M}(\mathrm{D}_2 \twoheadleftarrow \mathrm{S}_{02}^2)$ *is* coNP*-complete.*

Proof We show $\mathcal{M}(A \twoheadleftarrow \mathrm{S}_0^m) \leq_m^p \mathcal{M}(A \twoheadleftarrow \mathrm{S}_{02}^m)$ and $\mathcal{M}(\mathrm{D}_2 \twoheadleftarrow \mathrm{S}_0^2) \leq_m^p \mathcal{M}(\mathrm{D}_2 \twoheadleftarrow \mathrm{S}_{02}^2)$. The lemma follows with the two previous lemmas. Let f be a S_0^m-formula, i.e. a formula containing only $\rightarrow$- and dual(h_n)-gates. For $n \in \mathbb{N}$, we construct formulas z_n as follows:

- $z_1 :\equiv x_1 \vee (x_1 \wedge \overline{x_1})$
- $z_{i+1} :\equiv x_{i+1} \vee (z_i \wedge \overline{x_{i+1}})$

It is obvious that $z_n = x_1 \vee \cdots \vee x_i$ and $|z_n|$ is linear in n. Now, we replace every occurring $\rightarrow$-gate in f as follows: Instead of $f_1 \rightarrow f_2$ for input gates f_1, f_2, we introduce a gate $f_2 \vee (z_n \wedge \overline{f_1})$ with a new copy of the z_n circuit (note $x \vee (y \wedge \overline{z})$ is a base function for S_{02}^m). We call the resulting formula f'.

We show $|f'| = O(|f|^2)$: There can at most be $|f|$ $\rightarrow$-gates in f. For every of these gates, we introduce a new sub-circuit of size $O(n)$ (recall that $n \leq |f|$) plus one $x \vee (y \wedge \overline{z})$-gate. Thus, the resulting formula f' is of size $O(|f|^2)$.

We claim:
For all $(\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$, $f'(\alpha_1, \ldots, \alpha_n) = f(\alpha_1, \ldots, \alpha_n) \wedge (\alpha_1 \vee \cdots \vee \alpha_n)$.
Let $(\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$.

Case 1: $(\alpha_1, \ldots, \alpha_n) = (0, \ldots, 0)$. Since f' is a S_{02}^m-formula by construction and $\mathrm{S}_{02}^m \subseteq \mathrm{R}_0$, we see $f'(0, \ldots, 0) = 0 = f(0, \ldots, 0) \wedge (0 \vee \cdots \vee 0)$ holds.

Case 2: Let $\alpha_1 \vee \cdots \vee \alpha_n = 1$. We claim in this case $f(\alpha_1, \ldots, \alpha_n) = f'(\alpha_1, \ldots, \alpha_n)$. Obviously it is sufficient to show the value at every replaced gate in the new formula is the same as the value of the $f_1 \to f_2$ gate in the original formula. For any gate $f_1 \to f_2$, we have $f_2 \vee (z_n \wedge \overline{f_1})(\alpha_1, \ldots, \alpha_n) = f_2 \vee (1 \wedge \overline{f_1})(\alpha_1, \ldots, \alpha_n) = (f_1 \to f_2)(\alpha_1, \ldots, \alpha_n)$. Therefore, we have $f'(\alpha_1, \ldots, \alpha_n) = f(\alpha_1, \ldots, \alpha_n) = (f \wedge (x_1 \vee \cdots \vee x_n))(\alpha_1, \ldots, \alpha_n)$.

Thus, the circuit for f' calculates the same Boolean function as $f \wedge (x_1, \ldots, x_n)$.

Now we see $f \in \mathcal{M}(A) \Leftrightarrow f' \in \mathcal{M}(A)$ with Lemma 18 for $\mathrm{S}_{02} \subseteq A \subseteq \mathrm{S}_{02}^{m+1}$ (note for $f \in \mathcal{M}(\mathrm{S}_{02}^m)$, $f \in \mathcal{M}(\mathrm{S}_0^k) \Leftrightarrow f \in \mathcal{M}(\mathrm{S}_{02}^k)$ holds). For $\mathcal{M}(\mathrm{D}_2 \twoheadleftarrow \mathrm{S}_{02}^2)$, we use the following reduction (with f' as constructed above):

Let h some S_{02}^2-formula such that $h \notin \mathcal{M}(\mathrm{D}_2)$.

Let $g :\equiv \begin{cases} f', & \text{if } f(0, \ldots, 0) = 0 \\ h, & \text{if } f(0, \ldots, 0) = 1. \end{cases}$

We claim $f \in \mathcal{M}(\mathrm{D}_2) \Leftrightarrow g \in \mathcal{M}(\mathrm{D}_2)$.

Let $f \in \mathcal{M}(\mathrm{D}_2)$. Since $f \in \mathcal{M}(\mathrm{S}_0^2) \subseteq \mathcal{M}(\mathrm{R}_1)$, we know $f(1, \ldots, 1) = 1$. Since $f \in \mathcal{M}(\mathrm{D}_2)$, this implies $f(0, \ldots, 0) = 0$. Thus, $g \equiv f' = f \wedge (x_1 \vee \cdots \vee x_n) = f \in \mathcal{M}(\mathrm{D}_2)$.

Let $f \notin \mathcal{M}(\mathrm{D}_2)$.

Case 1 $f(0, \ldots, 0) = 0$. Then, as above, $g = f$, and thus $g \notin \mathcal{M}(\mathrm{D}_2)$.

Case 2 $f(0, \ldots, 0) = 1$. Then $g \equiv h \notin \mathcal{M}(\mathrm{D}_2)$.

□

4.3 S_{00}-, S_{00}^k-, S_{01}-, S_{01}^k-formulas and open problems

In this section we will discuss membership problems for formulas from classes below S_{01}^2. A lot of membership problems for these formulas are easy, because $\mathrm{S}_{01}^2 \subseteq \mathrm{M}$, and we have seen in Theorem 12 that for classes A, B such that $A \subseteq \mathrm{S}_{01}$ and $B \subseteq \mathrm{M}$, $\mathcal{M}(A \twoheadleftarrow B)$ is polynomial-time solvable.

For $k > m$, we cannot decide the complexity of $\mathcal{M}(\mathrm{S}_{01}^k \twoheadleftarrow \mathrm{S}_{01}^m)$ or $\mathcal{M}(\mathrm{S}_{00}^k \twoheadleftarrow \mathrm{S}_{00}^m)$. However, we can show a relationship between these:

Lemma 22 *Let $k > m \geq 2$. Then $\mathcal{M}(\mathrm{S}_{01}^k \twoheadleftarrow \mathrm{S}_{01}^m) \leq_m^p \mathcal{M}(\mathrm{S}_{00}^k \twoheadleftarrow \mathrm{S}_{00}^m)$.*

Proof Let f a S_{01}^m-formula. Construct S_{00}^m-formulas z_n as follows (note $x \vee (y \wedge z)$ is a base function for S_{00}^m):

- $z_1 :\equiv x_1 \vee (x_1 \wedge x_1)$
- $z_{i+1} :\equiv z_i \vee (x_{i+1} \wedge x_{i+1})$

It is obvious $z_n = (x_1 \vee \cdots \vee x_n)$, and $|z_n|$ is linear in n. Now, replace every occurring 1-gate in f with z_n, and call the result f'. Similar to the proof for Lemma 21, we can show $f' = f \wedge (x_1 \vee \cdots \vee x_n)$. (This is obvious, since for any $(\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$ with $\alpha_1 \vee \cdots \vee \alpha_n = 1$, the resulting formula describes the same function as f, since the replacement for 1 always evaluates to true. Since f' is a S_{00}-formula by construction, $f'(0, \ldots, 0) = 0$. Formally, this can be proven similarly to Lemma 21.)

Now the proposition follows with Lemma 18. □

An other open problem is $\mathcal{M}(S_0^k \twoheadleftarrow M)$ for $k \geq 3$. Again, we can state a relationship. The proof for the following lemma is based on a proof from Böhler's work. The actual reduction used is the same, our case is just more complicated technically, since we have to construct a S_{00}^m-formula of polynomial length instead of just showing the function is a member of S_{00}^m.

Lemma 23 *Let $k > m \geq 2$. $\mathcal{M}(S_0^k \twoheadleftarrow M_2) \leq_m^p \mathcal{M}(S_0^k \twoheadleftarrow S_{00}^m)$.*

Proof Let f a M_2, that is a $\{\vee, \wedge\}$-formula. First, construct formulas z_n as in Lemma 22, such that $z_n = x_1 \vee \cdots \vee x_n$, and $|z_n| = O(n) = O(|f|)$.

Let $y_1, \ldots, y_{m+1}$ new variables, $g_m := \text{dual}(h_m)$. Replace every gate

- $f_1 \vee f_2$ with $f_1 \vee (f_2 \wedge z_n)$
- $f_1 \wedge f_2$ with $g_m(y_1, \ldots, y_{m+1}) \vee (f_1 \wedge f_2)$

(note $x \vee (y \wedge z)$ is a base function for S_{00}^m.) Call the result f'', and let $f' :\equiv g_m(y_1, \ldots, y_{m+1}) \vee (f'' \wedge f'')$. From the above follows the length of f' is polynomial in $|f|$.

We claim $f' = f \vee g_m$. Let $(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_{m+1}) \in \{0,1\}^{n+m+1}$.

Case 1 $g_m(\overrightarrow{\beta}) = 1$. Then $f'(\overrightarrow{x} = \overrightarrow{\alpha}, \overrightarrow{y} = \overrightarrow{\beta}) = 1 = (f \vee g_m)(\overrightarrow{x} = \overrightarrow{\alpha}, \overrightarrow{y} = \overrightarrow{\beta})$.

Case 2 $g_m(\overrightarrow{\beta}) = 0$. In this case we have to prove $f''(\overrightarrow{x} = \overrightarrow{\alpha}, \overrightarrow{y} = \overrightarrow{\beta}) = f(\overrightarrow{x} = \overrightarrow{\alpha})$. If $\overrightarrow{\alpha} = \overrightarrow{0}$, then, since $f \in \mathcal{M}(\mathrm{M}_2) \subseteq \mathcal{M}(\mathrm{R}_0)$ and f'' is a S_{00}^m-formula, we have $f(\overrightarrow{x} = \overrightarrow{\alpha}) = f'(\overrightarrow{x} = \overrightarrow{\alpha}, \overrightarrow{y} = \overrightarrow{\beta}) = 0$. Thus we can assume $\overrightarrow{\alpha} \neq \overrightarrow{0}$, therefore we have $z_n(\overrightarrow{\alpha}) = 1$. We show the equality $f = f''$ for every gate in the circuit. Let v be a gate in f. We show the value at v and the value at the replacement gate for v in f'' are identical for the input $\alpha_1, \ldots, \alpha_n$.

Case a v is a $f_1 \vee f_2$-gate. Then we have $f_1 \vee (f_2 \wedge z_n) = f_1 \vee (f_2 \wedge 1) = f_1 \vee f_2$ (for the assignment $\overrightarrow{x} = \overrightarrow{\alpha}, \overrightarrow{y} = \overrightarrow{\beta}$).

Case b v is a $\wedge$-gate. Since $g_m(\overrightarrow{\beta}) = 0$, obviously $f_1 \wedge f_2 = g_m \vee f_1 \wedge f_2$ holds.

Thus, we have $f' = f \vee g_m(y_1, \ldots, y_{m+1})$. We claim $f \in \mathcal{M}(\mathrm{S}_0^k) \Leftrightarrow f' \in \mathcal{M}(\mathrm{S}_0^k)$.

Let $f \in \mathcal{M}(\mathrm{S}_0^k)$. Since $f \leq f'$, the proposition follows with Lemma 17.

Let $f \notin \mathcal{M}(\mathrm{S}_0^k)$. Let $\overrightarrow{\alpha_1}, \ldots, \overrightarrow{\alpha_k}$ such that $f(\overrightarrow{x} = \overrightarrow{\alpha_i}) = 0$ for $1 \leq i \leq k$ and $\overrightarrow{\alpha_1} \vee \cdots \vee \overrightarrow{\alpha_k} = 1$. Now, let

$$\overrightarrow{\gamma_i} := \begin{cases} (\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{m-i+1}), & \text{if } i \leq m+1 \\ (\underbrace{0, \ldots, 0}_{m+1}), & \text{otherwise.} \end{cases}$$

Note that since $k > m$, for every $i \in \{1, \ldots, m+1\}$, there is a γ_j with the i-th position of γ_j being 1. Thus, $f'(\overrightarrow{x} = \overrightarrow{\alpha}, \overrightarrow{y} = \overrightarrow{\gamma_i}) = 0$ for all $1 \leq i \leq k$, and $\overrightarrow{\alpha_1} \vee \cdots \vee \overrightarrow{\alpha_k} = \overrightarrow{1}$, and $\overrightarrow{\gamma_1} \vee \cdots \vee \overrightarrow{\gamma_k} = \overrightarrow{1}$. Thus, $f' \notin \mathcal{M}(\mathrm{S}_0^k)$.

□

Lemma 24 $\mathcal{M}(\mathrm{D}_2 \twoheadleftarrow \mathrm{S}_{01}^2) \leq_m^p \mathcal{M}(\mathrm{D}_2 \twoheadleftarrow \mathrm{S}_{00}^2)$.

Proof Let f a S_{01}^2-formula. Like in the proof to Lemma 22, construct a S_{00}^2-formula f' in polynomial time such that $f' = f \wedge (x_1 \vee \cdots \vee x_n)$. Now, we use the same reduction as in the corresponding proposition for S_0^2 and S_{02}^2:

Let h some S_{02}^2-formula such that $h \notin \mathcal{M}(\mathrm{D}_2)$.

Let $g :\equiv \begin{cases} f', & \text{if } f(0, \ldots, 0) = 0 \\ h, & \text{if } f(0, \ldots, 0) = 1. \end{cases}$

We claim $f \in \mathcal{M}(\mathrm{D}_2) \Leftrightarrow g \in \mathcal{M}(\mathrm{D}_2)$.

Let $f \in \mathcal{M}(\mathrm{D}_2)$. Since $f \in \mathcal{M}(\mathrm{S}_0^2) \subseteq \mathcal{M}(\mathrm{R}_1)$, we know $f(1,\ldots,1) = 1$. Since $f \in \mathcal{M}(\mathrm{D}_2)$, we have $f(0,\ldots,0) = 0$. Thus, $g \equiv f' = f \wedge (x_1 \vee \cdots \vee x_n) = f \in \mathcal{M}(\mathrm{D}_2)$.

Let $f \notin \mathcal{M}(\mathrm{D}_2)$.

Case 1 $f(0,\ldots,0) = 0$ Then, as above, $g = f$, and thus $g \notin \mathcal{M}(\mathrm{D}_2)$.

Case 2 $f(0,\ldots,0) = 1$ Then $g \equiv h \notin \mathcal{M}(\mathrm{D}_2)$.

□

So we have seen deciding membership problems for S_{01}^k-formulas is not harder than for S_{00}^k-formulas. It seems plausible to assume the reverse is also true, since S_{00}^k is a subset of S_{01}^k, but there does not seem to be a straightforward way to convert S_{00}^k-formulas into equivalent S_{01}^k-formulas in polynomial time. To do this canonically, we have to find some S_{01}^k-formula for $x \vee (y \wedge z)$ with each of the variables x, y, z occurring only once.

5 Formulas representing monotonic functions

In this section, we will examine membership problems for M-, M_1- and M_2-formulas. The results follow directly from a "dualization" of a proof for the the corresponding proposition for 1-separating functions in Böhler's work. Note that since for $M' \in \{\mathrm{M}, \mathrm{M}_2\}$, $M' = \mathrm{dual}(M')$ and $\mathrm{base}(M') = \mathrm{dual}(\mathrm{base}(M'))$ holds. Therefore, we only need to consider subclasses of M and M_2 on the left side of Post's lattice due to Lemma 4.

Lemma 25 *Let $A \in \mathcal{P}$, $\mathrm{D}_2 \subseteq A \subseteq \mathrm{S}_{00}^2$. Then $\mathcal{M}(A \twoheadleftarrow \mathrm{M}_2)$ is coNP-complete.*

Proof We show $EQ^F(\{\wedge, \vee\}) \leq_m^p \mathcal{M}(A \twoheadleftarrow \mathrm{M}_2)$. The lemma follows with Theorem 7.

Let f_1, f_2 be $\{\wedge, \vee\}$-formulas. Let $g(x_1, \ldots, x_n, y, z) :\equiv (y \vee f_1) \wedge (z \vee \mathrm{dual}(f_2)) \wedge (y \vee z)$. Since for a M_2-formula calculating the dual function is just exchanging every $\vee$ with a $\wedge$ and vice versa, this can be expressed as a M_2-formula in polynomial time. Observe the following equations hold:

$$\begin{array}{lcl}
g(\overrightarrow{x} = \overrightarrow{\alpha}, y = 1, z = 0) & = & 1 \wedge \mathrm{dual}(f_2)(\overrightarrow{\alpha}) \wedge 1 \\
 & = & \mathrm{dual}(f_2)(\overrightarrow{\alpha}) \\
g(\overrightarrow{x} = \overrightarrow{\alpha}, y = 0, z = 1) & = & f_1(\overrightarrow{\alpha}) \wedge 1 \wedge 1 \\
 & = & f_1(\overrightarrow{\alpha}) \\
\mathrm{dual}(g)(\overrightarrow{x} = \overrightarrow{\alpha}, y = 1, z = 0) & = & \neg(0 \vee f_1(\overline{\overrightarrow{\alpha}})) \wedge (1 \vee \mathrm{dual}(f_2)(\overline{\overrightarrow{\alpha}})) \wedge (0 \vee 1) \\
 & = & \neg f_1(\overline{\overrightarrow{\alpha}}) \\
 & = & \mathrm{dual}(f_1)(\overrightarrow{\alpha}) \\
\mathrm{dual}(g)(\overrightarrow{x} = \overrightarrow{\alpha}, y = 0, z = 1) & = & \neg(1 \vee f_1(\overline{\overrightarrow{\alpha}})) \wedge (0 \vee \mathrm{dual}(f_2)(\overline{\overrightarrow{\alpha}})) \wedge (1 \vee 0) \\
 & = & \neg \mathrm{dual}(f_2)(\overline{\overrightarrow{\alpha}}) \\
 & = & f_2(\overrightarrow{\alpha}) \\
g(\overrightarrow{x} = \overrightarrow{\alpha}, y = 0, z = 0) & = & 0 \\
g(\overrightarrow{x} = \overrightarrow{\alpha}, y = 1, z = 1) & = & 1
\end{array}$$

We claim $f_1 = f_2 \Leftrightarrow g \in \mathcal{M}(A)$.

Let $f_1 = f_2$. Then $\mathrm{dual}(f_1) = \mathrm{dual}(f_2)$, and from the above equations follows $\mathrm{dual}(g) = g$. Since $g \in \mathcal{M}(\mathrm{M})$, we have $g \in \mathcal{M}(\mathrm{M} \cap \mathrm{D}) = \mathcal{M}(\mathrm{D}_2) \subseteq \mathcal{M}(A)$.

Now, without loss of generality, let $\overrightarrow{\alpha}$ such that $f_1(\overrightarrow{\alpha}) = 0, f_2(\overrightarrow{\alpha}) = 1$. Then we have

$$\begin{array}{lclclcl}
g(\overrightarrow{x} = \overrightarrow{\alpha}, y = 0, z = 1) & = & f_1(\overrightarrow{\alpha}) & = & 0 & & \\
g(\overrightarrow{x} = \overline{\overrightarrow{\alpha}}, y = 1, z = 0) & = & \mathrm{dual}(f_2)(\overline{\overrightarrow{\alpha}}) & = & \neg f_2(\overrightarrow{\alpha}) & = & 0
\end{array}$$

but obviously the two input tuples do not have a common 0, thus $g \notin \mathcal{M}(\mathrm{S}_0^2) \supseteq \mathcal{M}(A)$. □

Corollary 26 *The following problems are coNP-complete:* $\mathcal{M}(\mathrm{D}_2 \twoheadleftarrow \mathrm{M}_1)$, $\mathcal{M}(\mathrm{D}_2 \twoheadleftarrow \mathrm{M})$, $\mathcal{M}(\mathrm{S}_{00}^2 \twoheadleftarrow \mathrm{M}_2)$, $\mathcal{M}(\mathrm{S}_{00}^2 \twoheadleftarrow \mathrm{M}_1)$, $\mathcal{M}(\mathrm{S}_{00}^2 \twoheadleftarrow \mathrm{M})$, $\mathcal{M}(\mathrm{S}_{01}^2 \twoheadleftarrow \mathrm{M}_1)$, $\mathcal{M}(\mathrm{S}_{01}^2 \twoheadleftarrow \mathrm{M})$.

Proof The first four cases are trivial, since the bases for M_1, M_2 are supersets of the base for M_2. The remaining two cases follow from $\mathcal{M}(\mathrm{S}_{00}^2 \twoheadleftarrow \mathrm{M}_2) = \mathcal{M}(\mathrm{S}_{01}^2 \twoheadleftarrow \mathrm{M}_2) \leq_m^p \mathcal{M}(\mathrm{S}_{01}^2 \twoheadleftarrow \mathrm{M}_1) \leq_m^p \mathcal{M}(\mathrm{S}_{01}^2 \twoheadleftarrow \mathrm{M})$. □

6 Formulas representing self-dual functions

We will now consider D- and D_1-formulas. Note $\mathcal{M}(A \twoheadleftarrow \mathrm{D}_2)$ is in P for any class A from $\mathcal{P}$.

Lemma 27 *Let* $A \subseteq \mathrm{M}$, $B \in \{\mathrm{D}, \mathrm{D}_1\}$. *Then* $\mathcal{M}(A \twoheadleftarrow B)$ *is coNP-complete.*

Proof We show $EQ^F(B) \leq_m^p \mathcal{M}(A \twoheadleftarrow B)$. The result follows with Theorem 7. Let f_1, f_2 be B-formulas. Since $\mathrm{L}_2 \subseteq B$, with Lemma 6, we can construct a B-formula g in polynomial time, such that $g = f_1 \oplus f_2 \oplus y$. We claim $f_1 = f_2$ if and only if $g \in \mathcal{M}(A)$.

Let $f_1 = f_2$. Then $g = y \in \mathcal{M}(I_2) \subseteq \mathcal{M}(A)$.

Let $\alpha_1, \ldots, \alpha_n \in \{0, 1\}$ such that $f_1(\alpha_1, \ldots, \alpha_n) \neq f_2(\alpha_1, \ldots, \alpha_n)$. Then we have

$$g(x_1 = \alpha_1, \ldots, x_n = \alpha_n, y = 0) = f_1(\alpha_1, \ldots, \alpha_n) \oplus f_2(\alpha_1, \ldots, \alpha_n) \oplus 0 = 1$$

$$g(x_1 = \alpha_1, \ldots, x_n = \alpha_n, y = 1) = f_1(\alpha_1, \ldots, \alpha_n) \oplus f_2(\alpha_1, \ldots, \alpha_n) \oplus 1 = 0$$

thus, $g \notin \mathcal{M}(\mathrm{M}) \supseteq \mathcal{M}(A)$. □

Lemma 28 *Let $A, B \in \mathcal{P}$ such that $A \subseteq \mathrm{L}$ and $B \in \{\mathrm{D}, \mathrm{D}_1\}$. Then $\mathcal{M}(A \twoheadleftarrow B)$ is coNP-complete.*

Proof We show $EQ^F(B) \leq_m^p \mathcal{M}(A \twoheadleftarrow B)$. The proposition follows with Theorem 7. Let h be some B-formula such that $h \notin \mathcal{M}(A)$. Now, let f_1, f_2 be any B-formulas. If $f_1(0, \ldots, 0) \neq f_2(0, \ldots, 0)$, then let $g :\equiv h$. Otherwise, let $g :\equiv y f_1 \vee y \overline{f_2} \vee f_1 \overline{f_2}$. This can be expressed as a B-formula in polynomial time with Lemma 6. We claim $f_1 = f_2 \Leftrightarrow g \in \mathcal{M}(A)$.

Let $f_1 = f_2$. Then $g = y f_1 \vee y \overline{f_1} \vee f_1 \overline{f_1} = y \in \mathcal{M}(\mathrm{I}_2) \subseteq \mathcal{M}(A)$.

Let $f_1 \neq f_2$.

Case 1: $f_1(0, \ldots, 0) \neq f_2(0, \ldots, 0)$. Then $g \equiv h \notin \mathcal{M}(A)$.

Case 2: $f_1(0, \ldots, 0) = f_2(0, \ldots, 0) =: \beta$. Let $\alpha_1, \ldots, \alpha_n \in \{0, 1\}$ such that, without loss of generality,

$$f_1(\alpha_1, \ldots, \alpha_n) = 0$$
$$f_2(\alpha_1, \ldots, \alpha_n) = 1$$

(Otherwise, since f_1 and f_2 are self-dual, choose $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$.) Now we have:

$$g(x_1 = 0, \ldots, x_n = 0, y) = y\beta \vee y\overline{\beta} \vee \beta\overline{\beta} = y$$

Thus, y is a relevant variable for g. Assume $g \in \mathcal{M}(A) \subseteq \mathcal{M}(L)$. Then, since y is relevant for g, the negation of y's value would negate the value of g as well. But we have

$$g(x_1 = \alpha_1, \ldots, x_n = \alpha_n, y = 0) = (0 \wedge 0) \vee (0 \wedge 0) \vee (0 \wedge 1) = 0$$
$$f(x_1 = \alpha_1, \ldots, x_n = \alpha_n, y = 1) = (1 \wedge 0) \vee (1 \wedge 0) \vee (0 \wedge 1) = 0$$

so, $g \notin \mathcal{M}(\mathrm{L}) \supseteq \mathcal{M}(A)$.

□

7 Conclusions and generalizations

In all cases we were able to solve, it has been shown the membership problem for B-formulas is as hard to solve as the membership problem for $\{\vee, \wedge, \neg\}$ circuits with promise B. This is surprising, since this means the knowledge of the actual representation of a Boolean function as a B-formula does not give us any significant advantage over knowing the described function is from the class B.

Although we always focused on a single fixed base for every class, most of the results can easily be generalized for arbitrary bases, since Lemma 6 can be stated for any base. Thus, we can use the same reductions we used for our proofs for coNP-completeness. There are only two kinds of proofs dependant on explicit bases: The proofs for membership problems for S_{0x}^k-formulas (Lemma 21 and Lemma 22) - in those proofs, we transformed a circuit into another, which only works under the given bases. The other case is the coNP-completeness result for M-formulas (Lemma 25), where we used the fact that for a given M_2-formula f, $\mathrm{dual}(f)$ is a M_2-formula as well.

All polynomial-time proofs only used the fact that the value of a Boolean circuit can always be calculated in polynomial time, and thus are also independent of the base chosen.

We were not able to decide the complexity of $\mathcal{M}(\mathrm{S}_{01}^k \twoheadleftarrow \mathrm{M})$ for $k > 3$. It seems plausible to assume these problems are coNP-complete, since this is the case for $k = 2$, and there seems to be no reason why this should be more difficult than the general case. If this problem is in fact coNP-complete, we know $\mathcal{M}(\mathrm{S}_{00}^k \twoheadleftarrow \mathrm{S}_{00}^m)$ is coNP-complete as well for $k > m$, and it seems plausible to assume $\mathcal{M}(\mathrm{S}_{01}^k \twoheadleftarrow \mathrm{S}_{01}^m)$ cannot be easier than $\mathcal{M}(\mathrm{S}_{00}^k \twoheadleftarrow \mathrm{S}_{00}^m)$. So the main question here remains that of the complexity of $\mathcal{M}(\mathrm{S}_{01}^k \twoheadleftarrow \mathrm{M})$ for $k > 3$.

The other open problem is $\mathcal{M}(\mathrm{D}_2 \twoheadleftarrow B)$ for $B \in \{\mathrm{S}_{00}^2, \mathrm{S}_{01}^2\}$. Since $\mathcal{M}(A \wr_B)$ and $\mathcal{M}(A \twoheadleftarrow B)$ are of the same complexity for all known cases and $\mathcal{M}(\mathrm{D}_2 \wr_{\mathrm{S}_{00}^2})$ is coNP-complete, these problems are most likely coNP-complete as well. Looking a Böhler's proof, the straightforward way to show $\mathcal{M}(\mathrm{D}_2 \twoheadleftarrow \mathrm{S}_{00}^2)$ is coNP-complete would be to construct, for a given S_{00}^2-formula f a S_{00}^2-formula which is equivalent to $f \vee \mathrm{dual}(f)$. Such a formula surely exists, since $f \vee \mathrm{dual}(f)$ is in S_{00}^2 again, but it is not clear how to do this in polynomial time and length.

8 Collection of results

In this concluding section, we give an overview of our results. For the following, let $k, m \in \mathbb{N}$ such that $k > m \geq 2$. Since membership problems for B-formulas with $B \subseteq \mathrm{V}$, $B \subseteq \mathrm{L}$, $B \subseteq \mathrm{D}_2$ or $B \subseteq \mathrm{E}$ are always polynomial-time solvable, these results are not repeated here. For subclasses from L, this follows from Theorem 11, for classes below V, this is a consequence from Theorem 12. When some result is referred to as "trivial", this means it is of the form $\mathcal{M}(A \twoheadleftarrow B)$ for $A \in \{B \cap \mathrm{R}_0, B \cap \mathrm{R}_1, B \cap \mathrm{R}_2\}$, and therefore only one or two values of the B-circuit must be calculated to decide the membership problem.

cNPc is used as an abbreviation for "coNP-complete" in this table.

Problem	Comp	Source
$\mathcal{M}(S_{02}^m \twoheadleftarrow R_2)$	cNPc	Lemma 13
$\mathcal{M}(S_{02} \twoheadleftarrow R_2)$	cNPc	Lemma 13
$\mathcal{M}(S_{00}^m \twoheadleftarrow R_2)$	cNPc	Lemma 13
$\mathcal{M}(S_{00} \twoheadleftarrow R_2)$	cNPc	Lemma 13
$\mathcal{M}(S_{12}^m \twoheadleftarrow R_2)$	cNPc	Lemma 14
$\mathcal{M}(S_{12} \twoheadleftarrow R_2)$	cNPc	Lemma 14
$\mathcal{M}(S_{10}^m \twoheadleftarrow R_2)$	cNPc	Lemma 14
$\mathcal{M}(S_{10} \twoheadleftarrow R_2)$	cNPc	Lemma 14
$\mathcal{M}(M_2 \twoheadleftarrow R_2)$	cNPc	Lemma 13
$\mathcal{M}(D_1 \twoheadleftarrow R_2)$	cNPc	Lemma 13
$\mathcal{M}(D_2 \twoheadleftarrow R_2)$	cNPc	Lemma 13
$\mathcal{M}(L_2 \twoheadleftarrow R_2)$	cNPc	Lemma 13
$\mathcal{M}(I_2 \twoheadleftarrow R_2)$	cNPc	Lemma 13
$\mathcal{M}(V_2 \twoheadleftarrow R_2)$	cNPc	Lemma 13
$\mathcal{M}(E_2 \twoheadleftarrow R_2)$	cNPc	Lemma 13
$\mathcal{M}(S_{02}^m \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(S_{02} \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(S_{01}^m \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(S_{01} \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(S_{00} \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(S_{00}^m \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(S_{12}^m \twoheadleftarrow R_1)$	cNPc	Lemma 14
$\mathcal{M}(S_{10}^m \twoheadleftarrow R_1)$	cNPc	Lemma 14
$\mathcal{M}(S_{10} \twoheadleftarrow R_1)$	cNPc	Lemma 14
$\mathcal{M}(S_{12} \twoheadleftarrow R_1)$	cNPc	Lemma 14
$\mathcal{M}(M_2 \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(D_1 \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(D_2 \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(I_2 \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(V_2 \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(L_2 \twoheadleftarrow R_1)$	cNPc	Lemma 15
$\mathcal{M}(L_1 \twoheadleftarrow R_1)$	cNPc	Lemma 15
$\mathcal{M}(E_2 \twoheadleftarrow R_1)$	cNPc	Lemma 14
$\mathcal{M}(S_0^m \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(S_{02}^m \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(S_0 \twoheadleftarrow R_1)$	coNPc	Lemma 13
$\mathcal{M}(S_{02} \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(V_1 \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(I_1 \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(M_1 \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(E_1 \twoheadleftarrow R_1)$	cNPc	Lemma 13
$\mathcal{M}(S_{00}^k \twoheadleftarrow S_0^m)$	cNPc	Lemma 20
$\mathcal{M}(S_{00} \twoheadleftarrow S_0^m)$	cNPc	Lemma 20
$\mathcal{M}(S_{02}^m \twoheadleftarrow S_0^m)$	P	trivial
$\mathcal{M}(S_{01}^m \twoheadleftarrow S_0^m)$	cNPc	Lemma 19
$\mathcal{M}(S_{00}^m \twoheadleftarrow S_0^m)$	cNPc	Lemma 19
$\mathcal{M}(S_{02}^k \twoheadleftarrow S_{02}^m)$	cNPc	Lemma 21
$\mathcal{M}(S_{00}^m \twoheadleftarrow S_{02}^m)$	cNPc	Lemma 19
$\mathcal{M}(S_{00}^k \twoheadleftarrow S_{02}^m)$	cNPc	Lemma 19
$\mathcal{M}(S_{00} \twoheadleftarrow S_{02}^m)$	cNPc	Lemma 19
$\mathcal{M}(S_{01} \twoheadleftarrow S_{02}^m)$	cNPc	Lemma 19
$\mathcal{M}(S_{01} \twoheadleftarrow S_{02}^m)$	cNPc	Lemma 21
$\mathcal{M}(V_1 \twoheadleftarrow S_{02}^m)$	cNPc	Lemma 19
$\mathcal{M}(V_2 \twoheadleftarrow S_{02}^m)$	cNPc	Lemma 19
$\mathcal{M}(I_1 \twoheadleftarrow S_{02}^m)$	cNPc	Lemma 19
$\mathcal{M}(I_2 \twoheadleftarrow S_{02}^m)$	cNPc	Lemma 19

Problem	Comp	Source
$\mathcal{M}(V_1 \twoheadleftarrow S_0^m)$	cNPc	Lemma 20
$\mathcal{M}(V_2 \twoheadleftarrow S_0^m)$	cNPc	Lemma 20
$\mathcal{M}(I_1 \twoheadleftarrow S_0^m)$	cNPc	Lemma 19
$\mathcal{M}(I_2 \twoheadleftarrow S_0^m)$	cNPc	Lemma 19
$\mathcal{M}(S_0^k \twoheadleftarrow S_0^m)$	cNPc	Lemma 20
$\mathcal{M}(S_0 \twoheadleftarrow S_0^m)$	cNPc	Lemma 20
$\mathcal{M}(S_{02}^k \twoheadleftarrow S_0^m)$	cNPc	Lemma 20
$\mathcal{M}(S_{02} \twoheadleftarrow S_0^m)$	cNPc	Lemma 20
$\mathcal{M}(S_{01}^k \twoheadleftarrow S_0^m)$	cNPc	Lemma 20
$\mathcal{M}(S_{01} \twoheadleftarrow S_0^m)$	cNPc	Lemma 20
$\mathcal{M}(D_2 \twoheadleftarrow D_1)$	cNPc	Lemma 27
$\mathcal{M}(L_2 \twoheadleftarrow D_1)$	cNPc	Lemma 28
$\mathcal{M}(I_2 \twoheadleftarrow D_1)$	cNPc	Lemma 27
$\mathcal{M}(D_1 \twoheadleftarrow D)$	P	trivial
$\mathcal{M}(D_2 \twoheadleftarrow D)$	cNPc	Lemma 27
$\mathcal{M}(L_2 \twoheadleftarrow D)$	cNPc	Lemma 28
$\mathcal{M}(I_2 \twoheadleftarrow D)$	cNPc	Lemma 27
$\mathcal{M}(L_3 \twoheadleftarrow D)$	cNPc	Lemma 28
$\mathcal{M}(N_2 \twoheadleftarrow D)$	cNPc	Lemma 28
$\mathcal{M}(S_{00}^2 \twoheadleftarrow M_2)$	cNPc	Lemma 25
$\mathcal{M}(S_{00} \twoheadleftarrow M_2)$	P	Theorem 12
$\mathcal{M}(V_2 \twoheadleftarrow M_2)$	P	Theorem 12
$\mathcal{M}(I_2 \twoheadleftarrow M_2)$	P	Theorem 12
$\mathcal{M}(D_2 \twoheadleftarrow M_2)$	cNPc	Lemma 25
$\mathcal{M}(M_2 \twoheadleftarrow M_1)$	P	trivial
$\mathcal{M}(S_{00} \twoheadleftarrow M_1)$	P	Theorem 12
$\mathcal{M}(V_2 \twoheadleftarrow M_1)$	P	Theorem 12
$\mathcal{M}(I_2 \twoheadleftarrow M_1)$	P	Theorem 12
$\mathcal{M}(D_2 \twoheadleftarrow M_1)$	cNPc	Corollary 26
$\mathcal{M}(E_1 \twoheadleftarrow M_1)$	P	Theorem 12
$\mathcal{M}(E_2 \twoheadleftarrow M_1)$	P	Theorem 12
$\mathcal{M}(I_1 \twoheadleftarrow M_1)$	P	Theorem 12
$\mathcal{M}(S_{01} \twoheadleftarrow M_1)$	P	Theorem 12
$\mathcal{M}(V_1 \twoheadleftarrow M_1)$	P	Theorem 12
$\mathcal{M}(S_{00}^2 \twoheadleftarrow M_1)$	cNPc	Corollary 26
$\mathcal{M}(S_{01}^2 \twoheadleftarrow M_1)$	cNPc	Corollary 26
$\mathcal{M}(M_1 \twoheadleftarrow M)$	P	trivial
$\mathcal{M}(M_2 \twoheadleftarrow M)$	P	trivial
$\mathcal{M}(S_{00} \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(S_{01}^2 \twoheadleftarrow M)$	cNPc	Corollary 26
$\mathcal{M}(V_2 \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(I_2 \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(D_2 \twoheadleftarrow M)$	cNPc	Corollary 26
$\mathcal{M}(E_1 \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(E_2 \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(I_1 \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(S_{01} \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(V_1 \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(E \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(E_0 \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(V \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(V_1 \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(V_0 \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(I \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(I_0 \twoheadleftarrow M)$	P	Theorem 12
$\mathcal{M}(S_{00}^2 \twoheadleftarrow M)$	cNPc	Corollary 26

The complexity of $\mathcal{M}(A \twoheadleftarrow B)$ for selected combinations ($k > m > 2$):

$A \backslash B$	BF	R_1	M	M_2	S_0^2	S_0^m	S_0	S_{01}^2	S_{01}^m	S_{01}	D	D_2	L	V
BF	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$
R_1	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$
R_2	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$
M	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
M_1	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
M_2	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
S_0^2	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
S_0^k	$\bullet$	$\bullet$	?	?	$\bullet$	$\bullet$	$\circ$	?	?	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
S_0	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
S_{01}^2	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
S_{01}^k	$\bullet$	$\bullet$	?	?	$\bullet$	$\bullet$	$\bullet$	?	?	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
S_{01}	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
D	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	?	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$
D_1	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	?	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$
D_2	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	?	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
L	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
L_0	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
L_1	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
L_2	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
L_3	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
V	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
V_2	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
N	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
I	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$
I_2	$\bullet$	$\bullet$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\circ$	$\bullet$	$\circ$	$\circ$	$\circ$

$\circ$ polynomial time solvable, $\bullet$ coNP-complete, ? unknown

References

[Böh] Elmar Böhler *On the Relative Complexity of Post's Classes* Technical report 286, Univertität Würzburg

[Lew79] Harry R. Lewis *Satisfiability problems for propositional calculi* Mathematical Systems Theory, 13:45-53, 1979

[Pos41] Emil Leon Post. *Two-value iterative systems* Annals of Mathematical Studies, 5:1 122, 1941.

[ReiWag99] Steffen Reith, Klaus Wagner *The Complexity of Problems Defined by Subclasses of Boolean Functions* Technical report 218, Univertität Würzburg

[Rei01] Steffen Reith *Generalized Satisfiability Problems* PhD Thesis, Institut für Informatik, Universität Würzburg, Februar 2001

[Vol99] Heribert Vollmer *Introduction to Circuit Complexity* Springer, 1999