Grabmann, Konstantin:

Quantifier elimination for infinite atomic Boolean differential rings

Bachelorarbeit, Wintersemester 2023

Gutachter*in: Weitkämper, Felix

Fakultät für Mathematik, Informatik und Statistik
Institut für Informatik

Ludwig-Maximilians-Universität München

https://doi.org/10.5282/ubm/epub.129556

Bachelor's Thesis

Quantifier elimination for infinite atomic Boolean differential rings

Institut für Informatik
Lehr- und Forschungseinheit für Programmiersprachen und Künstliche Intelligenz
Ludwig-Maximilians-Universität München

Konstantin Bastian Grabmann

Munich, November 25th, 2023

Supervised by Felix Weitkämper

Abstract

The Boolean Differential Calculus expands on Boolean algebras with one or multiple differential operators. Weitkämper in his paper [9] provides an axiomatization for this calculus, which, for a Boolean algebra K, describes a Boolean algebra with derivative δ with $\ker(\delta) \cong K$ up to isomorphism. In this thesis, we first motivate the calculus and explore, using a simple example, how this characterization up to isomorphism behaves. After this, we are interested in the case where K is an infinite atomic Boolean algebra. We show that every model of this theory T_1^K is an atomic Boolean ring. Moreover, the form of all its atoms are described. Additionally, we also study finitely generated substructure of these models. Again, the atoms are described. Using this knowledge, we give a proof for quantifier elimination, where we only have to add countably many unary predicates C_n to the signature, which count the atoms below an element, and a new constant symbol, which gets interpreted as the Boolean function whose derivative is equal to one. We will do so by a standard back-and-forth argument and closely follow a proof of quantifier elimination in the theory of infinite atomic Boolean algebras extended by the C_n's, given by Derakhshan and Macintyre in [1].

Contents

1 Introduction

Boolean algebras provide a mathematical framework for reasoning about digital circuits. This goes back to Claude Shannon, who used the two-valued Boolean algebra as an aid towards the analysis and synthesis of switching circuits [6]. Given the real world applications, a lot of research was conducted to tackle problems arising when working with digital circuits. Extending Boolean algebras by derivative operations allows the observation of changes to function values. A recent textbook covering the Boolean Differential Calculus and its many applications is [8].

Weitkämper in his paper [9] introduced an axiomatization of the theory, which, for a Boolean algebra K, characterizes a derivative with kernel isomorphic to K up to isomorphism. In this bachelor's thesis we will show that, in the special case where K is an infinite atomic algebra, this theory T_1^K, enriched by predicates "n atoms lie below x" and a new constant symbol z corresponding to a Boolean function whose derivative is equal to 1, has quantifier elimination. The motivation for this result is twofold. Firstly, when K is an infinite atomless Boolean algebra, the theory T_1^K admits quantifier elimination. Whether this also holds when K is an infinite atomic Boolean algebra naturally arises. Secondly, T_1^K is the generic theory of the class of Boolean rings of switching function in n variables equipped with, for example, the much studied partial derivatives $\delta_i(f) := f(x_1, \dots, x_n) \oplus f(x_1, \dots, \bar{x}_i, \dots, x_n)$ with $1 \leq i \leq n$. This way, any sentence of the theory holds in all such rings of a certain size. They are the content of study when working with real world scenarios. Now quantifier elimination guarantees that for every formula there exists a quantifier-free formula, which is equivalent modulo the theory. A quantifier-free sentence here primarily equates to a Boolean differential equation, which can be decided algorithmically. Putting it all together, this hints towards an algorithm to decide properties about a whole class of switching functions for circuit of a certain size. We only provide a non-constructive proof for quantifier elimination, hence finding an efficient algorithm requires further research.

The proof follows the examples provided in Derakhshan and Macintyre's paper [1], which gives an alternative proof to a classical result of Tarksi, showing that the theory of infinite atomic Boolean rings enriched by relation symbols counting the atoms below an element admits quantifier elimination. As part of the proof we will classify all atoms of a finitely generated substructure. This in itself provides an interesting result. Moreover, the atoms are of simple form and can be described using only a special element z whose derivative is equal to one and the constants. Looking at the atoms of the whole structure, which are precisely the products of atoms from the kernel with z or its complement, we see that this follows a general pattern.

1.1 Organization

The first section provides an overview of all model-theoretic concepts and results needed. The most important part result is a criterion for quantifier elimination, which allows us to use structural knowledge.

After that, the main object of study, the Boolean ring of switching functions, is motivated and introduced. We bring up its link to digital circuit design to apply the purely mathematical concepts to real world problems. The section concludes with some generic properties of the theory T_1^K for an infinite atomic Boolean algebra, which will be used in the proof.

The proof for quantifier elimination will follow the criterion introduced before and use explicit description of the atoms.

Lastly, the conclusion gives a short summary of the proof, discusses some of the interesting result round and sketches a link to real world problems, hinting to further research.

2 Preliminaries

2.1 Model-theoretic Fundamentals

In this section we cover all model-theoretic results and definitions needed for the thesis. Some familiarity with first-order logic is expected, which can be found in most introductory textbooks on logic. If not stated otherwise, $\mathcal{L}$ is assumed to be a countable first-order language. As usual, $\vec{c}$ denotes a tuple of elements indexed by natural numbers. Additionally, $\mathcal{L}(\vec{c})$ is the first-order language obtained by adding every component of the tuple $\vec{c}$ to the constants of $\mathcal{L}$. Moreover, if A is an $\mathcal{L}$-structure and $\vec{a}$ is a tuple of elements from A of same length as $\vec{c}$, then $(A, \vec{a})$ is naturally an $\mathcal{L}(\vec{c})$-structure obtained by interpreting $\vec{c}$ as $\vec{a}$.

Often we are interested in the first-order theory of a model, being all first-order formulas that hold in the model. Two models which have the same theory are called elementary equivalent. The following proposition gives us an equivalent description of elementary equivalence.

Proposition 2.1 (Digram lemma, Lemma 1.4.2 of [3]). *Let A and B be $\mathcal{L}$-structures, $\vec{c}$ a sequence of constants, and $(A, \vec{a})$ and $(B, \vec{b})$ $\mathcal{L}(\vec{c})$-structures. The following are equivalent:*

(a) $(A, \vec{a}) \equiv_0 (B, \vec{b})$, meaning for every atomic sentence ϕ of $\mathcal{L}(c)$, $(A, \vec{a}) \models \phi \Leftrightarrow (B, \vec{b}) \models \phi$.

(b) There is an embedding $f : \langle \vec{a} \rangle_A \to B$ such that $f\vec{a} = \vec{b}$. $\langle \vec{a} \rangle_A$ denotes the smallest substructure of A containing $\vec{a}$.

Back-and-forth equivalence is another way of classifying models, which lies somewhere between isomorphism and elementary equivalence. We define back-and-forth equivalence using the formulation of back-and-forth systems.

Definition 2.2 (Lemma 3.2.2 of [3]). *Given $\mathcal{L}$-structures A and B, a back-and-forth system from A to B is a set I of pairs $(\vec{a}, \vec{b})$ of tuples, with $\vec{a}$ from A and $\vec{b}$ from B, such that*

- *if $(\vec{a}, \vec{b})$ is in I then $\vec{a}$ and $\vec{b}$ have the same length and $(A, \vec{a}) \equiv_0 (B, \vec{b})$,*
- *I is not empty,*
- *for every pair $(\vec{a}, \vec{b})$ in I and every element c of A there is an element d of B such that the pair $(\vec{a}c, \vec{b}d)$ is in I, and*

- *for every pair $(\vec{a}, \vec{b})$ in I and every element d of B there is an element c of A such that the pair $(\vec{a}c, \vec{b}d)$ is in I.*

A and B are said to be back-and-forth equivalent if there is a back-and-forth system from A to B. Note that we can easily transform a back-and-forth system from A to B to one from B to A and vice versa by reversing the tuples in the set, making this definition symmetric.

Often we have efficient algorithms for deciding quantifier-free sentences of a theory, but many interesting properties are formulated using quantifiers. The question naturally arises whether it is possible, given an arbitrary formula, to find a quantifier-free formula which is equivalent in all models of the theory. From this perspective, the interest lies in constructing quantifier-free equivalents by an algorithmic process. This is generally much harder than using a non-constructive proof. We give a criterion for quantifier elimination which has been successfully applied to infinite atomic Boolean algebras, but does not give much insight into constructing the quantifier-free formulas.

Definition 2.3. *Let T be a theory in $\mathcal{L}$. T has quantifier elimination if for every formula $\phi(\vec{x})$ of T there exists a quantifier-free formula $\tilde{\phi}(\vec{x})$ of T such that $A \models \phi \Leftrightarrow \tilde{\phi}$ for every model A of T.*

In order to state the criterion for quantifier elimination, we need the notion of ω-saturated models. Suppose that A is an $\mathcal{L}$-structure and X is set of elements from A. Let $\mathrm{Th}_X(A)$ be the set of all $\mathcal{L}(X)$-sentences true in A.

Definition 2.4. *A is called ω-saturated if for every finite set X of elements of A, all complete n-types over X with respect to A are already realized by elements in A. An n-type p is a set of $\mathcal{L}(X)$-formulas with free variables $v_1, \ldots, v_n$, such that $p \cup Th_X(A)$ is satisfiable. Moreover, p is called complete if $\phi \in p$ or $\neg\phi \in p$ for all $L(X)$-formulas ϕ with free variables from $v_1, \ldots, v_n$.*

In the case where A is a model of a complete theory, the n-types don't have to be complete. See Proposition 4.3.2 of [5]

To show that a set of $\mathcal{L}(X)$ formulas is an n-type, we have to prove that $p \cup \mathrm{Th}_X(A)$ is satisfiable. This is usually done using the compactness theorem for first-order-logic, which gives us a template for the proof.

Proposition 2.5 (Compactness theorem for first-order-logic, Theorem 6.1.1. of [3])**.** *Let T be a first-order theory. If every finite subset of T has a model then T has a model.*

We can now state an equivalent condition for quantifier elimination. This allows us to use structural information of the theory's models. As we see in the next section, we have quite a good structural understanding of the theory of infinite atomic Boolean differential algebras.

Proposition 2.6 (Exercise 8.4.4 of [3])**.** *Let T be a theory in $\mathcal{L}$. The following are equivalent.*

(a) T has quantifier elimination.

(b) *If A and B are any ω-saturated models of T and $\vec{a}$ is a tuple of elements from A and $\vec{b}$ is a tuple of elements from B of same length such that $(A, \vec{a}) \equiv_0 (B, \vec{b})$, then $(A, \vec{a})$ and $(B, \vec{b})$ are back-and-forth equivalent.*

Proof. See Theorem 5.4 of [2]. □

2.2 Boolean Structures and Constructions

A famous application of Boolean algebras lies in the analysis and synthesis of digital systems. This goes back to Claude Shannon, who used Boolean function to describe switching circuits in his master's thesis [6]. A switching circuit is an idealized network of switches with a strictly binary output, in which each switch is either open or closed. When placing two switches in sequence, both must be closed to close the circuit. This can be expressed by *and*: the first switch *and* the second switch have to be closed. If two switches are arranged in parallel, then it suffices if one of them is closed for the circuit to be closed, which correspondences to the mathematical *or*.

2.2.1 Boolean Algebras

By introducing Boolean algebras, we can capture this behavior in a mathematical framework. The definitions and results presented here can be found in most textbooks on Boolean algebras, e.g. [4].

Definition 2.7. *A Boolean algebra is a structure* $(A, +, \cdot, \bar{\ }, 0, 1)$ *with two binary operations* $+$ *and* $\cdot$, *a unary operation* $\bar{\ }$, *and two distinguished elements* 0 *and* 1 *such that for all* x, y *and* z *in* A *the following equations hold*

$$\begin{array}{lll}
\textit{(associativity)} & x + (y + z) = (x + y) + z, & x \cdot (y \cdot z) = (x \cdot y) \cdot z, \\
\textit{(commutativity)} & x + y = y + x, & x \cdot y = y \cdot x, \\
\textit{(absorption)} & x + (x \cdot y) = x, & x \cdot (x + y) = x, \\
\textit{(distributivity)} & x \cdot (y + z) = (x \cdot y) + (x \cdot z), & x + (y \cdot z) = (x + y) \cdot (x + z), \\
\textit{(complementation)} & x + \bar{x} = 1, & x \cdot \bar{x} = 0.
\end{array}$$

From these axioms one can derive many useful algebraic equations like the famous de Morgan's laws

$$\overline{(x + y)} = \overline{x} \cdot \overline{y}.$$

As usual, multiplication binds more strongly than addition, so $x \cdot y + z$ should be read as $(x \cdot y) + z$. Moreover, we often omit the operator for multiplication and write xy as a shorthand for $x \cdot y$.

One well known example is the two-element Boolean algebra $\mathbb{B} := \{0, 1\}$. Its operations are given by the table below.

x	y	$x + y$	$x \cdot y$	$\bar{x}$
0	0	0	0	1
0	1	1	0	1
1	0	1	0	0
1	1	1	1	0

x	y	z	$f(x,y,z)$	$g(x,y,z)$
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Table 1: Boolean functions defined by a truth table

By identifying 0 with *false* and 1 with *true*, we get a calculus of logic. Addition becomes the logical *or*, multiplication corresponds to *and*, and $\bar{x}$ is the *negation* of x. This should be familiar to readers with a background in computer science.

2.2.2 Boolean Functions

Digital circuits are built from many small logic gates. They perform logical operations and are connected to form a complex circuit. These logic gates correspond to mostly unary or binary Boolean functions. An example is the AND gate, which we can represent by the multiplication of the Boolean algebra $\mathbb{B}$. This is analogous to the interpretation of $\mathbb{B}$ as a calculus of logic. Another often used logic gate is the XOR gate, which, in the setting of $\mathbb{B}$, corresponds to addition modulo two. It is often also called the symmetric difference. We can define it in the language of Boolean algebras the following way:

$$x \oplus y := \bar{x}y + x\bar{y}.$$

Note that this definition works for any Boolean algebra and not just $\mathbb{B}$.

A truth or switching function is a function with signature $f : \mathbb{B}^n \to \mathbb{B}$ for some natural number $n \in \mathbb{B}$. There are 2^n different inputs to a truth function of n variables; it is therefore possible to define it by listing the function value at every input via a truth table, as shown in Table 1. Looking at the table, we can also see that a truth function of n variables is fully described by a binary vector of length 2^n. In our example the function g corresponds to the vector $(0,1,1,0,1,0,0,1)$. We can therefore identify the set of all truth functions in n variables with the set $\mathbb{B}^{2^n}$.

Defining a truth function by a Boolean expression is another possibility, as it is always possible to define the function using addition, multiplication, and negation (Theorem 4.3 of [7]). For example, the functions defined in Table 1 can be expressed as follows:

$$f(x,y,z) = z(x \oplus y) + xy.$$
$$g(x,y,z) = x \oplus y \oplus z.$$

Remember that the symmetric difference can be defined using addition, multiplication, and negation.

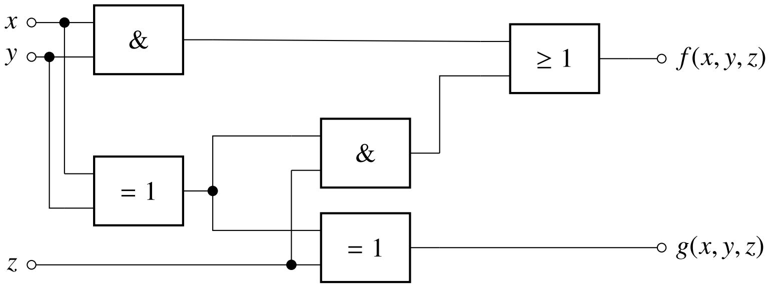

Figure 1: Schematic of the functions f and g

One advantage of this representation is that it forms a link to digital circuits. Different variables correspond to different signals and the logic operators correspond to logic gates. We can now draw a schematic of the circuit that represents the Boolean expression. In Table 1, the function f and g are drawn. The labeling is based on the European style, "&" stands for *and*, "= 1" stands for *xor*, and "≥ 1" stands for *or*. Note that, since both functions share the expression $x \oplus y$, we can "reuse" this part of the circuit.

This is not an arbitrary example, but in fact the schematic for a binary full adder. x and y are the operands, while z is the bit carried over from the previous stage. f produces the output carry and g the sum. By composing multiple full adders it is possible to add higher bit numbers.

Let X be an arbitrary set. By $\mathbb{B}^X$ we denote the set of all functions $h : X \to \mathbb{B}$. It is possible to define a Boolean algebra structure on $\mathbb{B}^X$. For the operators set $(p+q)(x) := p(x) + q(x)$, $(p \cdot q)(x) := p(x) \cdot q(x)$, and $\overline{p}(x) := \overline{p(x)}$ with $p, q \in \mathbb{B}^X$. The constants 0 and 1 correspond to the constant functions $0(x) = 0$ and $1(x) = 1$.

For example if $X = \{0, \ldots, n-1\}$, then this defines a Boolean algebra on tuples of elements from $\mathbb{B}$ of length n, where the operations are component-wise. As already argued, all truth functions in n variables can be identified by the set $\mathbb{B}^{2^n}$. Using the construction from before we obtain that the set of all truth functions of n variables is a Boolean algebra. More explicitly, let f and g be truth functions of n variables, then, as an example, $(f + g)(x) = f(x) + g(x)$.

2.2.3 Boolean Rings

In the previous sections we introduced the concept of Boolean algebras and their link to digital circuits. While it is possible to stay in the setting of Boolean algebras, we found it easier to work in the setting of Boolean rings.

Definition 2.8. *A Boolean ring is an unital ring R in which every element is idempotent. This means $r^2 = r$ for all $r \in R$.*

These conditions already imply a characteristic of two, meaning $r + r = 0$ for all $r \in \mathbb{R}$.

Proposition 2.9 (Proposition 1.27 of [4])**.** *There is one-to-one correspondence between Boolean rings and Boolean algebras. For a Boolean algebra $\mathcal{B} = (B, +, \cdot, \bar{}, 0, 1)$, let*

$$r\mathcal{B} = (B, \oplus, \cdot, 0, 1),$$

where $\oplus$ is the symmetric difference as defined before. For a Boolean ring $\mathcal{R} = (R, \oplus, \cdot, 0, 1)$, let

$$b\mathcal{R} = (R, +, \cdot, \bar{}, 0, 1),$$

where $x + y := x \oplus y \oplus xy$ and $\bar{x} := x \oplus 1$ for $x, y \in R$.

Let X be a set. The main example of a Boolean ring is $(\mathcal{P}(X), \triangle, \cap, \varnothing, X)$, where $\mathcal{P}(X)$ is the power set of X and $\triangle$ is the symmetric difference of sets, defined as $X_1 \triangle X_2 := (X_1 \backslash X_2) \cup (X_2 \backslash X_1)$. It is well known that the inclusion relation defines an order relation on the subsets. This idea can be generalized to Boolean rings the following way:

Definition 2.10. *Let R be a Boolean ring or Boolean algebra and $x, y \in R$. The canonical order relation is given by $x \leq y$ if $xy = x$.*

Let us return to the example of the power set ring $\mathcal{P}(X)$. Here the singleton sets, consisting of only one element from X, play a special role. They serve as a building block for every other element from $\mathcal{P}(X)$. Let $A \in \mathcal{P}(X)$, then it is possible to write A as the supremum of all singleton sets it encloses.

Definition 2.11. *Let R be a Boolean ring. An element $0 \neq a \in R$ is called atom if $y \leq a$ implies $a = y$ or $y = 0$ for every $y \in R$. Additionally, R is called atomic if there lies an atom below every non-zero element.*

As an example, finite Boolean rings are of a simple structure. Clearly, every finite Boolean ring is atomic. Moreover, the only defining property is the number of atoms.

Proposition 2.12 (Corollary 2.8 of [4])**.** *Let R be a finite atomic Boolean ring with n atoms, then R is isomorphic to the Boolean ring $\mathcal{P}(\{1, \dots, n\})$.*

We can construct an isomorphism between $\mathcal{P}(\{1, \dots, n\})$ and $\mathbb{B}^n$ by sending a subset A of $\{1, \dots, n\}$ to a binary vector $v_A := (\mathbb{1}_{i \in A})_{0<i\leq n}$ of length n. $\mathbb{1}_\phi$ is equal to one if the formula ϕ is true and else 0. The inverse is given by $(x_1, \dots, x_n) \mapsto \{i \mid x_i \neq 0\}$.

This allows us to phrase Proposition 2.12 in a slightly different language.

Proposition 2.13. *Let R be a finite atomic Boolean ring with n atoms, then $R \cong \mathbb{B}^n$ as rings. Moreover, a ring isomorphism is already given by a $\mathbb{B}$-vector space isomorphism. A $\mathbb{B}$-basis of R is given by the atoms.*

2.2.4 Boolean Differential Calculus

The field of Boolean differential calculus arose in the 1950s while studying changes of switching functions. Since then there has been a lot of research into the field. A recent textbook, which also covers numerous applications, is given by [8]. We briefly explore the Boolean partial derivative and its link to the analysis of error.

Definition 2.14. *Let $n \in \mathbb{N}$ and $f : \mathbb{B}^n \to \mathbb{B}$ be a switching function. The derivative of f with respect to the i-th coordinate $\delta_i(f)$, also called partial derivative, is given by*

$$\delta_i(f) \coloneqq f(x_1, \dots, x_i, \dots, x_n) \oplus f(x_1, \dots, \bar{x}_i, \dots, x_n)$$

One interesting question is whether a circuit is resistant to an erroneous input. Let f describe the circuit, then f is independent of x_i if and only if $\delta_i(f) = 0$. This way an error in the i-th input does not change the output of the circuit. More generally, $\delta_i(f)$ algebraically states the conditions in which an error in x_i causes an error at the output.

A generalization of the partial derivative is the so-called vectorial derivative. It is equal to 1 if the simultaneous change of a certain subset of variables changes the value of the function.

Definition 2.15 (Definition 2.2 of [8])**.** *Let $f : \mathbb{B}^n \to \mathbb{B}$ and $S \subseteq \{1, \dots, n\}$, then*

$$\delta_S(f) \coloneqq f(x_1, \dots, x_n) \oplus f(x_1 + \mathbb{1}_{1 \in S}, \dots, x_n + \mathbb{1}_{n \in S})$$

is the vectorial derivative of the function f with regard to S.

Given a partial or vectorial derivative δ, the map $\delta + \mathrm{id}$ is an involution of the Boolean ring of functions, see Proposition 9 of [9]. This observation leads to the following axiomatization in the language $\mathcal{L}_1$, consisting of the binary operators + and $\cdot$, the constant symbols 0 and 1, and the unary function δ.

Definition 2.16 (Definition 10 of [9])**.** *Let K be a Boolean ring and T_K a first-order theory of Boolean algebras expressed in the language of Boolean rings. Then T_1^K is the following theory in the language $\mathcal{L}_1$:*

1. *The axioms of Boolean rings,*
2. *$\sigma \coloneqq \delta + id$ is an involution of Boolean rings,*
3. $\ker(\delta) \models T_K$*,*
4. *δ is complete, i.e. $\exists z : \delta(z) = 1$.*

By Proposition 10 of [9], every model V of T_1^K is a free $\ker(\delta)$-module on two generators $(1, z)$. Moreover, the isomorphism classes of Boolean algebras K and models of T_1^K are in bijection by Proposition 11 of [9].

Let us see how these results play out in the case of $K = \mathbb{B}^2$. For the two models V and V' of T_1^K, we choose the ring of Boolean functions in two variables with elements given by Table 2. The derivative of V is δ_1 and the derivative of V' is chosen as δ_S, where S is the set $\{0, 1\}$. Firstly, we have to check that V and V' are indeed models of T_1^K. By directly calculating all the derivatives, we can find the constants and the preimages of 1.

	$\ker(\delta)$	$\delta^{-1}(1)$
V	$\{f_0, f_5, f_{10}, f_{15}\}$	$\{f_3, f_6, f_9, f_{12}\}$
V'	$\{f_0, f_6, f_9, f_{15}\}$	$\{f_3, f_5, f_{10}, f_{12}\}$

x_0	x_1	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Table 2: Logic functions of two variables

In both cases, the preimage of 1 is not empty. For example, $\delta_1^{-1}(1)$ is the set of switching functions which are linear in x_1. Thus, a change in x_1 will always change the output of the function. Moreover, the kernels each form a four-element Boolean algebra, thus they are isomorphic. Finally, an isomorphism F of $\mathcal{L}$-structures from V to V' can be given as follows. In both cases we consider the models as free ker(δ)-modules with generators (f_{15}, f_3).

$$\begin{array}{llll}
f_0 \mapsto f_0, & f_4 \mapsto f_4, & f_8 \mapsto f_8, & f_{12} \mapsto f_{12}, \\
f_1 \mapsto f_2, & f_5 \mapsto f_6, & f_9 \mapsto f_{10}, & f_{13} \mapsto f_{14}, \\
f_2 \mapsto f_1, & f_6 \mapsto f_5, & f_{10} \mapsto f_9, & f_{14} \mapsto f_{13}, \\
f_3 \mapsto f_3, & f_7 \mapsto f_7, & f_{11} \mapsto f_{11}, & f_{15} \mapsto f_{15}.
\end{array}$$

We can check by hand if this defines an isomorphism between models of T_1^K, but the following result gives us an easier way:

Proposition 2.17. *Let $\mathcal{L}_1$ be the first-order language of Definition 2.16 enriched by a new constant symbol z. An isomorphism F of models A and B of T_1^k is given by an isomorphism of Boolean rings which also respects z pointwise and the constants setwise.*

Proof. For clarity, we will index the symbols of our language with the structure in which they are interpreted in. Let $x \in A$. There are $k, k' \in \ker(\delta_A)$ with $x = k + k'z_A$.

$$F(\delta_A(k + k'z_A)) = F(k') = \delta_B(F(k')z_B) \overset{F(k)\in\ker(\delta_B)}{=} \delta_B(F(k'z_A) + F(k)) = \delta_B(F(k + k'z_A))$$

This shows that F respects δ. Moreover, since the only relation symbol in our signature is equality, F already is an isomorphism. □

An axiomatization up to isomorphism allows for simpler reasoning. If we, for example, want to show some property that is preserved under isomorphism for all vectorial derivatives, it already suffices to prove it for the simpler partial derivative with respect to the first coordinate. Therefore, any such property transfers to any other derivative that falls under the axiomatization.

We will now narrow our focus to the case where K is an infinite atomic Boolean algebra. This has two reasons. Firstly, it is well known that the theory of infinite atomic Boolean algebras is complete and consequently, by Theorem 2 of [9], T_1^K is also complete. Secondly, the following result makes a link between T_1^K and switching functions of finite variables. In real world scenarios we deal with finite circuits, so this is especially interesting. Let $\mathbb{S}_n$ be the Boolean ring of switching functions in n variables. By equipping $\mathbb{S}_n$ with one of the already discussed Boolean derivatives, $\mathbb{S}_n$ becomes an $\mathcal{L}_1$-structure.

Proposition 2.18 (Theorem 6 of [9])**.** *Let $\varphi \in T_1^K$ for an infinite atomic Boolean algebra K. There is an $N \in \mathbb{N}$ such that $\mathbb{S}_n \models \varphi$ for all $n \geq N$.*

If we formulate a property of digital circuits as a sentence in the language $\mathcal{L}_1$, and it is derivable from the theory, it also holds for all sufficiently large circuits. More on this in the last section.

3 Quantifier Elimination

Let $\mathcal{L}_1'$ be the first-order language consisting of the binary operators $+$ and $\cdot$, the constant symbols 0, 1, and z, the unary function δ, and relation symbols C_n for $n \in \mathbb{N}$. Note that $\mathcal{L}_1'$ is an extension of the language $\mathcal{L}_1$ given in Definition 2.16. In this section we prove the following statement:

Proposition 3.1. *Let K be an infinite atomic Boolean ring and T_K a first-order theory of infinite atomic Boolean algebras expressed in the language of Boolean rings. Θ_1^K is the following theory in the language $\mathcal{L}_1'$:*

1. *The axioms of a Boolean ring,*
2. *$\sigma := \delta + id$ is an involution of Boolean rings,*
3. $\ker(\delta) \models T_K$*,*
4. *δ is complete, i.e. $\delta(z) = 1$,*
5. *for every $n \in \mathbb{N}$, $C_n(x)$ if and only if there are at least n atoms below x.*

Θ_1^K admits quantifier elimination.

The following result is used in the proof of Proposition 3.1:

Proposition 3.2. *Let V be a model of T_1^K for an atomic Boolean ring K, then V is an atomic Boolean ring. Its atoms are precisely of the form ηz or $\eta\bar{z}$ with η an atom of K.*

Proof. It was already discussed that V is a Boolean ring, so it remains to show that V is atomic. Let $0 \neq x \in V$. Since V is a K-module on two generators $(1, z)$, we can write $x = \eta + \delta(x)z$ for some $\eta \in \ker(\delta)$. Depending on the form of x, we construct an atom of V below x.

Case 1: $\eta = 0$.

K is atomic by assumption. Moreover, since $\delta(x) \in K$, we can pick an atom ζ of K below $\delta(x)$. We claim that the element ζz is an atom of V below x. Firstly, ζz

lies below x as $\zeta z x = \zeta \eta z^2 = \zeta z$. Secondly, ζz is an atom of V. Let $y \in V$ with $y = \eta' + \delta(y) z$ for some $\eta' \in K$. The products $\zeta \eta'$ and $\zeta \delta(y)$ are either zero or equal to ζ because ζ is an atom of K. Now if ζ is below both η' and $\delta(y)$ or none, then $\zeta z y = 0$ and otherwise $\zeta z y = \zeta z$. This precisely means that ζz is an atom of V.

Case 2: $\eta \neq 0$.

Choose an atom ζ of K below η. This especially means $\zeta \neq 0$. ζ intersects non-trivially with $\bar{z}$, else we get the following contradiction:

$$0 = \delta(0) = \delta(\zeta \bar{z}) = \delta(\zeta + \zeta z) = \zeta \delta(1) + \zeta \delta(z) = \zeta.$$

The product $\zeta \bar{z}$ is smaller or equal to x by construction. To show that $\zeta \bar{z}$ is an atom of V, let $y = \eta' + \delta(y) z$ as in Case 1. Similar to above, it holds

$$\zeta \bar{z} y = \zeta \eta' \bar{z} = \begin{cases} \zeta \bar{z} & \text{if } \zeta \leq \eta', \\ 0 & \text{else.} \end{cases}$$

The same argument shows that γz and $\gamma \bar{z}$ are atoms of V for all atoms γ of K. Lastly, all atoms have to be of this form. Let x be an atom of V. By the construction above, we can find a nonzero element of the desired form below x. Therefore, x has to be equal to this element. □

We can now proceed to prove Proposition 3.1.

Proof. The proof uses Proposition 2.6, therefore let $\mathbb{B}_1$ and $\mathbb{B}_2$ be two ω-saturated models of Θ^1_K. Proposition 3.2 shows that $\mathbb{B}_1$ and $\mathbb{B}_2$ are atomic. Next, we pick a tuple of elements $\vec{\alpha}$ from $\mathbb{B}_1$ and a tuple of elements $\vec{\beta}$ of the same length from $\mathbb{B}_2$ such that $(A, \vec{\alpha}) \equiv_0 (B, \vec{\beta})$. We have to show that $(A, \vec{\alpha})$ and $(B, \vec{\beta})$ are back-and-forth equivalent. Let R_1 denote the smallest substructure of $\mathbb{B}_1$ containing $\vec{\alpha}$ and $R_2 := \langle \vec{\beta} \rangle_{\mathbb{B}_2}$ analogously. By Proposition 2.1, there is an isomorphism of $\mathcal{L}$-structures

$$F : R_1 \to R_2$$

with $F\vec{\alpha} = \vec{\beta}$.

To construct the back-and-forth system, let $\alpha \in \mathbb{B}_1 \backslash R_1$. If we can find a $\beta \in \mathbb{B}_2 \backslash R_2$ such that we can extend the isomorphism F to $F' : \langle \vec{\alpha}\alpha \rangle_{\mathbb{B}_1} \to \langle \vec{\beta}\beta \rangle_{\mathbb{B}_2}$ with $F'(\vec{\alpha}\alpha) = \vec{\beta}\beta$, then by Proposition 2.1 $(A, \vec{\alpha}\alpha) \equiv_0 (B, \vec{\beta}\beta)$. In the proof, we make no further assumption about $\vec{\alpha}$, $\vec{\beta}$, and α, thus showing the back-and-forth equivalence as we can iterate this argument and even reverse the roles of α and β.

The following function, which counts the number of atoms below an element, is used throughout the proof:

$$\#(x) = \begin{cases} n & \text{if } C_n(x) \wedge \neg C_{n+1}(x) \\ \infty & \text{if no such } n \text{ exists} \end{cases}.$$

Any morphism respecting all predicates C_n also preserves $\#(\_)$.

We start by giving a better description of $R_1\langle \alpha \rangle := \langle \vec{\alpha}\alpha \rangle_{\mathbb{B}_1}$. By assumption, $\mathbb{B}_1$ is a free $\ker(\delta)$ module on two generators $(1, z)$, so there is $\rho \in \ker(\delta)$ such that $\alpha = \rho + \delta(\alpha) z$.

Claim 1. *$R_1\langle\alpha\rangle$ is a free* $\ker(\delta) \cap R_1\langle\alpha\rangle$ *module on two generators* $(1, z)$.

Proof. Let $x \in R_1\langle\alpha\rangle$. There is $\eta \in \ker(\delta)$ such that $x = \eta + \delta(x)z$. If $\eta, \delta(x)$ are already elements of $R_1\langle\alpha\rangle$, then $(1, z)$ is a generating set of $R_1\langle\alpha\rangle$. Linear independence is inherited from the module structure on $\mathbb{B}_2$. $R_1\langle\alpha\rangle$ is closed under δ, so it holds that $\delta(x) \in S$. Furthermore, $\delta(x)z \in R_1\langle\alpha\rangle$, as z is part of the signature. This additionally shows $\eta \in R_1\langle\alpha\rangle$, concluding the proof. □

Claim 1 demonstrates that all new elements from $\ker(\delta)$ which we add are created by $\rho, \delta(\alpha)$, and elements from $R_1 \cap \ker(\delta)$. Conclusively,

$$R_1\langle\alpha\rangle = \{\, r + s_1\rho + s_2\delta(\alpha) + s_3\rho\delta(\alpha) \mid r, s_1, s_2, s_3 \in R_1 \,\}.$$

From the characterization of $R_1\langle\alpha\rangle$ and a simple inductive argument, we can see that $R_1\langle\alpha\rangle$ is finite. Indeed, if $\vec{\alpha}$ is the empty vector, then $R_1 = \{\, 0, z, \bar{z}, 1 \,\}$ and when adding α, $R_1\langle\alpha\rangle$ stays finite. As a result, $R_1\langle\alpha\rangle$ is atomic.

There are finitely many atoms of $R_1\langle\alpha\rangle$ not in R_1. We get from R_1 to $R_1\langle\alpha\rangle$ by successive adjoins of those atoms. Adjoining an element means creating the smallest substructure containing the new element. Without loss of generality, assume that α is an atom of $R_1\langle\alpha\rangle$.

Claim 2. *α is either of the form $\alpha = \delta(\alpha)z$ or $\alpha = \delta(\alpha)\bar{z}$.*

Proof. First assume $\rho\delta(\alpha) = 0$, then $\alpha\delta(\alpha)z = \rho\delta(\alpha)z + \delta(\alpha)^2z = \delta(\alpha)z$. Since α is atomic, either $\delta(\alpha)z = 0$ or $\alpha = \delta(\alpha)z$. The case $\delta(\alpha)z = 0$ is not possible, as is shown in the following. Assume $\delta(\alpha)z = 0$, implying $\alpha = \rho$. Now ρ is atomic, so $\rho z \in \{\, 0, \rho \,\}$. Remember that $\rho \in \ker(\delta)$, so after applying δ we get $\rho = 0$, a contradiction to $\alpha \neq 0$. This shows $\alpha = \delta(\alpha)z$ as desired.

Now assume $\rho\delta(\alpha) \neq 0$. We first show that $\rho\delta(\alpha)\bar{z}$ lies below α and is nonzero. Firstly, $\alpha\rho\delta(\alpha)\bar{z} = (\rho + \delta(\alpha)z)\rho\delta(\alpha)\bar{z} = \rho\delta(\alpha)\bar{z}$. It remains to prove $\rho\delta(\alpha)\bar{z} \neq 0$. Assume otherwise. Applying δ on the equation yields $\rho\delta(\alpha) = 0$, a contradiction. Therefore, $\alpha = \rho\delta(\alpha)\bar{z}$ as α is atomic by assumption. Finally, $\delta(\alpha) = \delta(\rho\delta(\alpha)\bar{z}) = \rho\delta(\alpha)$, which concludes the proof. □

We can observe that Claim 2 is equivalent to the statement ”either $\rho = 0$ or $\rho = \delta(\alpha)$”. This way, simpler description of $R_1\langle\alpha\rangle$ can be given:

$$R_1\langle\alpha\rangle = \{\, r + s\delta(\alpha) \mid r, s \in R_1 \,\}.$$

It is possible to ”resolve” the case distinction in Claim 2 with the help of the following result:

Claim 3. *Both $\delta(\alpha)z$ and $\delta(\alpha)\bar{z}$ are atoms of $R_1\langle\alpha\rangle$.*

Proof. Let $x \in R_1\langle\alpha\rangle$. There is $\eta \in \ker(\delta)$ s.t. $x = \eta + \delta(x)z$. Claim 2 implies that $\delta(\alpha)z$ or $\delta(\alpha)\bar{z}$ is atomic. Firstly, assume that $\delta(\alpha)z$ is an atom.

$$x\delta(\alpha)\bar{z} = (\eta + \delta(x)z)(\delta(\alpha) + \delta(\alpha)z) = \eta\delta(\alpha) + \eta\delta(\alpha)z.$$

Either $\eta\delta(\alpha)z = 0$ or $\eta\delta(\alpha)z = \delta(\alpha)z$ because $\delta(\alpha)z$ is an atom of $R_1\langle\alpha\rangle$ and $\eta, \delta(x) \in R_1\langle\alpha\rangle$. In the first case, it also holds that $\eta\delta(\alpha) = 0$, which results in $x\delta(\alpha)\bar{z} = 0$. In the second case, we have $\eta\delta(\alpha) = \delta(\alpha)$, showing $x\delta(\alpha)\bar{z} = \delta(\alpha)\bar{z}$ as desired.

The same argument works if $\delta(\alpha)\bar{z}$ is an atom, just note that $x = (\eta + \delta(x)) + \delta(x)\bar{z}$ with $\eta + \delta(x) \in \ker(\delta)$, consider $x\delta(\alpha)z = x(\delta(\alpha) + \delta(\alpha)\bar{z})$, and work through the same steps. □

Claim 4. *$\delta(\alpha)z$ and $\delta(\alpha)\bar{z}$ lie below different, unique atoms γz and $\gamma'\bar{z}$ of R_1 respectively.*

Proof. If not, then there is an atom μ of R_1 such that $0 \neq \mu\delta(\alpha)z < \delta(\alpha)z$ - a contradiction. The same argument works for $\delta(\alpha)\bar{z}$. Claim 2 also shows us that all atoms of R_1 are of the kind μz or $\mu\bar{z}$ with $\mu \in \ker(\delta)$. Thus, the two unique atoms above $\delta(\alpha)z$ and $\delta(\alpha)\bar{z}$ are of this form. □

We can now characterize all atoms of $R_1\langle\alpha\rangle$. Let γz and $\gamma'\bar{z}$ be as in Claim 4, then the new atoms of $R_1\langle\alpha\rangle$ are

- the atoms of R_1 distinct from γz and $\gamma'\bar{z}$ denoted by the set A,
- $\delta(\alpha)z$ and $\overline{\delta(\alpha)}\gamma z$, its complement in γz,
- $\delta(\alpha)\bar{z}$ and $\overline{\delta(\alpha)}\gamma'\bar{z}$, its complement in $\gamma'\bar{z}$.

First, we characterize $\beta \in \mathbb{B}_2$ such that we can extend F to an isomorphism $F' : R_1\langle\alpha\rangle \to R_2\langle\beta\rangle$ with $F'(\vec{\alpha}\alpha) = \vec{\beta}\beta$ and then argue that it exists. Since $\delta(\alpha)z$ and $\delta(\alpha)\bar{z}$ are atoms of $R_1\langle\alpha\rangle$, $\delta(\beta)z$ and $\delta(\beta)\bar{z}$ must be atoms of $R_2\langle\beta\rangle$ as well. This already forces the following two conditions:

1. $0 < \delta(\beta)z < F(\gamma)z$,
2. $0 < \delta(\beta)\bar{z} < F(\gamma')\bar{z}$.

Claim 5. *Conditions 1 and 2 already define an isomorphism of Boolean rings*

$$F' : R_1\langle\alpha\rangle \to R_2\langle\beta\rangle$$

with $F(\vec{\alpha}\alpha) = \vec{\beta}\beta$.

Proof. First note $R_1\langle\alpha\rangle$ and $R_2\langle\beta\rangle$ are isomorphic, since they have the same number of atoms. By Proposition 2.13, we can define a homomorphism of atomic Boolean rings by giving images of the atoms. For η an atom of $R_1\langle\alpha\rangle$, set

$$F'(\eta) = \begin{cases} F(\eta) & \text{for } \eta \in A \\ \delta(\beta)z & \text{for } \eta = \delta(\alpha)z \\ \delta(\beta)\bar{z} & \text{for } \eta = \delta(\alpha)\bar{z} \end{cases}.$$

By construction of $\delta(\beta)$, the images of the atoms of $R_1\langle\alpha\rangle$ are pairwise different atoms of $R_2\langle\beta\rangle$. This way, F' is an isomorphism and $F'(\alpha) = \beta$ as desired. □

From now on, F refers to $F : R_1 \to R_2$ or its extension to $R_1\langle\alpha\rangle$. It is clear from context which one is referred to.

To use Proposition 2.17 it needs to hold that $\delta(\beta) \in \ker(\delta)\backslash R_2$. Additionally, F needs to respect $\#(\_)$. Note that every element x of $R_1\langle\alpha\rangle$ can be uniquely represented in the form

$$x = \epsilon_1\delta(\alpha)z + \epsilon_2\overline{\delta(\alpha)}\gamma z + \epsilon_3\delta(\alpha)\bar{z} + \epsilon_4\overline{\delta(\alpha)}\gamma'\bar{z} + \sum_{\tau\in A}\epsilon_\tau\tau,$$

where each ϵ_i is either 0 or 1. All summands are pairwise disjoint, so $\#(\_)$ is compatible with the sum

$$\#(x) = \epsilon_1\#(\delta(\alpha)z) + \epsilon_2\#(\overline{\delta(\alpha)}\gamma z) + \epsilon_3\#(\delta(\alpha)\bar{z}) + \epsilon_4\#(\overline{\delta(\alpha)}\gamma'\bar{z}) + \sum_{\tau\in A}\epsilon_\tau\#(\tau).$$

For F to respect $\#(\_)$, the following conditions suffice:

3. $\#(\delta(\beta)z) = \#(\delta(\alpha)z)$,

4. $\#(\overline{\delta(\beta)}F(\gamma)z) = \#(\overline{\delta(\alpha)}\gamma z)$,

5. $\#(\delta(\beta)\bar{z}) = \#(\delta(\alpha)\bar{z})$,

6. $\#(\overline{\delta(\beta)}F(\gamma')\bar{z}) = \#(\overline{\delta(\alpha)}\gamma'\bar{z})$.

We have to find $\delta(\beta)z$ and $\delta(\beta)\bar{z}$ according to the conditions mentioned above to get $\delta(\beta) = \delta(\beta)z + \delta(\beta)\bar{z}$. Then we can set $\beta := \delta(\beta)z$ or $\beta := \delta(\beta)\bar{z}$, depending on the form of α. We do this by choosing atoms below γz and $\gamma'\bar{z}$. Note that, since they are disjoint, we can consider the construction of $\delta(\beta)z$ and $\delta(\beta)\bar{z}$ independently. Thus, we only discuss the construction of $\delta(\beta)z$, as $\delta(\beta)\bar{z}$ works analogously.

Case 1: At least one of $\#(\delta(\alpha)z)$ and $\#(\overline{\delta(\alpha)}\gamma z)$ is finite.

W.l.o.g., assume $\#(\delta(\alpha)z) < \infty$. Now choose $\#(\delta(\alpha)z)$ atoms of $\mathbb{B}_2$ below $F(\gamma)z$ and set $\delta(\beta)z$ as their sum. Note that, by Claim 3.2, these atoms are of the form θz for $\theta \in \ker(\delta)$. $\#(\overline{\delta(\beta)}F(\gamma)z) = \#(\overline{\delta(\alpha)}\gamma z)$ then follows automatically since $\#(\gamma z) = \#(F(\gamma)z)$ by assumption.

Case 2: Both $\#(\delta(\alpha)z)$ and $\#(\overline{\delta(\alpha)}\gamma z)$ are infinite.

We want to show that the following set of $\mathcal{L}(R_2)$ formulas defines a 1-type of R_2 over $\mathbb{B}_2$,

$$\mathcal{X} := \{\, C_n(xz), C_n(\bar{x}c_\gamma z) \mid n \in \mathbb{N} \,\} \cup \{\, xz \neq c_r \neq \bar{x}c_\gamma z \mid r \in R_2 \,\} \cup \{\, \delta(x) = 0 \,\}.$$

Therefore, we have to confirm that $\mathcal{X} \cup \mathrm{Th}_{R_2}(\mathbb{B}_2)$ is satisfiable, which we will do using compactness. Let $\mathcal{X}[c]$ be the set of formulas in the language $\mathcal{L}(R_2, c)$, where every occurrence of the free variable x in $\mathcal{X}$ is replaced by the new constant symbol c. Take a finite subset of $\mathrm{Th}_{R_2}(\mathbb{B}_2) \cup \mathcal{X}[c]$. There is a maximal natural number m such that there are no formulas $C_n(cz)$ and $C_n(\bar{c}c_\gamma z)$ in this subset for $n \geq m$. By assumption, there are infinite atoms below γ, so take m atoms below

γ and interpret c as the sum of these atoms. This way $\mathbb{B}_2$, models this subset of formulas and, by the compactness theorem, $\mathrm{Th}_{R_2}(\mathbb{B}_2) \cup \mathcal{X}[c]$ has a model. Since $\mathbb{B}_2$ is ω-saturated and R_2 is finite, $\mathbb{B}_2$ already realizes this 1-type, which we choose as $\delta(\beta)z$. By the construction of $\mathcal{X}$ and the choice of $\delta(\beta)$, it holds that $\#(\overline{\delta(\beta)}F(\gamma)z) = \infty$.

Putting it all together, we find $\beta \in \mathbb{B}_2$ such that we can extend F to an isomorphism $F' : R_1\langle\alpha\rangle \to R_2\langle\beta\rangle$, with $F(\vec{\alpha}\alpha) = \vec{\beta}\beta$. This way, $(\mathbb{B}_1, \vec{\alpha})$ and $(\mathbb{B}_2, \vec{\beta})$ are back-and-forth equivalent. Using Proposition 2.6, the theory Θ_1^K has quantifier elimination. □

4 Conclusion

4.1 Summary

In this thesis we proved that the theory Θ_1^K of Definition 3.1 admits quantifier elimination. This was done by a standard back-and-forth argument. Firstly, we had to identify the atoms of finitely generated substructures of models of T_1^K. We found that these atoms can be nicely described by z and elements of K. Using this description, it was possible to build a back-and-forth system between two ω-saturated models of T_1^K. Finally, Proposition 2.6 concluded the proof.

4.2 Applications and Future Work

An interesting byproduct of the proof is the description of the atoms in substructures A of a model V of T_1^K. Claim 1 tells us that A is a free $\ker(\delta) \cap A$-module. Moreover, the same proof as in Proposition 3.2 tells us what the atoms look like. Every atom of R is precisely of the form ηz or $\eta\bar{z}$ with η an atom of $\ker(\delta) \cap R$. In the special case where $R = V$, this is exactly the statement of Proposition 3.2.

Additionally, if R is finitely generated by a tuple of elements $\vec{\alpha}$, we can explicitly calculate the atom without completely describing R. Start with the simplest substructure created by the empty tuple - the ring $\{0, z, \bar{z}, 1\}$. Here the atoms are clearly z and $\bar{z}$. Proceed inductively. Assume we know all atoms of $\langle(\alpha_1, \ldots, \alpha_i)\rangle_V$ denoted by A, with i a natural number smaller than the length of $\vec{\alpha}$. Now calculate all products $\eta\delta(\alpha_{i+1})$ for $\eta \in A$. There are some products which are not equal to zero. Each such product is of either the form $\eta\delta(\alpha_{i+1})z$ or $\eta\delta(\alpha_{i+1})\bar{z}$ for some $\eta \in A$. Remove ηz or $\eta\bar{z}$ from A and add $\eta\delta(\alpha_{i+1})z, \eta\overline{\delta(\alpha_{i+1})}z$ or $\eta\delta(\alpha_{i+1})\bar{z}, \eta\overline{\delta(\alpha_{i+1})}\bar{z}$ accordingly. We can iterate this step until all atoms of R are described.

It was already sketched how the result of quantifier elimination might be applied to real world applications. We now explore this in a bit more depth. Assume we are given a first-order sentence in the language $\mathcal{L}_1$. This sentence ϕ can use quantifiers and therefore describe properties about a whole class of switching functions. Quantifier elimination guarantees the existence of a quantifier-free sentence $\tilde{\phi}$, which is equivalent to ϕ in all models of Θ_1^K. Deciding this quantifier-free sentence is a much easier task than deciding an arbitrary sentence. If this property holds in any model of Θ_1^K, then it holds in all rings of switching functions of a certain size by Proposition 2.18. An open question that still has to be addressed is how one can algorithmically find the $\tilde{\phi}$. This remains work for further research.

5 References

[1] Jamshid Derakhshan and Angus Macintyre. Enrichments of boolean algebras by presburger predicates. *Fundamenta Mathematicae*, 239, 01 2017.

[2] C. Ward Henson. Model theory. `https://people.math.sc.edu/mcnulty/modeltheory/Henson.pdf`, 2010. [Online; accessed 14-august-2023].

[3] Wilfrid Hodges. *Model Theory*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1993.

[4] S. Koppelberg and R. Bonnet. *Handbook of Boolean Algebras: Vol. 1*. Elsevier, 1989.

[5] David Marker. *Model Theory*, volume 217 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[6] Claude Elwood Shannon. *A symbolic analysis of relay and switching circuits*. Thesis, Massachusetts Institute of Technology, 1940.

[7] Bernd Steinbach and Christian Posthoff. Logic Functions. In Bernd Steinbach and Christian Posthoff, editors, *Logic Functions and Equations: Fundamentals and Applications using the XBOOLE-Monitor*, pages 117–191. Springer International Publishing, Cham, 2022.

[8] Bernd Steinbach, Christian Posthoff, and Mitchell A. Thornton. *Boolean Differential Calculus*. Morgan & Claypool Publishers, May 2017.

[9] Felix Weitkämper. Axiomatizing boolean differentiation. In Rolf Drechsler and Daniel Große, editors, *Recent Findings in Boolean Techniques*, pages 83–104. Springer International Publishing, 2021.