Technische Universität Wien

SEMINAR PAPER

Boolean Equations

Raphael Gruber
Matriculation Number: 12211890

Supervisor:

Associate Prof. Dipl.-Ing. Dr.techn. Stefan Hetzl

Vienna, April 3, 2025

Contents

1 Introduction

This seminar paper aims to provide an overview of the theory of solving a special type of equations where the unknowns are elements of a Boolean algebra of arbitrary nature. The results and techniques we present are strongly based on [Rud74], making this paper a summary of the first two chapters of that book. The paper focuses on showcasing only the main definitions and results necessary to understand the solution theory contained in the referenced book.

The equations we are interested in are called *Boolean equations*. An example of a system of Boolean equations is

$$\begin{aligned} x_1 \cap x_2 &= a \\ x_1 \cup x_2 &= b \end{aligned} \tag{1.1}$$

where x_1, x_2 are unknown variables and a, b are given elements of a Boolean. The goal is to find all possible assignments of elements of the Boolean algebra we work in to the variables x_1, x_2, such that both equations are satisfied.

The paper is structured as follows: In Chapter 2, we introduce the basic definitions and tools to work with Boolean equations. In Chapter 3, we present the solution theory for Boolean equations and show how to find all solutions to a given system of Boolean equations.

2 Defining Boolean Equations

This chapter will begin by reviewing the definition of a Boolean algebra and then proceed to define and analyze Boolean functions. The chapter concludes with a definition of Boolean equations, their solutions and a way to bring any Boolean equation or system of equations into a standardized form.

2.1 Boolean Algebras

We build the structure of a Boolean algebra starting from more general algebraic structures, inspired by the approach taken by [Pin24]. In the following definitions, we will use the notation $\mathfrak{A} = (A, (f_i)_{i \in I})$ to denote an algebra $\mathfrak{A}$ with carrier set A and operations $(f_i)_{i \in I}$, as usual in abstract algebra. Each operation is a function $f_i : A^{n_i} \to A$ where $n_i \in \mathbb{N}$ is the arity of the operation. An operation of arity zero (a nullary operation) is a constant function that takes no inputs and can be seen as a distinct element of A. The signature of an algebra is the tuple $(n_i)_{i \in I}$ of all arities.

Definition 2.1. Let $\mathfrak{A} = (A, \cup)$ be an algebra of signature (2). $\mathfrak{A}$ is a ***commutative semigroup*** if and only if the operation $\cup$ is associative and commutative, or more specific, if the following equations hold for all $x, y, z \in A$:

$$x \cup (y \cup z) = (x \cup y) \cup z$$
$$x \cup y = y \cup x$$

Definition 2.2. Let $\mathfrak{L} = (L, \cup, \cap)$ be an algebra of signature $(2, 2)$. $\mathfrak{L}$ is a ***lattice*** if and only if the following conditions are satisfied:

1. $(L, \cup)$ and $(L, \cap)$ are commutative semigroups.
2. The absorption laws hold for all $x, y \in L$:

$$x \cap (x \cup y) = x$$
$$x \cup (x \cap y) = x$$

Definition 2.3. Let $\mathfrak{L} = (L, \cup, \cap)$ be a lattice. $\mathfrak{L}$ is a ***distributive lattice*** if and only if $\cup$ and $\cap$ distribute over each other, that is for all $x, y, z \in A$ the following equations hold:

$$x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$$
$$x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$$

Definition 2.4. Let $\mathfrak{L} = (L, \cup, \cap, 0, 1)$ be an algebra of signature $(2, 2, 0, 0)$. $\mathfrak{L}$ is a ***bounded lattice*** if and only if the following conditions are satisfied:

1. $(L, \cup, \cap)$ is a lattice.
2. The following equations hold for all $x \in L$:

$$x \cap 0 = 0$$
$$x \cup 1 = 1$$

Definition 2.5. Let $\mathfrak{L} = (L, \cup, \cap, \bar{\cdot}, 0, 1)$ be an algebra of signature $(2, 2, 1, 0, 0)$. $\mathfrak{L}$ is a ***complemented lattice*** if and only if the following conditions are satisfied:

1. $(L, \cup, \cap, 0, 1)$ is a bounded lattice.
2. The following equations hold for all $x \in L$:

$$x \cap \overline{x} = 0$$
$$x \cup \overline{x} = 1$$

Remark 2.6. We can combine the different variants of lattices by extending the above definitions to algebras with more operations. For example, it should be clear that a ***distributive bounded lattice*** is a bounded lattice $(L, \cup, \cap, 0, 1)$ where $(L, \cup, \cap)$ is a distributive lattice.

Definition 2.7 (Boolean Algebra)**.** An algebra $\mathfrak{B} = (B, \cup, \cap, \bar{\cdot}, 0, 1)$ of signature $(2, 2, 1, 0, 0)$ is a ***Boolean algebra*** if and only if $\mathfrak{B}$ is a distributive complemented lattice.

Example 2.8. The smallest possible Boolean algebra is given by $(\{0, 1\}, \vee, \wedge, \neg, 0, 1)$ where $\vee, \wedge, \neg$ are the common logical operations on the truth values 0 and 1. We will denote this algebra as B_2.

In our proofs we will often use the following properties or "rules of computation" that hold in any Boolean algebra.

Lemma 2.9. Let $(B, \cup, \cap, \bar{\cdot}, 0, 1)$ be a Boolean algebra. Then the following statements hold for all $x, y, z \in B$:

$$x \cap x = x \tag{2.1}$$
$$x \cup x = x \tag{2.2}$$
$$x \cap 1 = x \tag{2.3}$$
$$x \cup 0 = x \tag{2.4}$$
$$x \cap y = 1 \iff x = y = 1 \tag{2.5}$$
$$x \cup y = 0 \iff x = y = 0 \tag{2.6}$$
$$x \cap y = 0 \wedge x \cup y = 1 \iff y = \overline{x} \tag{2.7}$$
$$\overline{x \cap y} = \overline{x} \cup \overline{y} \tag{2.8}$$
$$\overline{x \cup y} = \overline{x} \cap \overline{y} \tag{2.9}$$
$$\overline{\overline{x}} = x \tag{2.10}$$
$$\overline{0} = 1 \tag{2.11}$$
$$\overline{1} = 0 \tag{2.12}$$
$$(x \cap \overline{y}) \cup (\overline{x} \cap y) \cup (x \cap y) = x \cup y \tag{2.13}$$

Proof. We will only prove the statements (2.11) to (2.13). For proof of the other equations see [Rud74, Theorem 1.2].

(2.11,2.12) We have $0 \cup 1 = 1$ and $0 \cap 1 = 0$ by the unit laws. With (2.7) we get $\overline{0} = 1$ and $\overline{1} = 0$.

(2.13) A simple calculation using (2.3) shows that

$$\left(a \cap \overline{b}\right) \cup \underbrace{(\overline{a} \cap b) \cup (a \cap b)}_{=(\overline{a} \cup a) \cap b = 1 \cap b = b} = \left(a \cap \overline{b}\right) \cup b = (a \cup b) \cap \left(\overline{b} \cup b\right) = a \cup b$$

holds.

□

Definition 2.10. For $x, y \in B$ we define the binary relation $\subseteq$ by

$$x \subseteq y :\Longleftrightarrow x \cup y = y.$$

Lemma 2.11. Let $(B, \cup, \cap, \bar{\cdot}, 0, 1)$ be a Boolean algebra. Then the following statements hold for all $x, y, z, a, b \in B$:

$$x \subseteq x \tag{2.14}$$
$$x \subseteq y \wedge y \subseteq x \Longleftrightarrow x = y \tag{2.15}$$
$$x \subseteq y \wedge y \subseteq z \Longrightarrow x \subseteq z \tag{2.16}$$
$$x \subseteq y \Longleftrightarrow x \cap z \subseteq y \cap z \tag{2.17}$$
$$x \subseteq y \Longleftrightarrow x \cap y = x \tag{2.18}$$
$$x \subseteq y \Longleftrightarrow x \cap \overline{y} = 0 \tag{2.19}$$
$$0 \subseteq x \tag{2.20}$$
$$x \subseteq 0 \Longrightarrow x = 0 \tag{2.21}$$
$$x \subseteq y \wedge a \subseteq b \Longrightarrow x \cup a \subseteq y \cup b \tag{2.22}$$

Proof. Again we will only prove some statements, the other statements can be found in [Rud74, Theorem 1.3].

(2.21) By our assumption we have $x \subseteq 0$, by (2.20) we have $0 \subseteq x$. We can conclude with (2.15) that $x = 0$.

(2.22) A simple calculation under the assumptions $x \subseteq y$ and $a \subseteq b$ yields

$$x \cup a \cup y \cup b = (x \cup y) \cup (a \cup b) = y \cup b,$$

so by definition $x \cup a \subseteq y \cup b$.

□

Remark 2.12. The properties (2.14) to (2.16) show that $\subseteq$ is a partial order on B.

2.2 Boolean Functions

We can now define Boolean functions using structural induction. For the remainder of this text, let $(B, \cup, \cap, \bar{\cdot}, 0, 1)$ be a Boolean algebra.

Definition 2.13. We define the set of ***Boolean functions*** (on B) inductively using the following rules:

1. For any $n \in \mathbb{N}$, $b \in B$ the constant function $c_b^n : B^n \to B : x \mapsto b$ is a boolean function.
2. For any $n \in \mathbb{N}$, $1 \leq i \leq n$ the projection function $\pi_i^n : B^n \to B : (x_1, \dots, x_n) \mapsto x_i$ is a boolean function.
3. For any Boolean functions $f : B^n \to B, g : B^n \to B$ the functions
   a) $f \cup g : B^n \to B : x \mapsto f(x) \cup g(x)$
   b) $f \cap g : B^n \to B : x \mapsto f(x) \cap g(x)$
   c) $\overline{f} : B^n \to B : x \mapsto \overline{f(x)}$

   are Boolean functions.

Any function that can be constructed by applying the above rules a finite number of times is a Boolean function. The set of all Boolean functions on B is denoted as $\mathrm{BF}(B)$. We also define $\mathrm{BF}_n(B) \subseteq \mathrm{BF}(B)$ as the set of Boolean functions of arity n.

Definition 2.13 implicitly defines operations on Boolean functions. As shown in the following examples, these pointwise operations are useful to specify Boolean functions.

Example 2.14. Fix $b \in B$. The function $f : B^3 \to B : (x_1, x_2, x_3) \mapsto x_1 \cup (x_2 \cap b)$ is a Boolean function. It can be constructed as $\pi_1^3 \cup (\pi_2^3 \cap c_b^3)$.

Definition 2.15. We define $V_n(B) := \{0, 1\}^n$. The elements of $V_n(B)$ are called ***elementary vectors***. Let $e \in \{0, 1\}$, $a \in B$, $v = (v_1, \dots, v_n) \in V_B$, $x = (x_1, \dots, x_n) \in B^n$. We define the special operations

$$a^e := \begin{cases} a & \text{if } e = 1 \\ \overline{a} & \text{if } e = 0 \end{cases}$$

and

$$x^v := \bigcap_{i=1}^{n} x_i^{v_i}.$$

Lemma 2.16. Let $x \in B^n$ be a vector. Then the following statements hold:

1. $$\bigcup_{v \in V_n(B)} x^v = 1. \tag{2.23}$$
2. For any $w, u \in V_n(B)$ with $w \neq u$
   $$x^w \cap x^u = 0. \tag{2.24}$$

3. For any $a, b \in \{0, 1\}$

$$a^b = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases}. \tag{2.25}$$

4. For any $w, u \in V_n(B)$

$$w^u = \begin{cases} 1 & \text{if } w = u \\ 0 & \text{if } w \neq u \end{cases}. \tag{2.26}$$

Proof. 1. By induction on $n \in \mathbb{N}$. In the base case $n = 1$ the statement reduces to the trivial fact $x \cup \overline{x} = 1$. For the induction step, assume that the statement holds for $n \in \mathbb{N}$. Take any $x = (x_1, \ldots, x_{n+1}) \in B^{n+1}$ and set $y \coloneqq (x_2, \ldots, x_{n+1}) \in B^n$. We can derive

$$\bigcup_{v \in V_{n+1}(B)} x^v = \left[x_1 \cap \left(\bigcup_{w \in V_n(B)} y^w \right) \right] \cup \left[\overline{x_1} \cap \left(\bigcup_{w \in V_n(B)} y^w \right) \right] = 1$$

using the induction hypothesis in the second step, which proves the statement for $n + 1$. The induction is complete.

2. The condition $w \neq u$ implies that for some $j \in \{1, \ldots, n\}$ we have $w_i \neq u_i$. W.l.o.g. assume $w_i = 0$ and $u_i = 1$. Then $x_i^{w_i} \cap x_i^{u_i} = 0$ and therefore $x^w \cap x^u = \bigcap_{i=1}^n (x_i^{w_i} \cap x_i^{u_i}) = 0$.

3. By simple verification of all four cases using (2.11) and (2.12).

4. If $w \neq u$, there exists some $j \in \{1, \ldots, n\}$ such that $w_j \neq u_j$. Then ${w_j}^{u_j} = 0$ by (2.25) and thus $w^u = 0$. If $w = u$, again by (2.25) we have $w_i^{u_i} = 1$ for any $i \in \{1, \ldots, n\}$ which implies $w^u = 1$.

$\square$

Theorem 2.17. Let $f : B^n \to B$ be a function. f is a Boolean function if and only if it can be written in the form

$$f(x) = \bigcup_{v \in V_n(B)} (d_v \cap x^v) \tag{2.27}$$

for all $x \in B^n$, where the coefficients $d_v \in B$ are uniquely determined by $d_v = f(v)$. This form is called the ***canonical disjunctive form*** of f.

Proof. "$\Rightarrow$" By structural induction on $\mathrm{BF}(B)$. We start by considering the basic Boolean functions. Choose $n \in \mathbb{N}$ and $x \in B^n$ arbitrarily. Using (2.23), the constant functions can be written as

$$c_b^n(x) = b \cap \left(\bigcup_{v \in V_n(B)} x^v \right) = \bigcup_{v \in V_n(B)} (b \cap x^v) = \bigcup_{v \in V_n(B)} (c_b^n(v) \cap x^v),$$

which is exactly the form of (2.27) with $d_v = c_b^n(v)$.

Set $y_i \coloneqq (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. Then we can also write the projection functions in canonical disjunctive form as

$$\pi_i^n(x) = \bigcup_{w \in V_{n-1}(B)} (x_i \cap y_i^w) = \bigcup_{\substack{v \in V_n(B) \\ v_i = 1}} x^v = \bigcup_{v \in V_n(B)} (\pi_i^n(v) \cap x^v),$$

where we have used (2.23) again.

For the induction step, assume that the theorem holds for two Boolean functions $f, g \in \mathrm{BF}_n(B)$ where $n \in \mathbb{N}$ is arbitrary. Then the functions can be written in the form $f(x) = \bigcup_{v \in V_n(B)} (f(v) \cap x^v)$ and $g(x) = \bigcup_{v \in V_n(B)} (g(v) \cap x^v)$.

Then $f \cup g$ can be brought into canonical disjunctive form as

$$f(x) \cup g(x) = \bigcup_{v \in V_n(B)} (f(v) \cup g(v)) \cap x^v$$

by the distributive law.

Using the generalized distributive law and (2.24) we can observe that

$$\begin{aligned}
f(x) \cap g(x) &= \bigcup_{v \in V_n(B)} (f(v) \cap x^v) \cap \bigcup_{v \in V_n(B)} (g(v) \cap x^v) \\
&= \bigcup_{v \in V_n(B), w \in V_n(B)} (f(v) \cap x^v) \cap (g(w) \cap x^w) \\
&= \bigcup_{v \in V_n(B)} (f(v) \cap g(v)) \cap x^v.
\end{aligned}$$

This shows that $f \cap g$ can be written in canonical disjunctive form.

From the facts we have already shown about $f \cap g$ and $f \cup g$, we can now observe that

$$f(x) \cup \bigcup_{v \in V_n(B)} \left(\overline{f(v)} \cap x^v\right) = \bigcup_{v \in V_n(B)} \left(f(v) \cup \overline{f(v)}\right) \cap x^v = \bigcup_{v \in V_n(B)} 1 \cap x^v = 1$$

and

$$f(x) \cap \bigcup_{v \in V_n(B)} \left(\overline{f(v)} \cap x^v\right) = \bigcup_{v \in V_n(B)} \left(f(v) \cap \overline{f(v)}\right) \cap x^v = \bigcup_{v \in V_n(B)} 0 \cap x^v = 0$$

Because the complement is unique (see (2.7)), we can conclude that $\overline{f}$ can be written in canonical disjunctive form as

$$\overline{f}(x) = \overline{\bigcup_{v \in V_n(B)} (f(v) \cap x^v)} = \bigcup_{v \in V_n(B)} \left(\overline{f(v)} \cap x^v\right).$$

This completes the induction step, the theorem holds for all Boolean functions.

"$\Leftarrow$" If a function can be written in the form given in the theorem, it is clearly a Boolean function.

The last step is to show that the coefficients d_v are uniquely determined by $f(v)$. Assume that a Boolean function f can be written in the form given by (2.27).

Then we can calculate for any $w \in V_n(B)$ that

$$f(w) = \bigcup_{v \in V_n(B)} (d_v \cap w^v) = d_w \cap w^w = d_w$$

by (2.26), which concludes the proof. □

The set of Boolean functions $\mathrm{BF}(B)$ will be central to our definition of Boolean equations. However, to also include systems of Boolean equations in our treatment, we need to expand our definition to multivalued Boolean functions. We will do so without introducing a special notation, by treating a multivalued function f as a vector $f = (f_1, \ldots, f_m)$ where $f_i : B^n \to B$ for all $1 \leq i \leq m$. We define the set of m-valued boolean functions of arity n as $\mathrm{BF}_n^m(B) \coloneqq \{(f_1, ..., f_m) : B^n \to B^m \mid f_1, \ldots, f_m \in \mathrm{BF}_n(B)\}$.

2.3 Boolean Equations

We can now define Boolean equations and different notions of solutions to them.

Definition 2.18. Let $f, g \in \mathrm{BF}_n^m(B)$ be Boolean functions. A ***system of Boolean equations*** is an equation of the form $f(x) = g(x)$. If $m = 1$, we say that the system of Boolean equations is a ***Boolean equation***.

When specifying Boolean equations in practice we will treat $x_1, \ldots, x_n$ like variables in their own right but in doing so implicitly define the Boolean functions f and g from the formal definition. This is illustrated in the following examples. The arity n of these functions will always be the number of distinct variables appearing in a given equation.

These conventions show that Definition 2.18, which is deliberately kept formal to allow for more rigorous proofs, indeed covers equations in unknowns as presented in Chapter 1.

Example 2.19. The equation $x_1 \cup x_2 = x_1 \cap x_2$ is a Boolean equation. The Boolean functions $f, g \in \mathrm{BF}_2^1$ from Definition 2.18 are given by $f(x_1, x_2) = x_1 \cup x_2$ and $g(x_1, x_2) = x_1 \cap x_2$.

Example 2.20. The equations

$$\begin{aligned} x_1 \cap \overline{x_2} &= x_3 \cap \overline{x_4} \\ \overline{x_1} \cap x_2 &= \overline{x_3} \cap x_4 \end{aligned}$$

are a system of Boolean equations. The Boolean functions $f, g \in \mathrm{BF}_4^2$ from Definition 2.18 are given by $f(x_1, x_2, x_3, x_4) = (x_1 \cap \overline{x_2}, \overline{x_1} \cap x_2)$ and $g(x_1, x_2, x_3, x_4) = (x_3 \cap \overline{x_4}, \overline{x_3} \cap x_4)$.

Definition 2.21. Let $f(x) = g(x)$ be a Boolean equation with $f, g \in \mathrm{BF}_n^m(B)$. A ***particular solution*** of the equation is a vector $\xi \in B^n$ such that $f(\xi) = g(\xi)$. The ***solution*** set S is defined as $\{\xi \in B^n \mid f(\xi) = g(\xi)\}$. ***Solving a Boolean equation*** means determining the solution set S of a given equation explicitly. If S is the empty set, the equation is called ***inconsistent***, otherwise it is called ***consistent***.

Example 2.22. We want to find the solution set S of the equation $x_1 \cup x_2 = x_1 \cap x_2$ from Example 2.19. First, assume that $x \in B^2$ is a solution. Then

$$x_1 = (x_1 \cup x_2) \cap x_1 \stackrel{*}{=} (x_1 \cap x_2) \cap x_1 = x_1 \cap x_2$$

where we used the boolean equation in the step marked with an asterisk. But in the same manner

$$x_2 = (x_1 \cup x_2) \cap x_2 = (x_1 \cap x_2) \cap x_2 = x_1 \cap x_2,$$

so we have $x_1 = x_2$. On the other hand, if $x_1 = x_2$ then $x_1 \cup x_2 = x_1 \cap x_2$ is trivially fulfilled. So in general we have $S = \{(t, t) \mid t \in B\}$. In the special case $B = B_2$ we can explicitly specify $S = \{(0, 0), (1, 1)\}$.

In general, the solution set of a Boolean equation might be large or even infinite. Using an infinite Boolean algebra B in Example 2.22 demonstrates such a situation. Enumerating all solutions is not always feasible and in the infinite case impossible, which motivates the concept of parametric solutions to Boolean equations.

Definition 2.23. Let $f(x) = g(x)$ be a Boolean equation with solution set S and $f, g \in \mathrm{BF}_n^m(B)$. A ***parametric solution*** of the equation is a function $\Xi : B^n \to S$. If Ξ is surjective we call it a ***general parametric solution***. If $\Xi \restriction_S = \mathrm{id}_S$ we call Ξ a ***reproductive general solution***.

Remark 2.24. Altough general parametric solutions are not necessarily unique, we still talk about "the" general parametric solution of any given equation. This is because all general parametric solutions are equivalent in the sense that they fully describe the solution set. The same applies to reproductive general solutions.

To specify parametric solutions we use the more readable notation $x_i = f_i(t_1, \ldots, t_n)$ for $i \in \{1, \ldots, n\}$. This is to be interpreted as specifying the parametric solution

$$\Xi(t_1, \ldots, t_n) \coloneqq (f_1(t_1, \ldots, t_n), \ldots, f_n(t_1, \ldots, t_n)).$$

Example 2.25. In Example 2.22 we have shown that the solutions of $x_1 \cup x_2 = x_1 \cap x_2$ are $S = \{(t, t) \mid t \in B\}$ in any Boolean algebra B. Consider the function $\Xi : B^2 \to B^2 : (t_1, t_2) \mapsto (t_1, t_1)$. It is easy to see that $\Xi(B^2) \subseteq S$ and $\Xi \restriction_S = \mathrm{id}_S$. Therefore Ξ is the reproductive general solution of the equation. In the short notation we say that $x_1 = t_1, x_2 = t_1$ is the reproductive general solution.

2.4 Reducing Systems of Boolean Equations

In this section we will show that any system of Boolean equations can be reduced to a Boolean equation of the form $f(x) = 0$ with $f \in \mathrm{BF}_n(B)$, which justifies our focus on single equations in Chapter 3.

Theorem 2.26. Let $f(x) = g(x)$ be a system of Boolean equations with $f, g \in \mathrm{BF}_n^m(B)$. Then there exists a Boolean function $h \in \mathrm{BF}_n^1(B)$ such that the equation $h(x) = c_0^n(x)$ has the same solution set as $f(x) = g(x)$.

Proof. Let $f(x) = g(x)$ be an equation as defined in the theorem. We consider the following cases:

- First we consider the case that $m = 1$. Define $h : B^n \to B$ as
$$h := (f \cap \overline{g}) \cup \left(\overline{f} \cap g\right).$$
We want to show that the equation $h(x) = c_0^n(x)$ has the same solution set as $f(x) = g(x)$.
Assume that $h(\xi) = 0$ for any $\xi \in B$. We arrive at the equation
$$h(\xi) \cup (f(\xi) \cap g(\xi)) = f(\xi) \cap g(\xi).$$
By expanding $h(\xi)$ and applying (2.13) on the left-hand side of the equation above we obtain
$$f(\xi) \cup g(\xi) = f(\xi) \cap g(\xi).$$
As we know from Example 2.22 this implies that $f(\xi) = g(\xi)$, so ξ is a particular solution to $f(x) = g(x)$.
On the other hand, if we assume $f(\xi) = g(\xi) =: c$ for an arbitrary chosen $\xi \in B^n$, then
$$h(\xi) = (c \cap \overline{c}) \cup (\overline{c} \cap c) = 0,$$
so ξ is a particular solution to $h(x) = c_0^n(x)$.
- Now consider the case $m > 1$. Using the previous case we can construct $h : B^n \to B^m$ such that $h(x) = 0$ has the same solution set as $f(x) = g(x)$. We need to reduce this system to a single equation.
With induction, we can extend (2.6) to $\bigcup_{i=1}^{l} a_i = 0 \Leftrightarrow \forall\, i \in \{1, \dots, l\} : a_i = 0$ for $a_1, \dots, a_l \in B$. So for any $\xi \in B^n$ we have
$$h(\xi) = 0 \Longleftrightarrow \forall\, i \in \{1, \dots, m\} : h_i(\xi) = 0 \Longleftrightarrow \bigcup_{i=1}^{m} h_i(\xi) = 0.$$
So in summary, setting $h' := \bigcup_{i=1}^{m} h_i \in \mathrm{BF}_n^1(B)$ the Boolean equation $h'(x) = c_0^n(x)$ has the same solution set as $f(x) = g(x)$.

□

Remark 2.27. In the remainder of the text, we will not distinguish between the constant function c_b^n and the constant b. We will use the notation b for both. Also, we will say that an equation of the form $f(x) = 0$ is in ***normal form***.

Example 2.28. We can reduce the system (1.1) from Chapter 1 to a single equation. We start by replacing each line of the system with the equivalent statement where the right-hand side is 0. This gives us the system
$$(x_1 \cap x_2 \cap \overline{a}) \cup ((\overline{x_1} \cup \overline{x_2}) \cap a) = 0$$
$$((x_1 \cup x_2) \cap \overline{b}) \cup (\overline{x_1} \cap \overline{x_2} \cap b) = 0$$

which is equivalent to the original system. We can now combine the two equations to the single equation

$$(x_1 \cap x_2 \cap \overline{a}) \cup ((\overline{x_1} \cup \overline{x_2}) \cap a) \cup ((x_1 \cup x_2) \cap \overline{b}) \cup (\overline{x_1} \cap \overline{x_2} \cap b) = 0 \tag{2.28}$$

which is now in normal form.

3 Solving Boolean Equations

In this chapter we will show necessary and sufficient conditions for the consistency of Boolean equations, as well as methods for finding their solution set and the general reproductive solution. We start with the case of equations in one unknown, and then generalize to equations in multiple unknowns.

3.1 Boolean Equations in One Unknown

In this section we will consider a Boolean equation $f(x) = 0$ in one unknown, so $f \in \mathrm{BF}_1(B)$. According to Theorem 2.17 we can write f in canonical disjunctive form as

$$f(x) = (a \cap x) \cup (b \cap \overline{x})$$

where $a = f(1)$ and $b = f(0)$. Thus, we will only consider equations of this form. The following lemma establishes the conditions under which such an equation is consistent.

Lemma 3.1. Let $a, b \in B$. The Boolean equation $(a \cap x) \cup (b \cap \overline{x}) = 0$ is consistent if and only if $a \cap b = 0$.

Proof. "$\Rightarrow$" Assume $\xi \in B$ is a particular solution of the equation. Then $a \cap \xi = 0$ and $b \cap \overline{\xi} = 0$ by (2.6). We calculate

$$a \cap b = (a \cap b) \cap (\overline{\xi} \cup \xi) = (a \cap b \cap \overline{\xi}) \cup (a \cap b \cap \xi) = 0,$$

which shows that our condition is necessary.

"$\Leftarrow$" Conversely, if we assume $a \cap b = 0$, we get

$$f(b) = (a \cap b) \cup (b \cap \overline{b}) = 0,$$

which means that b is a particular solution of the equation, and the equation is thus consistent. We have therefore shown that the condition $a \cap b = 0$ is also sufficient.

□

We can now fully describe the solution set of a Boolean equation in one unknown.

Theorem 3.2. Let $a, b \in B$. Assume that the Boolean equation $(a \cap x) \cup (b \cap \overline{x}) = 0$ is consistent.

Then the solution set S of the equation is given by

$$S = \{\xi \in B \mid b \subseteq \xi \subseteq \overline{a}\}$$

and

$$\Xi : B \to S : t \mapsto b \cup (\overline{a} \cap t)$$

is the reproductive general solution of the equation.

Proof. We will first show that for any $x \in B$ the equivalence

$$(a \cap x) \cup (b \cap \overline{x}) = 0 \iff b \subseteq x \subseteq \overline{a} \tag{3.1}$$

holds. To see this, note that by (2.6) the left statement is equivalent to

$$a \cap x = 0 \wedge b \cap \overline{x} = 0.$$

Because these two statements are equivalent to the inequality on the right side of (3.1) by (2.10) and (2.19), we have shown the equivalence. The statement of the lemma about the solution set follows directly from (3.1).

According to our assumption the Boolean equation is consistent, so with Lemma 3.1 we have that $a \cap b = 0$. Now take any $t \in B$. Using (2.9), we get

$$f(b \cup (\overline{a} \cap t)) = (a \cap (b \cup (\overline{a} \cap t))) \cup (b \cap \overline{(b \cup (\overline{a} \cap t))}) = \underbrace{(a \cap b)}_{=0} \cup (\underbrace{a \cap \overline{a}}_{=0} \cap t) \cup (\underbrace{b \cap \overline{b}}_{=0} \cap \overline{(\overline{a} \cap t)}) = 0,$$

so $\Xi(t) \in S$. We conclude that Ξ is a parametric solution of the equation.

Now we check that Ξ is a reproductive solution. If $x \in B$ is a particular solution, we have shown that $b \subseteq x \subseteq \overline{a}$ holds. By (2.18) and the definition of the relation $\subseteq$ we get that $x \cap \overline{a} = x$ and $x = b \cup x$, so using these facts $\Xi(x) = b \cup (\overline{a} \cap x) = b \cup x = x$, which means that Ξ is a reproductive general solution of the equation. □

3.2 Boolean Equations in Multiple Unkowns

We will now consider the Boolean equation $f(x) = 0$ in multiple unknowns, so $f \in \mathrm{BF}_n(B)$. First we will present a necessary and sufficient condition for the consistency of such an equation, and then a method for solving these equations. The theme of this section is to generalize the results we have for equations in one unknown.

3.2.1 Consistency

Theorem 3.3. Let $f \in \mathrm{BF}_n(B)$ be a Boolean function. The Boolean equation $f(x) = 0$ is consistent if and only if $\bigcap_{v \in V_n(B)} f(v) = 0$.

Proof. "⇒" Assume that $f(x) = 0$ is consistent, and $\xi \in B^n$ is a particular solution of the equation. Then

$$f(\xi) = \bigcup_{v \in V_n(B)} f(v) \cap \xi^v = 0.$$

Let $v \in V_n(B)$ be an elementary vector. Obviously, $\left(\bigcap_{w \in W_n(B)} f(w)\right) \subseteq f(v)$ is true by (2.18). So using (2.17) we have $\left(\bigcap_{w \in W_n(B)} f(w)\right) \cap \xi^v \subseteq f(v) \cap \xi^v$.

By taking the union over all elementary vectors $v \in V_n(B)$, using the inequality we have already established and (2.22) we arrive at

$$\bigcup_{v \in V_n(B)} \left(\bigcap_{w \in W_n(B)} f(w) \right) \cap \xi^v \subseteq f(\xi).$$

But the left-hand side of this equation simplifies to

$$\bigcup_{v\in V_n(B)} \left(\bigcap_{w\in W_n(B)} f(w) \right) \cap \xi^v = \left(\bigcap_{w\in W_n(B)} f(w) \right) \cap \bigcup_{v\in V_n(B)} \xi^v = \bigcap_{w\in W_n(B)} f(w),$$

which shows that $\bigcap_{w\in W_n(B)} f(w) = 0$, by (2.21).

"$\Leftarrow$" We will use induction on the number of variables n. The base case $n = 1$ has already been shown in Lemma 3.1.

For the induction step, assume that the theorem holds for all Boolean functions in $\mathrm{BF}_{n-1}(B)$ and that $\bigcap_{v\in V_n(B)} f(v) = 0$. Set $g(x_1, \dots, x_{n-1}) := f(1, x_1, \dots, x_{n-1}) \cap f(0, x_1, \dots, x_{n-1})$. Then we can see that

$$\bigcap_{w\in V_{n-1}(B)} g(w) = \bigcap_{v\in V_n(B)} f(v) = 0.$$

By the induction hypothesis, the Boolean equation $g(x_1, \dots, x_{n-1}) = 0$ is consistent, and we can find a particular solution $\xi = (\xi_1, \dots, \xi_{n-1}) \in B^{n-1}$ of the equation $g(x) = 0$.

Because ξ is a particular solution of $g(x) = 0$, we have

$$f(1, \xi_1, \dots, \xi_{n-1}) \cap f(0, \xi_1, \dots, \xi_{n-1}) = 0$$

and by Lemma 3.1 we can conclude that a particular solution $\xi' \in B$ of the equation

$$(f(1, \xi_1, \dots, x_{n-1}) \cap x) \cup (f(0, \xi_1, \dots, \xi_{n-1}) \cap \overline{x}) = 0$$

exists.

Now we can define $\rho := (\xi', \xi_1, \dots, \xi_2)$ and see by application of (2.27) on the Boolean function $f(\cdot, \xi_1, \dots, \xi_{n-1})$ that

$$f(\rho) = \big(f(1, \xi_1, \dots, \xi_{n-1}) \cap \xi'\big) \cup \big(f(0, \xi_1, \dots, \xi_{n-1}) \cap \overline{\xi'}\big) = 0.$$

This concludes the induction step, because we have shown that $\rho \in B^n$ is a particular solution of the equation $f(x) = 0$ and therefore that the equation is consistent. $\square$

3.2.2 Method of Successive Eliminations

We will now show a method for solving Boolean equations by eliminating variables one by one. Consider the Boolean equation $f(x) = 0$ with $f \in \mathrm{BF}_n(B)$.

Define the functions

$$f^p(x_1, \dots, x_p) := \bigcap_{v\in V_{n-p}(B)} f(x_1, \dots, x_p, v_1, \dots, v_{n-p})$$

for $p \in \{1, \dots, n\}$. Note that in particular $f^n = f$.

In the step $n-p+1$ of the method, so starting at $p=n$, we can write the equation $f^p(x_1,\dots,x_p)=0$ as

$$(f^p(x_1,\dots,x_{p-1},1)\cap x_p)\cup(f^p(x_1,\dots,x_{p-1},0)\cap\overline{x_p})=0$$

by applying Theorem 2.17 on the Boolean function $x_p\mapsto f^p(x_1,\dots,x_{p-1},x_p)$.

When we consider $x_1,\dots,x_{p-1}$ as fixed elements of B, the solutions to the equation above are given by

$$f^p(x_1,\dots,x_{p-1},0)\subseteq x_p\subseteq\overline{f^p(x_1,\dots,x_{p-1},1)} \tag{3.2}$$

according to Theorem 3.2, provided that the consistency condition

$$f^p(x_1,\dots,x_{p-1},1)\cap f^p(x_1,\dots,x_{p-1},0)=0 \tag{3.3}$$

is fulfilled. However, the left-hand side of the equation is exactly f^{p-1}, so we continue with the equation $f^{p-1}(x_1,\dots,x_{p-1})=0$ in the next step.

In the last step we have to solve the equation $f^1(x_1)=0$ which has the solution set

$$f^1(0)\subseteq x_1\subseteq\overline{f^1(1)} \tag{3.4}$$

and is consistent if $f^1(0)\cap f^1(1)=f^0=0$.

That this method leads to a description of the solution set is shown in the following theorem.

Theorem 3.4. Let $f\in\mathrm{BF}_n(B)$ be a Boolean function. For $p\in\{1,\dots,n\}$ set

$$f^p(x_1,\dots,x_p):=\bigcap_{v\in V_{n-p}(B)}f(x_1,\dots,x_p,v_1,\dots,v_{n-p}).$$

If $f^0=0$, the Boolean equation $f(x)=0$ is consistent and its solution set S is described by the recurrent inequalities

$$f^p(x_1,\dots,x_{p-1},0)\subseteq x_p\subseteq\overline{f^p(x_1,\dots,x_{p-1},1)}.$$

If otherwise $f_0\neq 0$, the equation is inconsistent.

Proof. The statement about the consistency of $f(x)=0$ is clear from Theorem 3.3 with the fact that $f^0=\bigcap_{v\in V_n(B)}f(v)$.

Now assume that $f^0=0$. We will show that the solution set S of the equation $f(x)=0$ is given by the recurrent inequalities. For this, we need to anlayse the method in reverse order. Because $f^0=0$, the equation $f^1(x_1)=0$ is consistent and has a non-empty solution set given by (3.4). This means that (3.3) of the previous step is fulfilled for all ξ_1 in the interval $f^1(0)\subseteq\xi_1\subseteq\overline{f^1(1)}$. By continuing this argument through the steps of the method in reverse order, we can see that for any $q\in\{1,\dots,n\}$, all vectors $\xi\in B^q$ that satisfy (3.2) for all $p<q$ are particular solutions to the equation $f^q(x)=0$. So, finally we arrive at $f^n(x)=f(x)=0$ and see that all vectors satisfying the recurrent inequalities are solutions to the equation.

It remains to verify that these are indeed all solutions. This can be seen easily however, because by describing the method we have already proven that any particular solution has to fulfill the recurrent inequalities.

□

Example 3.5. We will now solve the system of equations (1.1) from the introduction using the method of successive eliminations. From Example 2.28 we know the standard form of the problem:

$$(x_1 \cap x_2 \cap \overline{a}) \cup ((\overline{x_1} \cup \overline{x_2}) \cap a) \cup ((x_1 \cup x_2) \cap \overline{b}) \cup (\overline{x_1} \cap \overline{x_2} \cap b) = 0$$

Setting x_2 to 1 and 0 respectively to get the coefficients of the disjunctive normal form, we arrive at the equivalent equation

$$\left[\big((x_1 \cap \overline{a}) \cup (\overline{x_1} \cap a) \cup \overline{b}\big) \cap x_2\right] \cup \left[\big((x_1 \cap \overline{b}) \cup (\overline{x_1} \cap b) \cup a\big) \cap \overline{x_2}\right] = 0.$$

This equation is consistent iff

$$\big((x_1 \cap \overline{a}) \cup (\overline{x_1} \cap a) \cup \overline{b}\big) \cap \big((x_1 \cap \overline{b}) \cup (\overline{x_1} \cap b) \cup a\big) = 0$$

holds. We can simplify this equation by setting x_1 to 1 and 0 respectively to obtain

$$(\overline{b} \cap x_1) \cup (a \cap \overline{x_1}) = 0.$$

This equation is consistent iff $a \cap \overline{b} = 0$, or equivalentely $a \subseteq b$.

So eq. (1.1) is consistent iff $a \subseteq b$, and the solution set is given by the recurrent inequalities

$$\begin{gathered} a \subseteq x_1 \subseteq b \\ \big((x_1 \cap \overline{b}) \cup (\overline{x_1} \cap b) \cup a\big) \subseteq x_2 \subseteq \overline{\big((x_1 \cap \overline{a}) \cup (\overline{x_1} \cap a) \cup \overline{b}\big)}. \end{gathered}$$

We can further simplify the second inequality, if we assume the inequality $a \subseteq x_1 \subseteq b$. Then we get that the solutions are given by

$$\begin{aligned} a \subseteq x_1 &\subseteq b \\ x_2 &= b \cap (\overline{x_1} \cup a) \end{aligned}$$

because both bounds to x_2 turn out to be equal to $b \cap (\overline{x_1} \cup a)$.

Remark 3.6. By Theorem 3.2 we also know how we can characterize solutions for equations in one unknown in a parametric way. By using this approach in the method of successive eliminations, we can find a reproductive general solution of the equation instead of describing the solution set with recurrent inequalities.

Example 3.7. Continuing Example 3.5, we can write down the reproductive general solution of the system of equations (1.1) in a recurrent way as

$$\begin{aligned} x_1 &= a \cup (t \cap b) \\ x_2 &= b \cap (\overline{x_1} \cup a) \end{aligned}$$

or more detailed without recursion as

$$\begin{aligned} x_1 &= a \cup (t_1 \cap b) \\ x_2 &= b \cap (\overline{a \cup (t_1 \cap b)} \cup a) = b \cap (\overline{t_1} \cup a). \end{aligned}$$

3.3 Particular Solutions

A result due to Löwenheim allows us to gain a reproductive general solution of a Boolean equation once we know one particular solution.

To formulate this theorem, we will first extend the operation $\cap$ of the Boolean algebra to B^n. For $a \in B, b = (b_1, \dots, b_n) \in B^n$ we define

$$a \cap b := (a \cap b_1, \dots, a \cap b_n).$$

We start with two lemmas that will be used in the proof of the theorem.

Lemma 3.8. Let $t, x, y \in B$ be elements of B, $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in B^n$ vectors and $e \in \{0, 1\}$. Then the following equalities hold:

$$\big((t \cap x) \cup (\bar{t} \cap y)\big)^e = (t \cap x^e) \cup (\bar{t} \cap y^e) \tag{3.5}$$

$$\bigcap_{i=1}^{n} (t \cap a_i) \cup (\bar{t} \cap b_i) = \left(t \cap \bigcap_{i=1}^{n} a_i\right) \cup \left(\bar{t} \cap \bigcap_{i=1}^{n} b_i\right) \tag{3.6}$$

Proof. (3.5) The case $e = 1$ is trivial, because then the operation $x \mapsto x^e$ is the identity on B. For $e = 0$ we have to show that

$$\overline{(t \cap x) \cup (\bar{t} \cap y)} = (t \cap \overline{x}) \cup (\bar{t} \cap \overline{y})$$

holds. This is easy to see when we apply Theorem 2.17 to the function

$$t \mapsto \overline{(t \cap x) \cup (\bar{t} \cap y)}.$$

The right side of the equation is just the canonical disjunctive form of the function.

(3.6) Just as before, write $t \mapsto \bigcap_{i=1}^{n} (t \cap a_i) \cup (\bar{t} \cap b_i)$ in canonical disjunctive form. The coefficients are exactly the same as on the right side of the equation.

□

Lemma 3.9. Let $f \in \mathrm{BF}_n(B)$ be a Boolean function, $t \in B$ and $w = (w_1, \dots, w_n), u = (u_1, \dots, u_n) \in B^n$. Then

$$f\left((t \cap w) \cup (\bar{t} \cap u)\right) = (t \cap f(w)) \cup \left(\bar{t} \cap f(u)\right)$$

holds.

Proof. We use Theorem 2.17 to write f in canonical disjunctive form and calculate

$$\begin{aligned} f\left((t \cap w) \cup (\bar{t} \cap u)\right) &= \bigcup_{v \in V_n(B)} f(v) \cap \left((t \cap w) \cup (\bar{t} \cap u)\right)^v \\ &= \bigcup_{v \in V_n(B)} f(v) \cap \bigcap_{i=1}^{n} \left((t \cap w_i) \cup (\bar{t} \cap u_i)\right)^{v_i} \\ &= \bigcup_{v \in V_n(B)} f(v) \cap \bigcap_{i=1}^{n} (t \cap w_i^{v_i}) \cup (\bar{t} \cap u_i^{v_i}) \\ &= \bigcup_{v \in V_n(B)} f(v) \cap \left((t \cap \bigcap_{i=1}^{n} w_i^{v_i}) \cup (\bar{t} \cap \bigcap_{i=1}^{n} u_i^{v_i}) \right) \\ &= (t \cap \bigcup_{v \in V_n(B)} f(v) \cap w^v) \cup (\bar{t} \cap \bigcup_{v \in V_n(B)} f(v) \cap u^v) \\ &= (t \cap f(w)) \cup (\bar{t} \cap f(u)). \end{aligned}$$

In the third and fourth step we have used the identities from Lemma 3.8. □

We can now state and prove the theorem.

Theorem 3.10 (Löwenheim)**.** Let $f(x) = 0$ be a Boolean equation with $f \in \mathrm{BF}_n(B)$ and $\xi \in B^n$ a particular solution of the equation. Then

$$\Xi : B^n \to S : t \mapsto (\xi \cap f(t)) \cup (t \cap \overline{f(t)})$$

is the reproductive general solution of the equation.

Proof. Using Lemma 3.9 we can see that

$$f\left((\xi \cap f(t)) \cup (t \cap \overline{f(t)})\right) = (f(\xi) \cap f(t)) \cup (f(t) \cap \overline{f(t)}) = 0,$$

which means that Ξ is a parametric solution of the equation. Moreover, if $f(t) = 0$, we have that

$$\Xi(t) = (t \cap f(t)) \cup (t \cap \overline{f(t)}) = t,$$

so Ξ is a reproductive general solution of the equation. □

Example 3.11. We will once again consider the system of equations from Chapter 1. However, we will set $b = 1$ to make the system consistent for all $a \in B$. To summarize, the system we want to solve in this example is

$$\begin{aligned} x_1 \cap x_2 &= a \\ x_1 \cup x_2 &= 1. \end{aligned}$$

In this special case we can use Theorem 3.10 to obtain the general reproductive solution rather than following the method of successive eliminations (compare Example 3.5). That is because we can clearly see that $\xi_1 = a$, $\xi_2 = 1$ is a particular solution of the system.

Take the standard form of this system from Example 2.28:

$$f(x_1, x_2) \coloneqq (x_1 \cap x_2 \cap \overline{a}) \cup ((\overline{x_1} \cup \overline{x_2}) \cap a) \cup (\overline{x_1} \cap \overline{x_2}) = 0.$$

Because (ξ_1, ξ_2) is a particular solution to the system it also solves the standard form equation $f(x_1, x_2) = 0$. Therefore, we know by Theorem 3.10 that the reproductive general solution is given by

$$x_j = (\xi_j \cap f(t_1, t_2)) \cup (t_j \cap \overline{f(t_1, t_2)})$$

for $j = 1, 2$. Writing out these two expressions and simplifying them by computing the canonical disjunctive form in t_1 and t_2 yields the general reproductive solution

$$\begin{aligned} x_1 &= a \cup (t_1 \cap \overline{t_2}) \\ x_2 &= a \cup \overline{(t_1 \cap \overline{t_2})}. \end{aligned}$$

We can compare this to the reproductive general solution from Example 3.5, which was given by

$$\begin{aligned} x_1 &= a \cup t_1 \\ x_2 &= a \cup \overline{t_1}. \end{aligned}$$

These two solutions are not equal as functions on B^2, which demonstrates the non-uniqueness of general reproductive solutions. However, because the mapping $\psi : B^2 \to B : (t_1, t_2) \mapsto (t_1 \cap \overline{t_2})$ is a surjection, the two solutions are equivalent in the sense that they have the same range (compare Remark 2.24).

Bibliography

[Pin24] M. Pinsker. Algebra Lecture. 2024. Lecture notes available online at https://epsilon-equals-zero.github.io/algebra-2023s-vorlesung/document.pdf.

[Rud74] S. Rudeanu. *Boolean functions and equations*. North-Holland Publishing Co., Amsterdam, 1974.