university of groningen / faculty of science and engineering / mathematics and applied mathematics

An algebraic method for solving the Boolean Satisfiability Problem in Łukasiewicz logic

Bachelor's Project Mathematics

July 2022

Student: L. Marjanovic

First supervisor: Prof.dr. J. Top

Second assessor: Dr. S. Müller

Abstract

In this thesis we consider the Boolean Satisfiability Problem for the 3-valued Łukasiewicz logic. We reframe the problem in algebraic terms, showing how to represent propositional formulas as polynomials and using ring theory to determine when solutions exist for such polynomials. We then use Gröbner bases to determine precisely whether or not a polynomial, and therefore the propositional formula it represents, is satisfiable.

Contents

1 Introduction

The Boolean Satisfiability Problem is famous for being the first problem shown to be NP-complete. In complexity theory, P class problems are problems that can be solved in polynomial time, which means that if an input has size n, the total number N of operations required by an algorithm to solve the problem, can be expressed as a polynomial in n. For example, an algorithm requiring $N = n^2 + n$ operations would run in polynomial time. NP class problems, on the other hand, are not necessarily solved in polynomial time, but any potential solution can be verified in polynomial time. NP-complete means that any NP problem can be reduced (in polynomial time) to an NP-complete problem.

These concepts are central to the famous P vs NP problem. In the past, some NP problems have been shown to in fact be P, but this has never been shown for an NP-complete problem. If this where to be proved for even a single NP-complete problem, it would prove that all NP problems are in fact P, because any NP problem could be reduced to this particular NP-complete problem and subsequently solved in polynomial time. While most experts in the field doubt that this could be done, proving definitively one way or the other is one of the Millennium Prize Problems and would earn you $1,000,000.

2 What is the Boolean satisfiability problem?

We begin with a brief introduction to propositional logic before defining the Boolean Satisfiability Problem explicitly.

2.1 The basics of propositional logic

Definition 2.1. *Let $\mathcal{P} = \{p_i | i \in \mathbb{N}\}$ be a countable set of propositional atoms. A **propositional formula** is a well-formed formula (wff) defined as follows:*

1. *Every $p_i \in \mathcal{P}$ is a wff.*
2. *If P and Q are wff, then so are $\neg P$, $(P \wedge Q)$, $(P \vee Q)$, $(P \rightarrow Q)$, and $(P \equiv Q)$.*
3. *Nothing is a wff unless it can be constructed via repeated applications of (1) and (2).*

In general, we will refer to all elements of $\mathcal{P}$ as **propositional variables**, given in the upper case as P, Q, R, etc. Note that, due to the recursive nature of the above definition, propositional variables may represent propositional atoms or other propositional formulas, but that this doesn't affect any of the following theory.

Definition 2.2. *A **logic** is defined by the triple*

$$\langle \mathcal{V}, \mathcal{D}, \{f_c : c \in \mathcal{C}\} \rangle$$

where

- *$\mathcal{V}$ is a set of truth values*
- *$\mathcal{D}$ is a set of designated values (with $\mathcal{D} \subseteq \mathcal{V}$)*
- *$\mathcal{C}$ is the set of connectives $\{\neg, \wedge, \vee, \rightarrow, \equiv\}$ used to define propositional formulas. So an n-ary $c \in \mathcal{C}$ is a map $wffs^{(n)} \rightarrow wffs$*
- *for each n-ary connective $c \in \mathcal{C}$, there is a truth function $f_c : \mathcal{V}^{(n)} \rightarrow \mathcal{V}$*

Definition 2.3. *Let $v : \mathcal{P} \rightarrow \mathcal{V}$ be a function from the set of propositional variables to the set of truth values. We call $v(P)$ the **valuation** or **interpretation** of $P \in \mathcal{P}$. This function can be extended to all wffs by use of truth functions for each n-ary connective:*

$$v(c(A_1, \ldots, A_n)) = f_c(v(A_1), \ldots, v(A_n)), \tag{1}$$

the A_i denoting wffs.

The reason for having a valuation function and a truth value function is that propositional variables have no numerical value on their own. We must use the valuation function to assign them truth values. By extending the valuation function to each connective we show that every propositional variable P can be assigned a truth value $v(P)$, regardless of whether P represents a propositional atom or a propositional formula.

Example 1. (Classical Propositional Logic)

- $\mathcal{V} = \{0, 1\}$
- $\mathcal{D} = \{1\}$
- $\mathcal{C} = \{\neg, \wedge, \vee, \rightarrow, \equiv\}$ where

$f_\neg$	
0	1
1	0

$f_\wedge$	0	1
0	0	0
1	0	1

$f_\vee$	0	1
0	0	1
1	1	1

$f_\rightarrow$	0	1
0	1	1
1	0	1

$f_\equiv$	0	1
0	1	0
1	0	1

We also have $v : \mathcal{P} \rightarrow \mathcal{V}$ defined:

$$v(\neg P) = 1 - v(P) \qquad v((P \rightarrow Q)) = max\{1 - v(P), v(Q)\}$$
$$v((P \wedge Q)) = min\{v(P), v(Q)\} \qquad v((P \equiv Q)) = 1 - |v(P) - v(Q)|$$
$$v((P \vee Q)) = max\{v(P), v(Q)\}$$

An example of a propositional formula in Classical Propositional Logic might be

$$((P \wedge Q) \vee \neg R).$$

Let's give our propositional variables the valuation

$$v(P) = 1,\ v(Q) = 1,\ v(R) = 0.$$

We compute the valuation of the whole propositional formula using (1) as follows:

$$\begin{aligned} v(((P \wedge Q) \vee \neg R)) &= f_\vee(v(P \wedge Q), v(\neg R)) \\ &= f_\vee(f_\wedge(v(P), v(Q)), f_\neg(v(R))) \\ &= f_\vee(f_\wedge(1, 1), f_\neg(0)) \\ &= f_\vee(1, 1) \\ &= 1 \end{aligned}$$

Definition 2.4. *We say a propositional formula P is **satisfiable** if $v(P) \in \mathcal{D}$.*

As demonstrated in example (1), $((P \wedge Q) \vee \neg R)$ is an example of a satisfiable propositional formula.

Definition 2.5. *If a propositional formula is satisfied by any valuation, it is called a* ***tautology****. If it is never satisfiable, it is called a* ***contradiction****.*

An example of a tautology is

$$(P \vee \neg P). \tag{2}$$

This particular formula is known as the **law of the excluded middle** and can be interpreted as saying, 'either P is true, or it's false'. An example of a contradiction is

$$(P \wedge \neg P). \tag{3}$$

The negation of this formula, $\neg(P \wedge \neg P)$, is known as the **law of non-contradiction** and can be shown (via De Morgan's laws) to be logically equivalent to the law of the excluded middle.

Definition 2.6. *The* ***Boolean Satisfiability Problem (SAT)*** *asks: Is a given propositional formula P satisfiable?*

2.2 Łukasiewicz logic

The motivation for considering a three-valued logic is both fascinating and vague. There are many three-valued logics but the one we consider was developed by Jan Łukasiewicz of the Lwow-Warsaw school in the early 20th century. The Lwow-Warsaw school was primarily a philosophical movement although its members were also concerned with logic as well as traditional mathematics. Among their many debates at the time was the existence of so-called 'contradictory objects', a proposition that Łukasiewicz supported. This led him to attack the law of non-contradiction.
Later, while working on the theory of probability, he began to classify certain propositions as 'undefinite' [*sic*] and use fractional logical values to represent some propositions. For example, the proposition '$x^2 = 1$' on the set $\{-1, 0, 1\}$ would be given the truth value 2/3. Here he begins to use truth values in an unconventional manner.
The line of inquiry that finally led to the construction of a three-valued logic was the description of propositions concerning future events. Sentences like 'I shall be in Warsaw in a year' are not immediately true or false, so are assigned a third logical value interpreted as 'possibly' or 'undetermined'. [3][4]

Definition 2.7. *Łukasiewicz logic ($\mathcal{L}$) is defined*

- $\mathcal{V} = \{0, 1, 2\}$
- $\mathcal{D} = \{2\}$
- $\mathcal{C} = \{\neg, \wedge, \vee, \rightarrow, \equiv\}$ *where*

$f_\neg$		$f_\wedge$	0	1	2	$f_\vee$	0	1	2	$f_\rightarrow$	0	1	2	$f_\equiv$	0	1	2
0	2	0	0	0	0	0	0	1	2	0	2	2	2	0	2	1	0
1	1	1	0	1	1	1	1	1	2	1	1	2	2	1	1	2	1
2	0	2	0	1	2	2	2	2	2	2	0	1	2	2	0	1	2

$v : \mathcal{P} \rightarrow \mathcal{V}$ *is defined:*

$$v(\neg P) = 2 - v(P) \qquad v((P \rightarrow Q)) = min\{2, 2 - v(P) + v(Q)\}$$
$$v((P \wedge Q)) = min\{v(P), v(Q)\} \qquad v((P \equiv Q)) = 2 - |v(P) - v(Q)|$$
$$v((P \vee Q)) = max\{v(P), v(Q)\}$$

In Łukasiewcz's original definition, the third logical value was represented by 1/2, giving the truth value set $\mathcal{V} = \{0, 1/2, 1\}$. We have opted to use $\mathcal{V} = \{0, 1, 2\}$ in order to aid in future calculations, as will become more clear later on.
We must briefly discuss an important property of $\mathcal{L}$.

Definition 2.8. *A logic is* ***functionally complete*** *if every possible truth function exists as some superposition of f_c, $c \in \mathcal{C}$. Otherwise, we say the logic is* ***functionally incomplete****.*

Theorem 1. *$\mathcal{L}$ is functionally incomplete.*

Proof. First, we show that all truth functions in $\mathcal{L}$ can be defined in terms of $f_\neg$ and $f_\rightarrow$.

- $\alpha \vee \beta = (\alpha \rightarrow \beta) \rightarrow \beta$

α	β	$\alpha \rightarrow \beta$	$(\alpha \rightarrow \beta) \rightarrow \beta$	$\alpha \vee \beta$
0	0	2	0	0
0	1	2	1	1
0	2	2	2	2
1	0	1	1	1
1	1	2	1	1
1	2	2	2	2
2	0	0	2	2
2	1	1	2	2
2	2	2	2	2

- $\alpha \wedge \beta = \neg(\neg\alpha \vee \neg\beta)$

α	β	$\neg\alpha$	$\neg\beta$	$\neg\alpha \vee \neg\beta$	$\neg(\neg\alpha \vee \neg\beta)$	$\alpha \wedge \beta$
0	0	2	2	2	0	0
0	1	2	1	2	0	0
0	2	2	0	2	0	0
1	0	1	2	2	0	0
1	1	1	1	1	1	1
1	2	1	0	1	1	1
2	0	0	2	2	0	0
2	1	0	1	1	1	1
2	2	0	0	0	2	2

- $\alpha \equiv \beta = (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$

α	β	$\alpha \rightarrow \beta$	$\beta \rightarrow \alpha$	$(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$	$\alpha \equiv \beta$
0	0	2	2	2	2
0	1	2	1	1	1
0	2	2	0	0	0
1	0	1	2	1	1
1	1	2	2	2	2
1	2	2	1	1	1
2	0	0	2	0	0
2	1	1	2	1	1
2	2	2	2	2	2

Next, suppose for some $P \in \mathcal{P}$, $v(P) = 1$ for all valuations $v \in \mathcal{L}$. P cannot be an atomic sentence because then we could simply assign it the valuation 0 or 2. Therefore, either $P = \neg Q$ or $P = Q \to R$, for some $Q, R \in \mathcal{P}$. If $P = \neg Q$, then the valuaton $v(Q) = 0$ implies $v(P) = 2$. If $P = Q \to R$, then the valuation $v(Q) = 0$ also implies $v(P) = 2$. Having exhausted all possible options, we conclude that there exists no $P \in \mathcal{P}$, $v(P) = 1$ for all valuations $v \in \mathcal{L}$. Consequently, we cannot create the truth function

f	
0	1
1	1
2	1

in $\mathcal{L}$. Therefore, $\mathcal{L}$ is functionally incomplete. □

$\mathcal{L}$ can be viewed as a rejection of the law of the excluded middle. Instead of insisting that a proposition must be either true or false, we allow it to take a third value. Indeed, if we let $v(P) = 1$, keeping in mind that 1 now represents the third 'undetermined' truth value,

$$\begin{aligned} v((P \vee \neg P)) &= f_{\vee}(v(P), v(\neg P)) \\ &= f_{\vee}(v(P), f_{\neg}(v(P))) \\ &= f_{\vee}(1, f_{\neg}(1)) \\ &= f_{\vee}(1, 1) \\ &= 1 \end{aligned}$$

we see that $(P \vee \neg P)$ ceases to be a tautology.
The proposition

$$(P \equiv P),$$

known as the **law of identity** remains tautological in $\mathcal{L}$ but interestingly, the proposition

$$(P \equiv \neg P)$$

ceases to be a contradiction and in fact, $v((P \equiv \neg P)) = 2$ when $v(P) = 1$. We can construct a new contradiction for Łukasiewicz logic however, simply taking

$$\neg(P \equiv P).$$

We can see that satisfiability is not maintained when we move into $\mathcal{L}$.

Definition 2.9. *The* ***Boolean Satisfiability Problem for Łukasiewicz logic (SAT$_{\mathcal{L}}$)*** *asks: Is a given propositional formula P satisfiable in $\mathcal{L}$?*

3 An algebraic approach

Now that we have established $\mathrm{SAT}_{\mathcal{L}}$ we will begin the process of reframing the problem in order to take a more algebraic approach. Our goal is to represent propositional formulas as polynomials. Specifically, given our truth value set $\mathcal{V} = \{0, 1, 2\}$, we look at polynomials over the finite field $\mathbb{F}_3$.

Definition 3.1. *Polynomial Łukasiewicz logic ($\mathcal{L}_p$) is defined*

- $\mathcal{V} = \mathbb{F}_3$
- $\mathcal{D} = \{2\}$
- $\mathcal{C} = \{\neg, \wedge, \vee, \rightarrow, \equiv\}$
- *for each n-ary connective $c \in \mathcal{C}$, there is a truth function $f_c : \mathbb{F}_3^{(n)} \rightarrow \mathbb{F}_3$*

$f_\neg$		$f_\wedge$	0	1	2	$f_\vee$	0	1	2	$f_\rightarrow$	0	1	2	$f_\equiv$	0	1	2
0	2	0	0	0	0	0	0	1	2	0	2	2	2	0	2	1	0
1	1	1	0	1	1	1	1	1	2	1	1	2	2	1	1	2	1
2	0	2	0	1	2	2	2	2	2	2	0	1	2	2	0	1	2

- *for each n-ary truth function f_c, there is a polynomial $p_c \in \mathbb{F}_3[x_1, \ldots, x_n]$ such that $p_c = f_c$ when evaluated as a function.*

$v : \mathcal{P} \rightarrow \mathcal{V}$ is defined:

$$v(\neg P) = 2 - v(P) \qquad v((P \rightarrow Q)) = min\{2, 2 - v(P) + v(Q)\}$$
$$v((P \wedge Q)) = min\{v(P), v(Q)\} \qquad v((P \equiv Q)) = 2 - |v(P) - v(Q)|$$
$$v((P \vee Q)) = max\{v(P), v(Q)\}$$

We will first demonstrate that all such functions exist as polynomials, and also establish another important property in the process.

Theorem 2. *Let $R = \mathbb{F}_3[x_1, \ldots, x_n]$ and $S = \{f \mid f : \mathbb{F}_3^{(n)} \rightarrow \mathbb{F}_3\}$. Regarding a polynomial as a function yields a map $O\colon R \rightarrow S$ which is a surjective ring homomorphism with kernel*

$$J = \langle x_1^3 - x_1, x_2^3 - x_2, \ldots, x_n^3 - x_n \rangle.$$

(Here the ring structure of S is given by pointwise addition and multiplication of functions.)

Proof. First, consider S. Each function $f \in S$ takes elements in $\mathbb{F}_3^{(n)}$ and assigns to them elements in $\mathbb{F}_3$. We therefore consider $S \cong \mathbb{F}_3^{(N)}$ where $N = \#\mathbb{F}_3^{(n)} = 3^n$. Let $n = 1$. The map $\omega : \mathbb{F}_3[x] \rightarrow \mathbb{F}_3^{(3)}$, given by evaluating the elements of $\mathbb{F}_3[x]$ at all points $x \in \mathbb{F}_3$, has as its kernel $\langle x^3 - x \rangle$. To see this, note that the factor theorem states:

$$f(\alpha) = 0 \text{ iff } (x - \alpha) \text{ is a factor of } f(x).$$

Therefore if $f(0) = f(1) = f(2) = 0$, then $x(x-1)(x-2) = x^3 - x$ must be a factor of $f(x)$. The map ω is surjective due to the fact that

$$\mathbb{F}_3[x]/\langle x^3 - x\rangle \cong \mathbb{F}_3[x]/\langle x\rangle \times \mathbb{F}_3[x]/\langle x-1\rangle \times \mathbb{F}_3[x]/\langle x-2\rangle \cong \mathbb{F}_3^{(3)}. \quad (4)$$

The first isomorphism follows from the Chinese remainder theorem and the fact that the ideals $\langle x\rangle, \langle x-1\rangle$ and $\langle x-2\rangle$ are mutually coprime. The second isomorphism follows from the evaluation map

$$ev_\alpha : \mathbb{F}_3[x] \to \mathbb{F}_3,$$

which has $\langle x - \alpha\rangle$ as its kernel, and the first isomorphism theorem.
Now let $R = R'[x_n]$ where $R' = \mathbb{F}_3[x_1, \ldots, x_{n-1}]$ and assume the map

$$\rho : R' \to \mathbb{F}_3^{(N')}, N' = 3^{n-1},$$

given by evaluating the elements of R' at all points $(x_1, \ldots, x_{n-1}) \in \mathbb{F}_3^{(n-1)}$, is surjective with kernel $\langle x_1^3 - x_1, x_2^3 - x_2, \ldots, x_{n-1}^3 - x_{n-1}\rangle$.
The map

$$\sigma : R \to R'^{(3)},$$

given by evaluating x_n at all points in $\mathbb{F}_3$, has $\langle x_n^3 - x_n\rangle R'$ as its kernel.
Via similar reasoning to (4) the map is surjective

$$R'[x]/\langle x^3 - x\rangle \cong R'[x]/\langle x\rangle \times R'[x]/\langle x-1\rangle \times R'[x]/\langle x-2\rangle \cong R'^{(3)}.$$

Now consider the map

$$\Omega : R = R'[x_n] \to \mathbb{F}_3^{(N)}$$

which one decomposes as

$$R'[x_n] \to R' \times R' \times R' \to \mathbb{F}_3^{N'} \times \mathbb{F}_3^{N'} \times \mathbb{F}_3^{N'}.$$

This shows that Ω is surjective since it is a composition of surjective maps. By our assumption (induction hypothesis), the rightmost map has kernel

$$\langle x_1^3 - x_1, x_2^3 - x_2, \ldots, x_{n-1}^3 - x_{n-1}\rangle^{\oplus 3}$$

Writing φ for the leftmost map $\varphi\colon R'[x_n] \to R' \times R' \times R'$, the kernel of the composition Ω equals

$$\begin{gathered}\mathrm{Ker}(\varphi) + \varphi^{-1}\left(\langle x_1^3 - x_1, x_2^3 - x_2, \ldots, x_{n-1}^3 - x_{n-1}\rangle^{\oplus 3}\right) \\ = \\ \langle x_1^3 - x_1, x_2^3 - x_2, \ldots, x_n^3 - x_n\rangle.\end{gathered}$$

Induction finishes the proof. □

As we discussed previously, $\mathcal{L}$ is functionally incomplete. Specifically, the constant function $f_P = 1$ does not appear for any propositional formula P. This means that the set of all truth functions in $\mathcal{L}$ is only a subset of S. However,

since O is surjective, any subset of S can be represented in polynomial form. The significance of J is that, since O takes polynomials and views them as functions, the kernel of O precisely describes every polynomial that is always zero. In other words, the ideal J is the set of all contradictions in $\mathcal{L}_p$.

Example 2. Consider the propositional formula $P = \neg(Q \equiv Q)$. We discussed previously that P is a contradiction in $\mathcal{L}$. As we will see in the next section, P can be represented in $\mathbb{F}_3[x]$ by the polynomial

$$\begin{aligned} f_P = 2x^4 + x^3 + x^2 + 2x &= (2x^4 + x^2) + (x^3 + 2x), \\ &= 2x(x^3 + 2x) + (x^3 + 2x), \\ &= (2x + 1)(x^3 + 2x), \\ &= (2x + 1)(x^3 - x). \end{aligned}$$

where in the last equality we used the fact that $2 \cong -1 \mod 3$. Therefore, $f_P \in J$ as expected.

3.1 Polynomization

Now we will define explicitly the polynomial representation of each truth function in $\mathcal{L}_p$.
Negation is our only unary connective and we simply take it as

$$p_\neg(x) = 2 - x.$$

Clearly we have $p_\neg(x) = f_\neg(x)$ for all $x \in \mathbb{F}_3$.
Looking at the binary connectives, the first thing to note is that since $t^3 = t$ for all $t \in \mathbb{F}_3$, $t^n = t$ if n is odd and $t^n = t^2$ if n is even. Therefore, any polynomial representation is equivalent to one of the form

$$p(x, y) = ax^2y^2 + bx^2y + cxy^2 + dx^2 + exy + fy^2 + gx + hy + k : a, b, c, d, e, f, g, h, k \in \mathbb{F}_3.$$

So if we are looking for

$$p(x, y) = f_c(x, y), \forall x, y \in \mathbb{F}_3$$

which is equivalent to

$$p(x, y) - f_c(x, y) = 0, \forall x, y \in \mathbb{F}_3.$$

By computing $p(x, y) - f_c(x, y)$ for each $(x, y) \in \mathbb{F}_3 \times \mathbb{F}_3$ we will produce a system of linear equations that we can solve for the coefficients of p.

Taking $f_\wedge(x, y)$ for example, $p(x, y) - f_\wedge(x, y) : \forall (x, y) \in \mathbb{F}_3 \times \mathbb{F}_3$ gives the following

$$
\begin{aligned}
p(0,0) - f_\wedge(0,0) &= k \\
p(1,0) - f_\wedge(1,0) &= d + g + k \\
p(2,0) - f_\wedge(2,0) &= d + 2g + k \\
p(0,1) - f_\wedge(0,1) &= f + h + k \\
p(1,1) - f_\wedge(1,1) &= a + b + c + d + e + f + g + h + k - 1 \\
p(2,1) - f_\wedge(2,1) &= a + b + 2c + d + 2e + f + 2g + h + k - 1 \\
p(0,2) - f_\wedge(0,2) &= f + 2h + k \\
p(1,2) - f_\wedge(1,2) &= a + 2b + c + d + 2e + f + g + 2h + k - 1 \\
p(2,2) - f_\wedge(2,2) &= a + 2b + 2c + d + e + f + 2g + 2h + k - 2
\end{aligned}
$$

which gives

$$a = 2, b = 2, c = 2, d = 0, e = 1, f = 0, g = 0, h = 0, k = 0$$

and thus

$$p_\wedge = 2x^2y^2 + 2x^2y + 2xy^2 + xy.$$

Via this process we find that the polynomial forms of the remaining interpretations are as follows:

$$
\begin{aligned}
p_\vee(x,y) &= x^2y^2 + x^2y + xy^2 + 2xy + x + y \\
p_\to(x,y) &= 2x^2y^2 + 2x^2y + 2xy^2 + xy + 2x + 2 \\
p_\equiv(x,y) &= x^2y^2 + x^2y + xy^2 + 2xy + 2x + 2y + 2.
\end{aligned}
$$

Example 3. Let's look again at the law of the excluded middle.

$$
\begin{aligned}
v((P \vee \neg P)) &= f_\vee(v(P), f_\neg(v(P))) \\
&= f_\vee(x, f_\neg(x)) \\
&= p_\vee(x, p_\neg(x)) \\
&= x^2 p_\neg(x)^2 + x^2 p_\neg(x) + x p_\neg(x)^2 + 2x p_\neg(x) + x + p_\neg(x) \\
&= x^2(2-x)^2 + x^2(2-x) + x(2-x)^2 + 2x(2-x) + x + (2-x) \\
&= x^2 + x + 2
\end{aligned}
$$

Here we have simply allowed $v(P)$ to be some variable $x \in \mathbb{F}_3$. Just as before, we can see that if $x = 1$

$$(1)^2 + 1 + 2 = 4 \cong 1$$

Theorem 3. *Let P be a propositional formula in $\mathcal{L}$. P is satisfiable if and only if its polynomial representation in $\mathcal{L}_p$ equals 2 for some variable assignment.*

Proof. If P is a propositional atom then we simply let $v(P) = x$. Clearly,

$$v(P) = 2 \leftrightarrow x = 2.$$

Otherwise, P is made up of some combination of connectives. From the definition of the valuation function (1), for n-ary connective

$$v(c(A_1, \ldots, A_n)) = f_c(v(A_1), \ldots, v(A_n)).$$

And by construction, we have

$$f_c(v(A_1), \ldots, v(A_n)) = p_c(v(A_1), \ldots, v(A_n)).$$

Therefore for any connective, we have

$$v(c(A_1, \ldots, A_n)) = p_c(v(A_1), \ldots, v(A_n))$$

and so

$$v(c(A_1, \ldots, A_n)) = 2 \leftrightarrow p_c(v(A_1), \ldots, v(A_n)) = 2.$$

Since any propositional formula is constituted of some combination of atoms and connectives, this concludes the proof. □

3.2 Finding zeros in $\mathbb{F}_3[x_1, \ldots, x_n]$

We will now formulate a critical result which will allow us to solve $\mathrm{SAT}_{\mathcal{L}}$.

Theorem 4. *Let* $f \in \mathbb{F}_3[x_1, \ldots, x_n]$ *and*

$$I = \langle f, x_1^3 - x_1, x_2^3 - x_2, \ldots, x_n^3 - x_n \rangle, I \subset R = \mathbb{F}_3[x_1, \ldots, x_n]$$

If $1 \in I$*, then* f *has no zero in* $\mathbb{F}_3^{(n)}$*. Otherwise,* f *has a zero in* $\mathbb{F}_3^{(n)}$*.*

Proof. Let $1 \in I$. We must be able to write

$$1 = c_0 f + c_1(x_1^3 - x_1) + \ldots + c_n(x_n^3 - x_n), c_i \in R.$$

By construction, $x_i^3 - x_i = 0$ for all $x = (x_1, \ldots, x_n) \in \mathbb{F}_3^{(n)}$. So, for all $x \in \mathbb{F}_3^{(n)}$ we have

$$1 = c_0(x) \cdot f(x)$$

If there existed an x such that $f(x) = 0$, then we would have $1 = 0$. Therefore, there exists no x such that $f(x) = 0$. Let $I = J + Rf$, where

$$J = \langle x_1^3 - x_1, \ldots, x_n^3 - x_n \rangle$$

The map $R/J \to R/I$ is surjective with kernel Rf/J, via the first ring homomorphism theorem. If 1 is not in I, then Rf/J is a **proper** subset of R/J. Suppose f has no zero. Then $f^2 = 1$ and $f^2 - 1$ is in J. Therefore, $Rf^2/J = R/J$. Since $Rf^2/J \subset Rf/J$, we have $R/J \subset Rf/J$. This is a contradiction since $Rf/J \subsetneq R/J$. Therefore, if $1 \in I$, then f must have a zero. □

Note that this theorem allows us to determine if f has a zero, but we want to know if there exists an assignment such that $f = 2$. The fix for this is rather straightforward. We instead consider the polynomial $f' = f - 2$. If f' has no zero, then there is no assignment such that $f = 2$. If f' has a zero, then there does exist such an assignment.

At this point, the outline for solving $\mathrm{SAT}_{\mathcal{L}}$ begins to come into focus. We take some propositional formula $P \in \mathcal{L}$ and represent it as a polynomial $f_P \in \mathbb{F}_3[x_1, \ldots, x_n]$. This defines the associated polynomial $f'_P = f_P - 2$. We then construct the ideal

$$I = \langle f'_P, x_1^3 - x_1, \ldots, x_n^3 - x_n \rangle.$$

If $1 \notin I$, then $f_P = 2$ for some $(x_1, \ldots, x_n) \in \mathbb{F}^{(n)}$ and thus P is satisfiable. Otherwise, $f_P = 2$ for no $(x_1, \ldots, x_n) \in \mathbb{F}^{(n)}$ and P is unsatisfiable. We will now discuss how we will determine if $1 \in I$.

4 What is a Gröbner basis?

4.1 Introduction

Gröbner bases were introduced by Bruno Buchberger along with the algorithm for computing them in 1965 in his PhD thesis. Named for his doctoral advisor, Wolfgang Gröbner, they have since become an important tool for many different varieties of algebra. The key advantages of Gröbner bases include showing equality between ideals, solving systems of polynomial equations, and, for our purposes, determining if a polynomial is a member of an ideal.

4.2 Monomial ordering

Definition 4.1. *Let k be a field. A **monomial** in $k[x_1, \ldots, x_n]$ is a polynomial of the form*

$$cx_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

where $c, x_i \in k$ and $\alpha_i \in \mathbb{Z}_{\geq 0}$. We write

$$cx_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} = cx^{\alpha}$$

where $x = (x_1, \ldots, x_n) \in k^{(n)}$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^{(n)}$.

Definition 4.2. *Let k be a field. A **monomial ordering** on $k[x_1, x_2, ..., x_n]$ is any relation $>$ on $\mathbb{Z}_{\geq 0}^{(n)}$ or equivalently, any relation on the set of monomials x^{α}, $\alpha \in \mathbb{Z}_{\geq 0}^{(n)}$, such that:*

1. *$>$ is a total ordering on $\mathbb{Z}_{\geq 0}^{(n)}$.*
2. *If $x^{\alpha} > x^{\beta}$ and $\gamma \in \mathbb{Z}_{\geq 0}^{(n)}$, then $x^{\alpha+\gamma} > x^{\beta+\gamma}$.*
3. *$>$ is a well-ordering on $\mathbb{Z}_{\geq 0}^{(n)}$.*

A monomial ordering is essentially a rule that allows us to put the terms of a multivariate polynomial in a specific and consistent order. There are many different possible monomial orderings with their own pros and cons, typically in computational efficiency. For our purposes however we will use the most simple ordering, known as lexicographic ordering.

Definition 4.3. *(Lexicographic ordering) Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}_{\geq 0}^{(n)}$. If the leftmost entry of $\alpha - \beta \in \mathbb{Z}^{(n)}$ is positive, then $\alpha >_{lex} \beta$. If $\alpha >_{lex} \beta$, then $x^{\alpha} >_{lex} x^{\beta}$.*

Example 4. Some examples:

1. $xy^3z^2 >_{lex} y^4z^3$ since $\alpha - \beta = (1, -1, -1)$.
2. $x^2y^2z >_{lex} x^2yz^3$ since $\alpha - \beta = (0, 1, -2)$.

3. $x^2y^2z^3 >_{lex} 2xy^2z$ since $\alpha - \beta = (1, 0, 2)$.

Definition 4.4. *Let $f = \sum_\alpha c_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \ldots, x_n]$ and let $>$ be a monomial order.*

1. *The **multidegree** of f is*

$$multideg(f) = max(\alpha \in \mathbb{Z}^n_{\geq 0} : c_\alpha \neq 0)$$

where the maximum is taken with respect to the monomial ordering $>$.

2. *The **leading coefficient** of f is*

$$LC(f) = c_{multideg(f)} \in k.$$

3. *The **leading monomial** of f is*

$$LM(f) = x^{multideg(f)}.$$

4. *The **leading term** of f is*

$$LT(f) = LC(f) \cdot LM(f).$$

Example 5. Consider the polynomial $f = 2x^2y^3z + 2x^2z + z^2$ with respect to the lexicographic ordering.

$$\begin{aligned} multideg(f) &= (2, 3, 1) \\ LC(f) &= 2 \\ LM(f) &= x^2y^3z \\ LT(f) &= 2x^2y^3z \end{aligned}$$

4.3 Division algorithm

We present a division algorithm that will allow us to divide a polynomial $f \in k[x_1, \ldots, x_n]$ by a set of polynomials $f_1, \ldots, _s \in k[x_1, \ldots, x_n]$. It allows us to write $f = \sum_{i=1}^s a_i f_i + r$ with $a_1, \ldots, a_s, r \in k[x_1, \ldots, x_n]$. We consider r to be the remainder of f on division by $\{f_1, \ldots, f_s\}$ and therefore is not divisible by $LT(f_i)$ for any i. With respect to a monomial ordering, the division algorithm proceeds as follows:

Data: $f_1, \ldots, f_s, f$
Result: $a_1, \ldots, a_s, r$ such that $f = \sum_{i=1}^{s} a_i f_i + r$
Initialization: $a_1 := 0, \ldots, a_s := 0, r := 0, p := f$;

while $p \neq 0$ **do**
  if $\{i \mid LT(f_i)$ *divides* $LT(p)\} \neq \emptyset$ **then**
    $i := min\{i \mid LT(f_i)$ *divides* $LT(p)\}$;
    $a_i := a_i + \dfrac{LT(p)}{LT(f_i)}$;
    $p := p - \dfrac{LT(p)}{LT(f_i)} f_i$;
  else
    $r := r + LT(p)$;
    $p := p - LT(p)$;
  end
end

Theorem 5. *Fix a monomial order and let $F = \{f_1, \ldots, f_s\}$ be an ordered s-tuple of polynomials in $k[x_1, \ldots, x_n]$. Then every f can be written as*

$$f = \sum_{i=1}^{s} a_i f_i + r$$

where $a_i, r \in k[x_1, \ldots, x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in k, of monomials, none of which is divisible by any of the $LT(f_1), \ldots, LT(f_s)$. Furthermore, we can show that if $a_i f_i \neq 0$, then we have $multideg(f) \geq multideg(a_i f_i)$.

Proof. [2] Theorem 3.2 □

Example 6. Let's try dividing $f = x^3y^2 + xy + x$ by $f_1 = y^2 + 1$ and $f_2 = xy + 1$, $f, f_1, f_2 \in \mathbb{F}_3[x_1, \ldots, x_n]$. First, let $a_1 = a_2 = r = 0$ and $p = x^3y^2 + xy + x$. We look to see if any $LT(f_i)$ divides $LT(p)$ and it turns out both $LT(f_1)$ and $LT(f_2)$ both do. So we begin

$$\begin{aligned} i &= 1, \\ a_1 &= 0 + \frac{LT(p)}{LT(f_1)} = \frac{x^3y^2}{y^2} = x^3, \\ p &= x^3y^2 + xy + x - x^3(y^2 + 1), \\ &= x^3y^2 + xy + x - x^3y^2 - x^3, \\ &= -x^3 + xy + x. \end{aligned}$$

Returning to the top of the if statement, we see that no $LT(f_i)$ divides $LT(p)$. So we proceed,

$$\begin{aligned} r &= 0 + (-x^3) = -x^3, \\ p &= -x^3 + xy + x - (-x^3) = xy + x. \end{aligned}$$

Returning to the top again we see that $LT(f_2)$ divides $LT(p)$.

$$\begin{aligned} i &= 2, \\ a_2 &= 0 + 1 = 1, \\ p &= xy + x - (xy + 1), \\ &= xy + x - xy - 1, \\ &= x - 1. \end{aligned}$$

Now, no $LT(f_i)$ divides $LT(p)$, so

$$\begin{aligned} r &= -x^3 + x, \\ p &= -1. \end{aligned}$$

And once again, no $LT(f_i)$ divides $LT(p)$, so

$$\begin{aligned} r &= -x^3 + x - 1 \cong 2x^3 + x + 2, \\ p &= 0. \end{aligned}$$

Now we have $p = 0$ so the algorithm terminates. We can see that our output has the desired form

$$\begin{aligned} a_1 f_1 + a_2 f_2 + r &= x^3(y^2 + 1) + (xy + 1) + (2x^3 + x + 2), \\ &= x^3 y^2 + 3x^3 + xy + x + 3, \\ &\cong x^3 y^2 + xy + x = f. \end{aligned}$$

4.4 Gröbner basis

Definition 4.5. *Let $I \in k[x_1, \ldots, x_n]$ be a nonzero ideal.*

1. *Let $LT(I)$ be the set of leading tearms of elements of I.*

$$LT(I) = \{cx^a | \text{ there exists } f \in I \text{ with } LT(f) = cx^a\}$$

2. *We denote by $\langle LT(I) \rangle$ the ideal generated by the elements of $LT(I)$.*

We are now finally ready to give the definition of a Gröbner basis.

Definition 4.6. *Fix a monomial ordering on $k[x_1, \ldots, x_n]$. A finite set of nonzero polynomials $G = \{g_1, \ldots, g_t\}$ contained in an ideal I is a **Gröbner basis** for I if*

$$\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle.$$

Theorem 6. *Let I be a non-zero ideal of $k[x_1, \ldots, x_n]$ and $G = \{g_1, \ldots, g_t\} \subseteq I$ be a Gröbner basis for I. Then for some $f \in k[x_1, \ldots, x_n]$, $f \in I$ if and only if the remainder of f on division by G is zero.*

Proof. [1] Theorem 1.6.2 □

Let's summarise our position now with respect to solving $\text{SAT}_{\mathcal{L}}$. We have shown that a propositional formula $P \in \mathcal{L}$ is satisfiable if and only its polynomial representation $f_P \in \mathbb{F}_3[x_1, \ldots, x_n]$ achieves the value 2 for some $(x_1, \ldots, x_n) \in \mathbb{F}_3^{(n)}$. Furthermore, we showed that f_P achieves such a value if and only if the ideal $I = \langle f'_P, x_1^3 - x_1, \ldots, x_n^3 - x_n \rangle \subset \mathbb{F}_3[x_1, \ldots, x_n]$ does not contain 1. We have just seen that $1 \in I$ if and only if the remainder of 1 on division by G, a Gröbner basis for I, is zero. We will now see that a Gröbner basis can always be constructed in a finite number of steps.

Definition 4.7. *Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials.*

1. *If $multideg(f) = \alpha$ and $multideg(g) = \beta$, then let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = max(\alpha_i, \beta_i)$ for each i. We call x^γ the **least common multiple** of $LT(f)$ and $LT(g)$.*
2. *The **S-polynomial** of f and g is given by:*

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g.$$

Theorem 7. *(Buchberger's Criterion) Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ for I is a Gröbner basis if and only if the remainder on division of $S(g_i, g_j)$ by G, denoted $\overline{S(g_i, g_j)}^G$, is zero for all $i \neq j$.*

Proof. [1] Theorem 1.7.4 □

Theorem 8. *(Buchberger's Algorithm) Let I be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps. Let*

$$F = \{f_i | \langle f_1, \ldots, f_s \rangle = I\}.$$

1. *Let $G = \{g_1, \ldots, g_s\}$, where each $g_i = f_i$. If any g_i divides some g_j, $i \neq j$, then remove g_j from G. Let $\Gamma = \{\{f_i, f_j\} \mid f_i \neq f_j \in G\}$.*
2. *While $\Gamma \neq \emptyset$:*
   - *2.1 Choose any $\{f, g\} \in \Gamma$.*
   - *2.2 Remove $\{f, g\}$ from Γ.*
   - *2.3 Let $h = \overline{S(f, g)}^G$.*
   - *2.4 If $h \neq 0$:*
     - *2.4.1 Add $\{\{u, h\} \mid \forall u \in G\}$ to Γ.*
     - *2.4.2 Add h to G.*

Proof. [1] Theorem 1.7.6 □

We thereby conclude our method for solving $\mathrm{SAT}_{\mathcal{L}}$. For any propositional formula $P \in \mathcal{L}$ we compute its polynomial representation $f_P \in \mathbb{F}_3[x_1, \ldots, x_n]$ and produce the ideal $I = \langle f'_P, x_1^3 - x_1, \ldots, x_n^3 - x_n \rangle \subset \mathbb{F}_3[x_1, \ldots, x_n]$. We construct a Gröbner basis G for I and calculate the remainder r of 1 on division by G. P is satisfiable if and only if $r = 0$.

Example 7. Consider once again the law of the excluded middle, $(P \vee \neg P)$. We showed previously in example (3) that it has the polynomial representation

$$f_{(P \vee \neg P)} = x^2 + x + 2,$$

so we let

$$\begin{aligned} f'_{(P \vee \neg P)} &= x^2 + x, \\ I &= \langle x^2 + x, x^3 - x \rangle. \end{aligned}$$

We will now compute a Gröbner basis for I. To start, we let

$$\begin{aligned} F &= \{f_1, f_2\}, && \text{where } f_1 = x^2 + x, f_2 = x^3 - x, \\ G &= \{g_1, g_2\}, && \text{where } g_1 = f_1, g_2 = f_2, \end{aligned}$$

We notice that $g_1 = x^2 + x = x(x+1)$ divides $g_2 = x^3 - x = x(x+1)(x-1)$ so G becomes

$$G = \{g_1\}.$$

Since $\Gamma = \emptyset$, we conclude that $G = \{g_1\}$ is a Gröbner basis for I. Therefore, since no $g_i \in G$ divides 1, $(P \vee \neg P)$ is satisfiable.

Example 8. Consider the propositional formula $(P \wedge \neg P)$.

$$\begin{aligned} f_{(P \wedge \neg P)} &= f_{\wedge}(v(P), f_{\neg}(v(P))), \\ &= 2x^2(2-x)^2 + 2x^2(2-x) + 2x(2-x)^2 + x(2-x), \\ &= 2x^4 + 4x^3 + 2x^2 + 4x^2 - 2x^3 + 2x^3 + 4x^2 + 2x + 2x - x^2, \\ &= 2x^2 + 2x, \end{aligned}$$

so we let

$$\begin{aligned} f'_{(P \wedge \neg P)} &= 2x^2 + 2x - 2 = 2x^2 + 2x + 1, \\ I &= \langle 2x^2 + 2x + 1, x^3 - x \rangle. \end{aligned}$$

Now to compute a Gröbner basis.

$$\begin{aligned} F &= \{f_1, f_2\}, && \text{where } f_1 = 2x^2 + 2x + 1, f_2 = x^3 - x, \\ G &= \{g_1, g_2\}, && \text{where } g_1 = f_1, g_2 = f_2, \\ \Gamma &= \{\{g_1, g_2\}, \{g_2, g_1\}\}. \end{aligned}$$

Choose $\{g_1, g_2\}$ and remove it from Γ so

$$\Gamma = \{\{g_2, g_1\}\}.$$

To calculate $S(g_1, g_2)$, first observe that $x^\gamma = 2x^3$.

$$\begin{aligned} S(g_1, g_2) &= \frac{x^\gamma}{LT(g_1)} \cdot g_1 - \frac{x^\gamma}{LT(g_2)} \cdot g_2, \\ &= \frac{2x^3}{2x^2} \cdot (2x^2 + 2x + 1) - \frac{2x^3}{x^3} \cdot (x^3 - x), \\ &= x(2x^2 + 2x + 1) - 2(x^3 - x), \\ &= 2x^3 + 2x^2 + x - 2x^3 + 2x, \\ &= 2x^2. \end{aligned}$$

$S(g_1, g_2) = g_1 + x + 2$ and so $h = \overline{S(g_1, g_2)}^G = x + 2$. Letting $h = g_3$,

$$\begin{aligned} \Gamma &= \{\{g_2, g_1\}, \{g_1, g_3\}, \{g_2, g_3\}\}, \\ G &= \{g_1, g_2, g_3\}. \end{aligned}$$

Choose $\{g_1, g_3\}$,

$$\Gamma = \{\{g_2, g_1\}, \{g_2, g_3\}\}.$$

To calculate $S(g_1, g_3)$, first observe that $x^\gamma = 2x^2$.

$$\begin{aligned} S(g_1, g_2) &= \frac{x^\gamma}{LT(g_1)} \cdot g_1 - \frac{x^\gamma}{LT(g_3)} \cdot g_3, \\ &= \frac{2x^3}{2x^2} \cdot (2x^2 + 2x + 1) - \frac{2x^3}{x} \cdot (x + 2), \\ &= x(2x^2 + 2x + 1) - 2x(x + 2), \\ &= 2x^2 + 2x + 1 - 2x^2 - 4x, \\ &= -2x + 1, \\ &= x + 1. \end{aligned}$$

$S(g_1, g_3) = g_3 + 2$ and so $h = \overline{S(f_1, f_2)}^G = 2$. Letting $h = g_4$,

$$\begin{aligned} \Gamma &= \{\{g_2, g_1\}, \{g_2, g_3\}, \{g_1, g_4\}, \{g_2, g_4\}, \{g_3, g_4\}\} \\ G &= \{g_1, g_2, g_3, g_4\}. \end{aligned}$$

At this point we may terminate the algorithm. We have shown that $g_4 = 2 \in G$, so $2(2) = 1 \in I$. $(P \wedge \neg P)$ is therefore unsatisfiable.

5 Conclusion

In this thesis, we have presented a method for solving the Boolean Satisfiability Problem for Łukasiewicz logic. The focus wasn't to show that this method is optimal, merely to show that it exists. Further work could be done to streamline the process, perhaps by finding an easier way to determine if $1 \in I$. Again, the computational complexity of $\mathrm{SAT}_{\mathcal{L}}$ wasn't the focus of this thesis, but it would be interesting to investigate this method's impact on the complexity of $\mathrm{SAT}_{\mathcal{L}}$. Furthermore, the method of translating propositional formulas into polynomials allows for a huge number of possibilities. Considering the wealth of algebraic theory available to us, it would be very interesting to see what other, completely different methods are available for solving this problem.

References

[1] WILLIAM W. ADAMS and PHILLIPE LOUSTAUNAU. *Introduction to grobner bases*. AMER MATHEMATICAL SOCIETY, 2022.

[2] P. W. BAKKER-KLOOSTER. An algebraic approach to the boolean satisfiability problem. Master's thesis, 2016.

[3] Miquel Bofill, Felip Manyà, Amanda Vidal, and Mateu Villaret. The complexity of 3-valued łukasiewicz rules. *Modeling Decisions for Artificial Intelligence*, page 221–229, 2015.

[4] Grzegorz Malinowski. *Many-valued logics*. Clarendon Press, 1993.