AN ALGEBRAIC STRUCTURE EQUIVALENT TO PROPOSITIONAL LOGIC

TAYLOR DUPUY

Abstract. A given propositional formula can be expressed as a a polynomial over $\mathbb{F}_2[x_1, x_2, \ldots, x_n]$. Expressing propositional formulas as polynomials gives us a very interesting structure to study. First we show that solving polynomial equations over $\mathbb{F}_2$ is an NP-complete problem. We next show that a given proposition is not satisfiable if and only if its polynomial has an irreducible factor with no solutions over the finite field. And finally, we interpret field extensions of $\mathbb{F}_2$ as logical extensions of the standard truth values. In this interpretation propositional forms like $X \wedge !X$ are satisfiable!

1. 3SAT

The *3SAT problem* asks you to find a polynomial time algorithm to determine the satisfiability of propositions in 3 Conjunctive Normal Form. Let $\vee$ mean "or" (for the latin vel), $\wedge$ mean "and", and ! means "not', This is essentially asking if

$$[X \vee Y \vee !Z] \wedge [X \vee !U \vee Y] \wedge [Y \vee Z \vee U]$$

has a valuation which make the sentence true. That is, find a substitution for X, Y, Z and U such that proposition will evaluate to true. In this example setting $X =$ True and $Y =$ True is enough to satisfy the formula (It doesn't matter how we set U or Z).

Looking at this problem is perceivably easier to understand in a framework which is well studied algorithmically. The idea was to convert these into the polynomials over the Galois field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ and try and study the algorithms in find roots finding of these polynomials.

2. Logic and $\mathbb{F}_2$

To do this, let 1 represent true and 0 represent false. It is well known that addition over $\mathbb{F}_2$ corresponds to the exclusive or operation. We will use xor for it in the propositional calculus. Similarly $\wedge$ converts to multiplication.

This is essentially saying $a + b$ over $\mathbb{F}_2$ is equivalent to (A xor B) and ab is equivalent to $(A \wedge B)$; this correspondence allows you to construct polynomials equivalent to propositional forms. See table 1 for a correspondence between the simplest propositional forms and polynomials over $\mathbb{F}_2$.

Knowing this, we can try converting some of our favorite propositional forms into polynomials.

- $((X \vee Y \vee Z) \wedge U)$ converts to $((x + y + xy) + z + (x + y + xy)z)u = xu + yu + xyu + zu + xzu + yzu + xyzu$.

The reason for doing this is because the algorithmic properties of roots finding have been well studied (because of Hilbert's 10th problem).

Propositional Calculus	$\mathbb{F}_2[a,b]$
True	1
False	0
$!A$	$a+1$
$A \wedge B$	ab
A xor B	$a+b$
$A \vee B$	$(a+b)+ab$
A nand B	$ab+1$
$A \implies B$	$ab+a+1$

Table 1. Correspondence between simple propositional formulas in propositional variables A and B and their corresponding polynomials over $\mathbb{F}_2$ with indeterminates a and b.

Finding roots over for these polynomials is equivalent to the satisfiability problem. Given a propositional from like the example above—you can convert it to a polynomial, set that polynomial equal to 1 and then look for roots.

For example, asking if $(X \vee X)$ is satisfiable is equivalent to asking if $x^2+x+x = x^2 = 1$ has a solution over $\mathbb{F}_2$. Again, we convert $X \vee X$ into a polynomial then set that polynomials equal to 1 (set the propositional form equal to true). The solutions of $x^2+1=0$ are 1 and 1—Since $(x^2+1) = (x+1)(x+1)$. Note that we have a root of multiplicity two at $x=1$! The polynomial representation makes x appear "doubly true" which is a neat property—it accounts for the *multiplicity* of the formula.

Similarly, when a proposition is unsatisfiable (i.e. we can't find a solution over $\mathbb{F}_2$) it's polynomial will be an irreducible with degree greater than 1.

For example take $(X \wedge !X)$. Satisfiability is equivalent to finding solutions of $x^2+x+1=0$. Since this polynomial doesn't have any roots in F_2 it is unsatisfiable. This is a general property.

Theorem 2.1. *A propositional form P is satisfiable if and only its polynomial has an irreducible factor which roots over $\mathbb{F}_2$.*

Now, because this conversion of propositional forms can be done in polynomial time, answering the question of whether a polynomial in multiple indeterminants has roots in $\mathbb{F}_2^n$ would give a solution to 3CNF in polynomial time. Thus root finding over $\mathbb{F}_2$ is an NP-complete problem.

Proposition 2.2. *The Language of encoded polynomials*

$$L = \{\langle f\rangle | f \in \mathbb{F}_2[X] \text{ and there exists some } A \in \mathbb{F}_2^k \text{ such that } f(A) = 0.\}$$

is NP-complete.

3. Algebraic Extensions

These polynomials have another very interesting property, You can use field extensions to satisfy propositions which are unsatisfiable over $\mathbb{F}_2$! That is consider the field extension in which you can find roots of the polynomials which are normally irreducible. This is tantamount to extending Truth Tables since the two problems are equivalent.

For a concrete example, consider $(X\wedge !X)$. This proposition is satisfiable over a logic with valuations in $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$.

It currently seems seems difficult to extend this to predicate logic. This would be interesting because for many reasons. Although it appears that unsatisfiable axioms would never come up in practice physicists seem to have them. The example that I'm thinking of is a combinatorial version of the EPR (Einstein, Podolsky, and Rosen) paradox, Called the Kochen-Specker paradox. The paradox is studied by John H. Conway and discussed in a video lecture online in which he provides axioms which can be converted into predicate logic [**?**].

In addition to the above there may be different interpretations of provability. Does any thing change about Gödel's *completeness* theorems—are the methods of proof still the same in the extension? See `www.u.arizona.edu/~tdupuy` for more information.