Understanding Weak Nullstellensatz and equivalence check

Vikas Rao
Department of Electrical and Computer Eng.
University of Utah, Salt Lake City, UT-84112
Vikas.k.rao@utah.edu

***Abstract*—$Nullstellensatz$ is a celebrated theorem which helps find the correspondence between ideals and varieties. The theorem will help us create a glossary between geometry and algebra, which in turn helps realize and model statements on varieties as expressions of ideals, and vice versa. We will try and understand the Weak $Nullstellensatz$, which is the first postulate to relate ideals and varieties over a finite field as well as it's algebraically closed counterpart. We shall also look into formulating a equivalence check over two different implementations of a circuit, convert them to CNF-SAT and solve them using a SAT solver, and verify the equivalence over Weak $Nullstellensatz$ as well.**

I. Introduction

A. Groundwork

Let $F = f_1, f_2...f_s$ denote a set of polynomials belonging to a finite field $\mathbb{F}_q$, and let $\overline{\mathbb{F}_q}$ be it's algebraically closed complement. Let $R = \mathbb{F}_q\{x_1, x_2...x_n\}$ be any ring in variables $x_i, 1 \leq i \leq n$ with it's coefficient from $\mathbb{F}_q$.

Let $J \subseteq R$ be the ideal generated from polynomials F which is given as

$$J = \langle f_1, f_2 \ldots, f_s \rangle \tag{1}$$

The set of solutions for polynomial equations $F = 0$, as in $\{f_1 = 0, f_2 = 0..f_s = 0\}$ is called a variety and let V denote such variety. The Varieties generated are actually dependent on the $ideal$ J and not on the polynomial itself, hence we can represent the varieties as a function of $ideals$; $V(J)$. Since the ideals here are defined over the finite fields, we can actually specify variety of ideals in terms of finite field as $V_{\mathbb{F}_q}(J)$. Let GB represent the Gröbner basis over a given field.

II. weak *Nullstellensatz*

A. Algebraically closed fields $\bar{\mathbb{F}}_q$

The motive behind weak $Nullstellensatz$ is to reason about presence or absence of feasible solutions to a given $ideal$ over algebraically closed fields. Stating the theorem formally -

Theorem 2.1: Let $J = \langle f_1, f_2 \ldots, f_s \rangle$ be an ideal over the algebraically closed field $\bar{\mathbb{F}_q}[x_1, x_2..x_n]$ and let $V_{\bar{\mathbb{F}_q}}(J)$ be it's variety. Given $J \subset \bar{\mathbb{F}_q}[x_1, x_2..x_n]$, $V_{\bar{\mathbb{F}_q}}(J) = \emptyset \Leftrightarrow J = \bar{\mathbb{F}_q}[x_1, x_2..x_n] \Leftrightarrow 1 \in J \Leftrightarrow GB = \{1\}$.

The theorem signifies that, over algebraically closed fields, if variety of a given $ideal$ is empty, then the $ideal$ encompasses the entire field. This implies that J also contains the unit constant as one of the elements.If we approach the problem from a Gröbner Basis perspective, the reduced GB over this J after finite number of iterations will end up with a unit polynomial as well, which can be used to reconstruct the entire Gröbner Set and in fact the whole Ring itself.

B. Not algebraically closed fields $\mathbb{F}_q$

Theorem 2.2: Let $J = \langle f_1, f_2 \ldots, f_s \rangle$ be an ideal over the field $\mathbb{F}_q[x_1, x_2..x_n]$ and let $\bar{\mathbb{F}_q}$ be it's algebraic closure. Let $V_{\bar{\mathbb{F}_q}}(J)$ be it's variety over $\mathbb{F}_q$. Given $J \subset \mathbb{F}_q[x_1, x_2..x_n]$, $V_{\bar{\mathbb{F}_q}}(J) = \emptyset \Leftrightarrow 1 \in J \Leftrightarrow GB = \{1\}$.

Over non closed fields, the theorem signifies that if variety of a given $ideal$ J is empty, then the unit constant should be part of ideal J. This also infers no solution over algebraic closure $\bar{\mathbb{F}}_q$, hence implying no solution over $\mathbb{F}_q$ as well. To check if unit constant is part of the $ideal$ J, we need to do ideal membership testing by computing Grobner basis.

Proof 1: Because it's tedious to compute solutions over finite fields, we need to consider the algebraically closed forms for the proof. We will see how to relate variety of $ideals$ over finite fields as compared to it's algebraically closed counterpart.

Let's consider $J_0 = \langle x_1^q - x_1..x_n^q - x_n \rangle$ as the set of vanishing polynomials over algebraically closed field. These polynomials when coupled with finite field, restrict the solutions to finite fields. we also know that variety of J_0 doesn't change over the closure and is equal to $V_{\bar{\mathbb{F}_q}}(J_0) = \mathbb{F}_q$.

Now to find out the existing solutions within the finite field, we need to find the intersection of varieties across algebraic closed fields and the finite field itself.

$$V_{\mathbb{F}_q}(J) = V_{\bar{\mathbb{F}_q}}(J) \cap \mathbb{F}_q$$
$$V_{\mathbb{F}_q}(J) = V_{\bar{\mathbb{F}_q}}(J) \cap V_{\mathbb{F}_q}(J_0)$$
$$V_{\mathbb{F}_q}(J) = V_{\bar{\mathbb{F}_q}}(J) \cap V_{\bar{\mathbb{F}_q}}(J_0)$$

we know that, intersection over varieties is addition in ideals-

$$V_{\mathbb{F}_q}(J) = V_{\bar{\mathbb{F}_q}}(J + J_0)$$

Hence to check if unit constant is a part of any finite field ideal, we can check if it is part of $J + J_0$ over it's algebraically closed field.

III. Equivalence check using SAT and *Nullstellensatz*

A. Using SAT

Let's take an example of two circuits whose equations are given as follows

$$f = (a \vee (\neg a \wedge b)) \tag{2}$$
$$g = (a \vee b) \tag{3}$$

We need to prove that either there exists no assignment which makes $f! = g$ (UNSATisfiable - functionality of two different implementations are same) or there exists an assignment which makes $f! = g$ (SATisfiable - the implementations are different).

Let's introduce some intermediate variables in the circuit to generate a CNF form. Let M be the final miter(XOR) output which will output 0 (both implementations same) if both it's inputs are same, or 1 (both implementations different) if the inputs are different.

$$M = f \oplus g$$

Using double implication rule, we can write the CNF for all the variables as follows

$i_1 = \neg a \implies (\neg i_1 \vee \neg a) \wedge (\neg i_i \vee a)$
$i_2 = i_1 \wedge b \implies (\neg i_2 \vee i_1) \wedge (\neg i_2 \vee b) \wedge (i_2 \vee \neg i_1 \vee \neg b)$
$f = i_2 \vee a \implies (i_2 \vee a \vee \neg f) \wedge (\neg i_2 \vee f) \wedge (\neg a \vee f)$
$g = a \vee b \implies (a \vee b \vee \neg g) \wedge (\neg a \vee g) \wedge (\neg b \vee g)$
$M = f \oplus g \implies (\neg f \vee \neg g \vee \neg M) \wedge (f \vee g \vee \neg M) \wedge (f \vee \neg g \vee M) \wedge (\neg f \vee g \vee M)$

To generate the final CNF-SAT for the full circuit, we will merge all the individual clauses into one and also add an additional clause in the form of M, as we need to find any satisfying assignment which can break the equivalence and make the output variable $M = 1$.
CNF-SAT for the circuit -

$(\neg i_1 \vee \neg a) \wedge (\neg i_i \vee a) \wedge (\neg i_2 \vee i_1) \wedge (\neg i_2 \vee b) \wedge (i_2 \vee \neg i_1 \vee \neg b) \wedge (i_2 \vee a \vee \neg f) \wedge (\neg i_2 \vee f) \wedge (\neg a \vee f) \wedge (a \vee b \vee \neg g) \wedge (\neg a \vee g) \wedge (\neg b \vee g) \wedge (\neg f \vee \neg g \vee \neg M) \wedge (f \vee g \vee \neg M) \wedge (f \vee \neg g \vee M) \wedge (\neg f \vee g \vee M) \wedge (M)$

we will generate a standard CNF file format from the given clauses to feed a SAT solver. The CNF file content for this circuit with the variable ordering and index $(a-1, b-2, i_1-3, i_2-4, f-5, g-6, M-7)$ is as given below.

```
c cnf-sat file for equivalence check of two circuits
p cnf 7 16
-3 -1 0
3 1 0
-4 3 0
-4 2 0
4 -3 -2 0
4 1 -5 0
-4 5 0
-1 5 0
1 2 -6 0
-1 6 0
-2 6 0
-5 -6 -7 0
5 6 -7 0
5 -6 7 0
7 0
-5 6 7 0
```

For the above CNF, picosat returns no satisfying assignments, thus deeming the two implementations equivalent.

B. Using weak nullstellensatz

We will formulate the equivalence check of the same circuit using $nullstellensatz$ over finite field.

For simplicity let's consider a Boolean ring over mod 2 for operation, and build an $ideal$ over $\mathbb{Z}_2$..

$f = (a \vee (\neg a \wedge b)) \implies f + a + (1+a)b + a(1+a)b$
$g = (a \vee b) \implies g + a + b + ab$

We need to prove that there exists no assignment which makes $f! = g$ and hence we need an additional polynomial representation for the outputs as part of $ideal$ - $f \neq g \implies f + g + 1$

The Gröbner basis(GB) over these $ideals$ -$GB(J)$, with a Lexicographic variable order $f > g > a > b$ using Buchberger's algorithm yields these results -

$$a^2b + ab + 1 \tag{4}$$
$$f + ab + a + b + 1 \tag{5}$$
$$g + ab + a + b \tag{6}$$

We can see that the unit constant is not part of the GB, but the variety $V(J) = \emptyset$, thus signifying that either there is a bug or our formulation is incomplete. To compute the correct formulation we also need to add vanishing polynomials as part of ideals and then compute $GB(J + J_0)$. where J_0 over boolean mod(2) field is given as

$$J_0 = \{f^2 - f, g^2 - g, a^2 - a, b^2 - b\} \tag{7}$$

over generic field $\mathbb{Z}_q$

$$J_0 = \{f^q - f, g^q - g, a^q - a, b^q - b\} \tag{8}$$

after finite reductions over GB computation, we will have $GB(J+J_0) = \{1\}$, thus verifying that there exists no solutions over closure as well. Hence the two different implementations of circuit are same as there are no assignments even over closure which prove $f! = g$.

IV. CONCLUSION

This report discusses the behavior of weak $nullstellensatz$ by formulating the relations between $ideals$ and varieties. We see that while the behavior is a straight implementation for algebraically closed fields, it is still a loose bound while working on finite fields. We analyzed how formulations over algebraically closed fields using vanishing polynomials helps us determine the behavior of variety over it's finite field easily and tightens the bound. We modelled an equivalence check problem using CNF-SAT clauses and SAT solver, and also showed how to apply weak $nullstellensatz$ to verify the same.