Nullstellensatz and Boolean Satisfiability

Application of Gröbner Bases for SAT

Priyank Kalla

Professor
Electrical and Computer Engineering, University of Utah
kalla@ece.utah.edu
http://www.ece.utah.edu/~kalla

Slides updated: Nov 4, 2019

Agenda

- Application of Gröbner Bases to Equivalence Checking and SAT
  - Based on Hilbert's Weak Nullstellensatz result
- Interesting application of algebraic geometry over finite fields and Boolean rings $\mathbb{F}_2 = \mathbb{Z}_2$
- Main References: [1] [2]

- The Weak Nullstellensatz reasons about the presence or absence of solutions to an ideal – over algebraically closed fields!

Theorem (Weak NullStellensatz)

Let $\overline{\mathbb{F}}$ be an algebraically closed field. Given ideal $J \subseteq \overline{\mathbb{F}}[x_1, \dots, x_n]$, $V_{\overline{\mathbb{F}}}(J) = \emptyset \iff J = \overline{\mathbb{F}}[x_1, \dots, x_n]$.

Theorem

Based on the above notation, $J = \overline{\mathbb{F}}[x_1, \dots, x_n] \iff 1 \in J$.

Theorem

Let G be a reduced Gröbner basis of J. Then $1 \in J \iff G = \{1\}$. Therefore, $V_{\overline{\mathbb{F}}}(J) = \emptyset \iff 1 \in J \iff G = \{1\}$.

Weak Nullstellensatz when $\mathbb{F}$ is not Algebraically Closed

Theorem (Weak Nullstellensatz)

Let $\mathbb{F}$ be a field and $\overline{\mathbb{F}}$ be its algebraic closure. Given ideal $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$, $V_{\overline{\mathbb{F}}}(J) = \emptyset \iff 1 \in J \iff$ reducedGB$(J) = \{1\}$.

There is no solution over the closure $\overline{\mathbb{F}}$ iff $1 \in J$!

No solution over the closure $\overline{\mathbb{F}}$ implies no solution over $\mathbb{F}$ itself.

SAT/UNSAT Checking

Compute reduced $G = GB(f_1, \ldots, f_s) = GB(J)$ and see if $G = \{1\}$.

Weak Nullstellensatz when $\mathbb{F}$ is not Algebraically Closed

Theorem (Weak Nullstellensatz)

Let $\mathbb{F}$ be a field and $\overline{\mathbb{F}}$ be its algebraic closure. Given ideal $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$, $V_{\overline{\mathbb{F}}}(J) = \emptyset \iff 1 \in J \iff$ $reducedGB(J) = \{1\}$.

There is no solution over the closure $\overline{\mathbb{F}}$ iff $1 \in J$!

No solution over the closure $\overline{\mathbb{F}}$ implies no solution over $\mathbb{F}$ itself.

SAT/UNSAT Checking

Compute reduced $G = GB(f_1, \ldots, f_s) = GB(J)$ and see if $G = \{1\}$.

But, what if $G \neq 1$?

Theorem (Weak Nullstellensatz)

Let $\mathbb{F}$ be a field and $\overline{\mathbb{F}}$ be its algebraic closure. Given ideal $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$, $V_{\overline{\mathbb{F}}}(J) = \emptyset \iff 1 \in J \iff reducedGB(J) = \{1\}$.

There is no solution over the closure $\overline{\mathbb{F}}$ iff $1 \in J$!

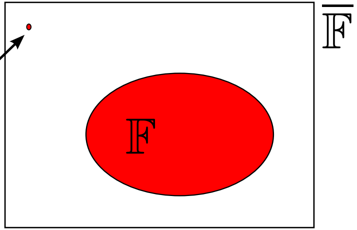
No solution over the closure $\overline{\mathbb{F}}$ implies no solution over $\mathbb{F}$ itself.

SAT/UNSAT Checking

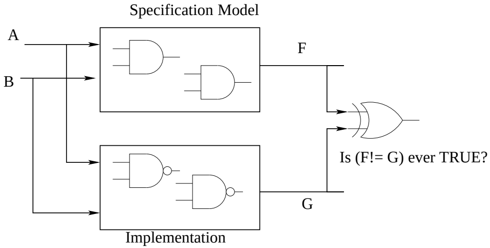
Compute reduced $G = GB(f_1, \ldots, f_s) = GB(J)$ and see if $G = \{1\}$.

But, what if $G \neq 1$? Where are the solutions? Somewhere in the closure.... [We don't know where]

Solution
can be
here if
$V_{\overline{\mathbb{F}}}(J) \neq \emptyset$



Demonstrate the difference between $GB(J)$ versus $GB(J + J_0)$ over $\mathbb{Z}_2$:



Spec: $x_1 = a \vee (\neg a \wedge b)$
Implementation: $y_1 = a \vee b$
Miter gate: $x_1 \oplus y_1$
Prove Equivalence using Nullstellensatz

From Boolean $\mathbb{B}$ to $\mathbb{Z}_2$

- Boolean AND-OR-NOT can be mapped to $+, \cdot \pmod 2$

$\mathbb{B} \rightarrow \mathbb{F}_2$:

$$\begin{aligned} \neg a &\rightarrow a + 1 \pmod 2 \\ a \vee b &\rightarrow a + b + a \cdot b \pmod 2 \\ a \wedge b &\rightarrow a \cdot b \pmod 2 \\ a \oplus b &\rightarrow a + b \pmod 2 \end{aligned} \tag{1}$$

where $a, b \in \mathbb{F}_2 = \{0, 1\}$.

Union and Intersection of Varieties

Definition (Sum/Product of Ideals [3])

If $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle$ are ideals in R, then the **sum** of I and J is defined as $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. Similarly, the **product** of I and J is $I \cdot J = \langle f_i g_j \mid 1 \leq i \leq r, 1 \leq j \leq s \rangle$.

Theorem (Union and Intersection of Varieties)

If I and J are ideals in R, then $\mathbf{V}(I + J) = \mathbf{V}(I) \bigcap \mathbf{V}(J)$ and $\mathbf{V}(I \cdot J) = \mathbf{V}(I) \bigcup \mathbf{V}(J)$.

Theorem

Finite unions and intersections of varieties are also varieties. Therefore, any finite set of points is a variety of some ideal.

Ideals and Varieties are Dual Concepts

Given a ring $R = \mathbb{F}[x_1, \ldots, x_n]$, any finite subset $V \subseteq \mathbb{F}^n$ is a variety. In other words, any finite set of points is a variety.

Finite unions and intersections of a varieties is a variety.

Let J_1, J_2 be ideals in R. Then,

- $V(J_1 + J_2) = V(J_1) \cap V(J_2)$
- $V(J_1 \cdot J_2) = V(J_1) \cup V(J_2)$
- If $J_1 \subset J_2$, then $V(J_1) \supset V(J_2)$

The Ideal of Vanishing Polynomials over $\mathbb{F}_q$

- Consider ring $R = \mathbb{F}_q[x_1, \ldots, x_n]$, $\overline{\mathbb{F}_q}$ be the closure of $\mathbb{F}_q$

The Ideal of Vanishing Polynomials over $\mathbb{F}_q$

- Consider ring $R = \mathbb{F}_q[x_1, \ldots, x_n]$, $\overline{\mathbb{F}_q}$ be the closure of $\mathbb{F}_q$
- $\forall x \in \mathbb{F}_q, x^q - x = 0$ (vanishing polynomial)

The Ideal of Vanishing Polynomials over $\mathbb{F}_q$

- Consider ring $R = \mathbb{F}_q[x_1, \ldots, x_n]$, $\overline{\mathbb{F}_q}$ be the closure of $\mathbb{F}_q$
- $\forall x \in \mathbb{F}_q, x^q - x = 0$ (vanishing polynomial)
- Denote $J_0 = \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n \rangle \subseteq R$

The Ideal of Vanishing Polynomials over $\mathbb{F}_q$

- Consider ring $R = \mathbb{F}_q[x_1, \ldots, x_n]$, $\overline{\mathbb{F}_q}$ be the closure of $\mathbb{F}_q$
- $\forall x \in \mathbb{F}_q, x^q - x = 0$ (vanishing polynomial)
- Denote $J_0 = \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n \rangle \subseteq R$
  - $J_0 =$ the ideal of all vanishing polynomials of R

The Ideal of Vanishing Polynomials over $\mathbb{F}_q$

- Consider ring $R = \mathbb{F}_q[x_1, \ldots, x_n]$, $\overline{\mathbb{F}_q}$ be the closure of $\mathbb{F}_q$
- $\forall x \in \mathbb{F}_q, x^q - x = 0$ (vanishing polynomial)
- Denote $J_0 = \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n \rangle \subseteq R$
  - $J_0 =$ the ideal of all vanishing polynomials of R
- What is $V(J_0)$?

The Ideal of Vanishing Polynomials over $\mathbb{F}_q$

- Consider ring $R = \mathbb{F}_q[x_1, \ldots, x_n]$, $\overline{\mathbb{F}_q}$ be the closure of $\mathbb{F}_q$
- $\forall x \in \mathbb{F}_q, x^q - x = 0$ (vanishing polynomial)
- Denote $J_0 = \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n \rangle \subseteq R$
  - $J_0 =$ the ideal of all vanishing polynomials of R
- What is $V(J_0)$?
  - What is $V_{\overline{\mathbb{F}_q}}(J_0)$? What is $V_{\mathbb{F}_q}(J_0)$?

The Ideal of Vanishing Polynomials over $\mathbb{F}_q$

- Consider ring $R = \mathbb{F}_q[x_1, \ldots, x_n]$, $\overline{\mathbb{F}_q}$ be the closure of $\mathbb{F}_q$
- $\forall x \in \mathbb{F}_q, x^q - x = 0$ (vanishing polynomial)
- Denote $J_0 = \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n \rangle \subseteq R$
  - $J_0 =$ the ideal of all vanishing polynomials of R
- What is $V(J_0)$?
  - What is $V_{\overline{\mathbb{F}_q}}(J_0)$? What is $V_{\mathbb{F}_q}(J_0)$?
  - $V_{\overline{\mathbb{F}_q}}(J_0) = V_{\mathbb{F}_q}(J_0) = \mathbb{F}_q^n$

The Ideal of Vanishing Polynomials over $\mathbb{F}_q$

- Consider ring $R = \mathbb{F}_q[x_1, \ldots, x_n]$, $\overline{\mathbb{F}_q}$ be the closure of $\mathbb{F}_q$
- $\forall x \in \mathbb{F}_q, x^q - x = 0$ (vanishing polynomial)
- Denote $J_0 = \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n \rangle \subseteq R$
  - $J_0 =$ the ideal of all vanishing polynomials of R
- What is $V(J_0)$?
  - What is $V_{\overline{\mathbb{F}_q}}(J_0)$? What is $V_{\mathbb{F}_q}(J_0)$?
  - $V_{\overline{\mathbb{F}_q}}(J_0) = V_{\mathbb{F}_q}(J_0) = \mathbb{F}_q^n$
- For arbitrary ideal J, think of $V(J) \cap \mathbb{F}_q^n$

The Ideal of Vanishing Polynomials over $\mathbb{F}_q$

- Consider ring $R = \mathbb{F}_q[x_1, \dots, x_n]$, $\overline{\mathbb{F}_q}$ be the closure of $\mathbb{F}_q$
- $\forall x \in \mathbb{F}_q, x^q - x = 0$ (vanishing polynomial)
- Denote $J_0 = \langle x_1^q - x_1, x_2^q - x_2, \dots, x_n^q - x_n \rangle \subseteq R$
  - $J_0 =$ the ideal of all vanishing polynomials of R
- What is $V(J_0)$?
  - What is $V_{\overline{\mathbb{F}_q}}(J_0)$? What is $V_{\mathbb{F}_q}(J_0)$?
  - $V_{\overline{\mathbb{F}_q}}(J_0) = V_{\mathbb{F}_q}(J_0) = \mathbb{F}_q^n$
- For arbitrary ideal J, think of $V(J) \cap \mathbb{F}_q^n$
- Also see Fig. One.1 in my Galois fields book chapter, to understand $V(x^4 - x)$ versus $V(x^{16} - x)$ [explained in class]

The Weak Nullstellensatz over Finite Fields

Theorem

Let $\mathbb{F}_q$ *be a finite field,* $\overline{\mathbb{F}_q}$ *be its algebraic closure, and ring* $R = \mathbb{F}_q[x_1, \dots, x_n]$. *Let* $J = \langle f_1, \dots, f_s \rangle \subset R$, *and let* $J_0 = \langle x_1^q - x_1, x_2^q - x_2, \dots, x_n^q - x_n \rangle$. *Then* $V_{\mathbb{F}_q}(J) = \emptyset$

The Weak Nullstellensatz over Finite Fields

Theorem

Let $\mathbb{F}_q$ be a finite field, $\overline{\mathbb{F}_q}$ be its algebraic closure, and ring $R = \mathbb{F}_q[x_1, \ldots, x_n]$. Let $J = \langle f_1, \ldots, f_s \rangle \subset R$, and let $J_0 = \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n \rangle$. Then $V_{\mathbb{F}_q}(J) = \emptyset$

$$\iff$$

The Weak Nullstellensatz over Finite Fields

Theorem

Let $\mathbb{F}_q$ *be a finite field,* $\overline{\mathbb{F}_q}$ *be its algebraic closure, and ring* $R = \mathbb{F}_q[x_1, \ldots, x_n]$*. Let* $J = \langle f_1, \ldots, f_s \rangle \subset R$*, and let* $J_0 = \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n \rangle$*. Then* $V_{\mathbb{F}_q}(J) = \emptyset$

$$\iff$$

$$1 \in$$

The Weak Nullstellensatz over Finite Fields

Theorem

Let $\mathbb{F}_q$ be a finite field, $\overline{\mathbb{F}_q}$ be its algebraic closure, and ring $R = \mathbb{F}_q[x_1, \ldots, x_n]$. Let $J = \langle f_1, \ldots, f_s \rangle \subset R$, and let $J_0 = \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n \rangle$. Then $V_{\mathbb{F}_q}(J) = \emptyset$

$$\iff$$

$$1 \in J + J_0 \iff reducedGB(J + J_0) = \{1\}$$

Proof

$$
\begin{aligned}
V_{\mathbb{F}_q}(J) &= V_{\overline{\mathbb{F}_q}}(J) \cap \mathbb{F}_q^n \\
&= V_{\overline{\mathbb{F}_q}}(J) \cap V_{\mathbb{F}_q}(J_0) \\
&= V_{\overline{\mathbb{F}_q}}(J) \cap V_{\overline{\mathbb{F}_q}}(J_0) \\
&= V_{\overline{\mathbb{F}_q}}(J + J_0)
\end{aligned}
$$

$$
V_{\mathbb{F}_q}(J) = \emptyset \iff V_{\overline{\mathbb{F}_q}}(J + J_0) = \emptyset
$$

$$
\iff 1 \in J + J_0 \iff \mathit{reducedGB}(J + J_0) = \{1\}
$$

Ideal J:

$$x_1 = a \vee (\neg a \wedge b) \quad \mapsto \quad x_1 + a + b \cdot (a+1) + a \cdot b \cdot (a+1) \pmod 2$$
$$y_1 = a \vee b \quad \mapsto \quad y_1 + a + b + a \cdot b \pmod 2$$
$$x_1 \neq y_1 \quad \mapsto \quad x_1 + y_1 + 1 \pmod 2$$

Compute $G = GB(J)$ over $\mathbb{Z}_2$ w.r.t. LEX $x_1 > y_1 > a > b$:

$$a^2 \cdot b + a \cdot b + 1$$
$$y_1 + a \cdot b + a + b$$
$$x_1 + a \cdot b + a + b + 1$$

$G \neq 1$, but $V(G) = \emptyset$ over $\mathbb{Z}_2$! Which means that there are solutions over the closure, so the bug = a don't care condition.

Let us take verification of GF multipliers as an example:

- Given specification polynomial: $f : Z = A \cdot B \pmod{P(x)}$ over $\mathbb{F}_{2^k}$, for given k, and given $P(x)$, s.t. $P(\alpha) = 0$
- Given circuit implementation C
  - Primary inputs: $A = \{a_0, \ldots, a_{k-1}\}, B = \{b_0, \ldots, b_{k-1}\}$
  - Primary Output $Z = \{z_0, \ldots, z_{k-1}\}$
  - $A = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{k-1}\alpha^{k-1}$
  - $B = b_0 + b_1\alpha + \cdots + b_{k-1}\alpha^{k-1}, \; Z = z_0 + z_1\alpha + \cdots + z_{k-1}\alpha^{k-1}$
- Does the circuit C correctly compute specification f?

Mathematically:

- Construct a miter between the spec f and implementation C
- Model the circuit (gates) as polynomials $\{f_1, \ldots, f_s\} \in \mathbb{F}_{2^k}[x_1, \ldots, x_d]$
- Apply Weak Nullstellensatz

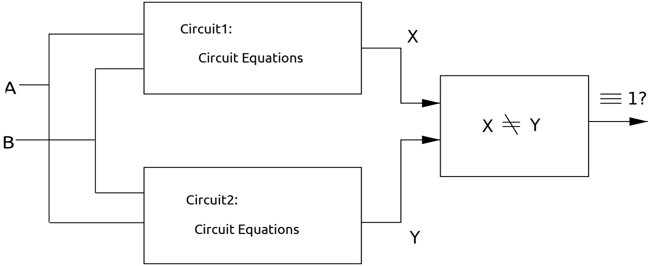


Figure: The equivalence checking setup: miter.

Spec can be a polynomial f, or a circuit implementation C
Model the miter gate as: $t(X - Y) = 1$, where t is a free variable

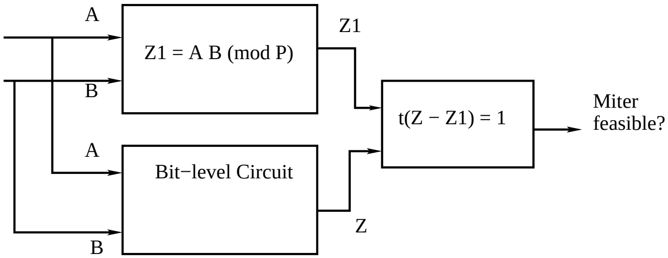


Figure: The equivalence checking setup: miter.

- When $Z = Z_1$, $t(Z - Z_1) = 1$ has no solution: infeasible miter
- When $Z \neq Z_1$: let $t^{-1} = (Z - Z_1)$. Then $t \cdot (t^{-1}) = 1$ always has a solution!
- Apply Nullstellensatz over $\mathbb{F}_{2^k}$

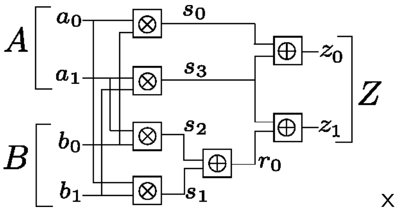


Figure: A 2-bit Multiplier

- Write $A = a_0 + a_1\alpha$ as a polynomial $f_A : A + a_0 + a_1\alpha$
- Polynomials modeling the entire circuit: ideal $J = \langle f_1, \ldots, f_{10} \rangle$

$f_1 : z_0 + z_1\alpha + Z$; $f_2 : b_0 + b_1\alpha + B$; $f_3 : a_0 + a_1\alpha + A$; $f_4 : s_0 + a_0 \cdot b_0$; $f_5 : s_1 + a_0 \cdot b_1$; $f_6 : s_2 + a_1 \cdot b_0$; $f_7 : s_3 + a_1 \cdot b_1$; $f_8 : r_0 + s_1 + s_2$; $f_9 : z_0 + s_0 + s_3$; $f_{10} : z_1 + r_0 + s_3$

Continue with multiplier verification

- So far, ideal $J = \langle f_1, \ldots, f_{10} \rangle$ models the implementation
- Let polynomial $f : Z_1 - A \cdot B$ denote the spec
- Miter polynomial $f_m : t \cdot (Z - Z_1) - 1$
- Update the ideal representation of the miter: $J = J + \langle f, f_m \rangle$
- Finally: ideal $J = \langle f_1, \ldots, f_{10},\ f,\ f_m \rangle$ represents the miter circuit
- $J \subseteq \mathbb{F}_{2^k}[A, B, Z, Z_1, a_0, a_1, b_0, b_1, r_0, s_0, \ldots, s_3, t]$
- Verification problem: is the variety $V_{\mathbb{F}_4}(J) = \emptyset$?
- How will we solve this problem?

Theorem (Weak Nullstellensatz over $\mathbb{F}_{2^k}$)

Let ideal $J = \langle f_1, \ldots, f_s \rangle \subset \mathbb{F}_{2^k}[x_1, \ldots, x_n]$ be an ideal. Let $J_0 = \langle x_1^{2^k} - x_1, \ldots, x_n^{2^k} - x_n \rangle$ be the ideal of all vanishing polynomials. Then:

$$V_{\mathbb{F}_{2^k}}(J) = \emptyset \iff V_{\overline{\mathbb{F}_{2^k}}}(J + J_0) = \emptyset \iff reducedGB(J + J_0) = \{1\}$$

Proof:

$$\begin{aligned} V_{\mathbb{F}_{2^k}}(J) &= V_{\overline{\mathbb{F}_{2^k}}}(J) \cap \mathbb{F}_{2^k} \\ &= V_{\overline{\mathbb{F}_{2^k}}}(J) \cap V_{\mathbb{F}_{2^k}}(J_0) = V_{\overline{\mathbb{F}_{2^k}}}(J) \cap V_{\overline{\mathbb{F}_{2^k}}}(J_0) \\ &= V_{\overline{\mathbb{F}_{2^k}}}(J + J_0) \end{aligned}$$

Remember: $V_{\mathbb{F}_q}(J_0) = V_{\overline{\mathbb{F}_q}}(J_0)$. The variety of J_0 does not change over the field or the closure!

- Note: Word-level polynomials $f_A : A + a_0 + a_1\alpha \in \mathbb{F}_{2^k}$
- Gate level polynomials $f_4 : s_0 + a_0 \cdot b_0 \in \mathbb{F}_2$
- Since $\mathbb{F}_2 \subset \mathbb{F}_{2^k}$, we can treat ALL polynomials of the miter, collectively, over the larger field $\mathbb{F}_{2^k}$, so $J \subseteq \mathbb{F}_{2^k}[A, B, Z, Z_1, a_0, a_1, \ldots, z_0, z_1]$
- Consider word-level vanishing polynomials: $A^{2^2} - A$
- What about bit-level vanishing polynomials: $a_0^2 - a_0$
- So, $J_0 = \langle W^{2^k} - W, B^2 - B \rangle$, where W are all the word-level variables, and B are all the bit-level variables
- Now compute $G = GB(J + J_0)$. If $G = \{1\}$, the circuit is correct. Otherwise there is definitely a BUG within the field $\mathbb{F}_{2^k}$

Recall the CNF-SAT problem

- Given a CNF formula $f(x_1, \ldots, x_n) = C_1 \wedge C_2 \wedge \cdots \wedge C_s$
  - Each C_i is a clause, i.e. a disjunction of literals
- Find an assignment to variables $x_1, \ldots, x_n$, s.t. $f = true$
- We can formulate this problem over the (Boolean) ring $\mathbb{Z}_2[x_1, \ldots, x_n]$
- Model clauses as polynomials $f_1, \ldots, f_s \in \mathbb{Z}_2[x_1, \ldots, x_n]$
- Apply Gröbner basis concepts to reason about SAT/UNSAT (think varieties!)

Be careful about problem formulation

In the SAT world, formula SAT means:

$$\begin{aligned} C_1 &= 1 \\ C_2 &= 1 \\ &\vdots \\ C_s &= 1 \end{aligned}$$

In the polynomial world, solving means:

$$\begin{aligned} f_1 &= 0 \\ f_2 &= 0 \\ &\vdots \\ f_s &= 0 \end{aligned}$$

Be careful about problem formulation

In the SAT world, formula SAT means:

$$\begin{aligned} C_1 &= 1 \\ C_2 &= 1 \\ &\vdots \\ C_s &= 1 \end{aligned}$$

In the polynomial world, solving means:

$$\begin{aligned} f_1 &= 0 \\ f_2 &= 0 \\ &\vdots \\ f_s &= 0 \end{aligned}$$

$$(C_i = 1) \iff (\overline{C_i} = 0) \iff (C_i \oplus 1 = 0)$$

Be careful about problem formulation

In the SAT world, formula SAT means:

$$\begin{aligned} C_1 &= 1 \\ C_2 &= 1 \\ &\vdots \\ C_s &= 1 \end{aligned}$$

In the polynomial world, solving means:

$$\begin{aligned} f_1 &= 0 \\ f_2 &= 0 \\ &\vdots \\ f_s &= 0 \end{aligned}$$

$$(C_i = 1) \iff (\overline{C_i} = 0) \iff (C_i \oplus 1 = 0)$$

Translate: $(C_i \oplus 1 = 0)$ as $f_i + 1 = 0$ over $\mathbb{Z}_2$

Example

- $f(a,b) = \underbrace{(a \vee \neg b)}_{C_1} \wedge \underbrace{(\neg a \vee b)}_{C_2} \wedge \underbrace{(a \vee b)}_{C_3} \wedge \underbrace{(\neg a \vee \neg b)}_{C_3}$
- Convert each C_i from $\mathbb{B}$ to $\mathbb{Z}_2$
- Consider $C_1 : (a \vee \neg b)$
  - $C_1 : (a \vee (1 \oplus b)) = a \oplus (a \oplus b) \oplus a(1 \oplus b) = 1 \oplus b \oplus ab$
  - Here $\oplus = XOR = + \pmod 2$
  - Over $\mathbb{Z}_2$, $+ \pmod 2$ is implicit, so we write: $C_1 : 1 + b + ab$
- Similarly: $C_2 : 1 + a + ab$; $C_3 : a + b + ab$; $C_4 : 1 + ab$

However: this still corresponds to $C_i = 1$, whereas we need $C_i + 1 = 0$ over $\mathbb{Z}_2$

Example

In the SAT world:

$$\begin{aligned} C_1: &\quad (a \vee \neg b) &= 1 \\ C_2: &\quad (\neg a \vee b) &= 1 \\ C_3: &\quad (a \vee b) &= 1 \\ C_4 &\quad (\neg a \vee \neg b) &= 1 \end{aligned}$$

In the polynomial world

$$\begin{aligned} f_1: &\quad b + ab &= 0 \\ f_2: &\quad a + ab &= 0 \\ f_3: &\quad a + b + ab + 1 &= 0 \\ f_4: &\quad ab &= 0 \end{aligned}$$

- Now $J = \langle f_1, \ldots, f_4 \rangle$ generates an ideal in $\mathbb{Z}_2[a, b]$
- We need to analyze $V_{\mathbb{Z}_2}(J)$

Apply Nullstellensatz to Boolean rings $\mathbb{Z}_2[x_1, \dots, x_n]$

Boolean rings: Rings with indempotence $a \wedge a = a$ or $a^2 = a$

- Consider the ideal of vanishing polynomials
  - In $\mathbb{Z}_p$, $x^p = x \pmod{p}$, or $x^p - x = 0$
  - In $\mathbb{Z}_2 : x^2 - x$ vanishes on $\{0, 1\}$: vanishing polynomial
- Let $J_0 = \langle x_1^2 - x_1, x_2^2 - x_2, \dots, x_n^2 - x_n \rangle$ denote the ideal of all vanishing polynomials
- $V_{\mathbb{Z}_2}(J_0) = (\mathbb{Z}_2)^n$ (the n-dimensional space over $\mathbb{Z}_2$)
- Variety of J_0 doesn't change over the closure: $V_{\overline{\mathbb{Z}_2}}(J) = (\mathbb{Z}_2)^n$
- These vanishing polynomial restrict the solutions to only over $\mathbb{Z}_2$
- So compute $G = GB(J + J_0) = GB(f_1, \dots, f_s, x_1^2 - x_1, x_2^2 - x_2, \dots, x_n^2 - x_n)$
- If $G \neq \{1\}$ then definitely there is a SAT solution within $\mathbb{Z}_2$

Weak Nullstellensatz over $\mathbb{F}_2 = \mathbb{Z}_2$

Theorem (Weak Nullstellensatz over Boolean Rings)

Let ideal $J = \langle f_1, \ldots, f_s \rangle \subset \mathbb{Z}_2[x_1, \ldots, x_n]$ and let $J_0 = \langle x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle$. Then $V_{\mathbb{Z}_2}(J) = \emptyset \iff$ the reduced $GB(J + J_0) = GB(f_1, \ldots, f_s,\ x_1^2 - x_1, \ldots, x_n^2 - x_n) = \{1\}$.

If $GB(J + J_0) = \{1\}$ then the problem is UNSAT.

If $GB(J + J_0) \neq \{1\}$ then there is definitely a solution in $\mathbb{Z}_2$.

Notation for Sum of Ideals: If $J_1 = \langle f_1, \ldots, f_s \rangle$ and $J_2 = \langle g_1, \ldots, g_t \rangle$, then $J_1 + J_2 = \langle f_1, \ldots, f_s,\ g_1, \ldots, g_t \rangle$

If $GB \neq \{1\}$, is $V(J)$ finite or infinite?

Theorem

Let $\mathbb{F}$ be any field and $\overline{\mathbb{F}}$ be its closure, and $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be an ideal. Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis of J. Then:

$$V_{\overline{\mathbb{F}}}(J) = finite \iff$$

$$\forall x_i \in \{x_1, \ldots, x_n\}, \ \exists g_j \in G, s.t. lm(g_j) = x_i^l, \text{for some } \ l \in \mathbb{N}$$

Example of a finite variety

Example

$R = \mathbb{Q}[x, y]$, $f_1 = \underbrace{(x-1)^2 + y^2 - 1}_{circle}$; $f_2 = \underbrace{4(x-1)^2 + y^2 + xy - 2}_{ellipse}$.

$G = GB(f_1, f_2)$ with lex $x > y$

$G = \{g_1 = 5y^4 - 3y^3 - 6y^2 + 2y + 2, \quad g_2 = x - 5y^3 + 3y^2 + 3y - 2\}$

Variety is finite.

A Gröbner basis example [From Cox/Little/O'Shea]

Solve the system of equations:

$$f_1 : x^2 - y - z - 1 = 0$$
$$f_2 : x - y^2 - z - 1 = 0$$
$$f_3 : x - y - z^2 - 1 = 0$$

Gröbner basis with lex term order $x > y > z$

$$\begin{aligned} g_1 :& x - y - z^2 - 1 &= 0 \\ g_2 :& y^2 - y - z^2 - z &= 0 \\ g_3 :& 2yz^2 - z^4 - z^2 &= 0 \\ g_4 :& z^6 - 4z^4 - 4z^3 - z^2 &= 0 \end{aligned}$$

- Is $V(\langle G \rangle) = \emptyset$? No, because $G \neq \{1\}$
- G tells me that $V(\langle G \rangle)$ is finite!
- G is *triangular*: solve g_4 for z, then g_2, g_3 for y, and then g_1 for x

Gröbner basis of Zero-Dimensional Ideal

Definition (Zero-Dimensional Ideals)

An ideal J is called zero dimensional when its variety $V(J)$ is a finite set.

- $V_{\mathbb{F}_q}(J)$ is a finite set
- $V_{\overline{\mathbb{F}_q}}(J)$ need not be a finite set, as $\overline{\mathbb{F}_q}$ is an infinite set
- So, ideal J may or maynot be zero dimensional
- $V_{\mathbb{F}_q}(J) = V_{\overline{\mathbb{F}_q}}(J + J_0) = V_{\mathbb{F}_q}(J + J_0)$ is always a finite set, as solutions are restricted to $\mathbb{F}_q$
- Ideal $J + J_0$ is zero dimensional!

The Gröbner basis of $J + J_0$ has a very special structure!

The GB of $J + J_0$ in $\mathbb{F}_q[x_1, \ldots, x_n]$

Theorem (*Gröbner bases in finite fields (application of Theorem 2.2.7 from [4] over $\mathbb{F}_q$)*)

For $G = GB(J + J_0) = \{g_1, \ldots, g_t\}$, the following statements are equivalent:

1. *The variety $V_{\mathbb{F}_q}(J)$ is finite.*
2. *For each $i = 1, \ldots, n$, there exists some $j \in \{1, \ldots, t\}$ such that $lm(g_j) = x_i^l$ for some $l \in \mathbb{N}$.*
3. *The quotient ring $\frac{\mathbb{F}_q[x_1 \ldots, x_n]}{\langle G \rangle}$ forms a finite dimensional vector space.*

Count the number of solutions

Example

$G = GB(J) = \{x^3y^2 - y;\ x^4 - y^2;\ xy^3 - x^2; y^4 - xy\}$. Consider only the leading monomials in G. $LT(G) = \{x^3y^2, x^4, xy^3, y^4\}$.
List all monomials m s.t. m is not divisible by any monomial in $LT(G)$:

Standard Monomials $SM = \{1, x, x^2, x^3, y, y^2, y^3, xy, xy^2, x^2y, x^2y^2, x^3y\}$

Cardinality $|SM|$ = an upper bound on the number of solutions (=12 in the above example)

In general, $|V(J)|$ is bounded by $|SM(J)|$, but over finite fields, the following result holds, where the upper bound becomes an equality!

Counting the number of solutions in $\mathbb{F}_q$ for $J + J_0$

For a GB G, let $LM(G)$ denote the set of leading monomials of all elements of G: $LM(G) = \{lm(g_1), \ldots, lm(g_t)\}$.

Definition (*Standard Monomials*)

Let $\mathbf{X}^{\mathbf{e}} = x_1^{e_1} \cdots x_n^{e_n}$ denote a monomial. The set of standard monomials of G is defined as $SM(G) = \{\mathbf{X}^{\mathbf{e}} : \mathbf{X}^{\mathbf{e}} \notin \langle LM(G) \rangle\}$.

Theorem (*Counting the number of solutions (Theorem 3.7 in [5])*)

Let $G = GB(J + J_0)$, and $|SM(G)| = m$, then the ideal J vanishes on m distinct points in $\mathbb{F}_q^n$. In other words, $|V_{\mathbb{F}_q}(J)| = |SM(G)|$.

Verification over Composite Fields

- Given arbitrary circuits C_1, C_2: m-bit inputs, n-bit outputs
- Suppose m does NOT divide n: $m \nmid n$
- For example, if $m = 3, n = 2$, then how to construct a miter over a single field $\mathbb{F}_q$?
- Solve the problem over the smallest single field containing both $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}$.
- Let $k = LCM(m, n)$, then solve the problem over $\mathbb{F}_{2^k}$.
  - Now $m|k$ and $n|k$
- What about primitive polynomials and primitive elements?

Composite Field Miter

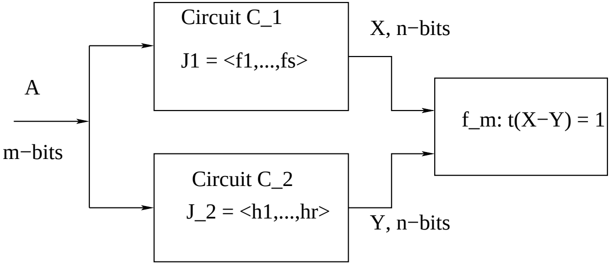


Figure: The equivalence checking setup: miter.

- $A \in \mathbb{F}_{2^m}, X, Y \in \mathbb{F}_{2^n}$
- Nets of the circuits: Boolean variables $x_1, \ldots, x_n \in \mathbb{F}_2$
- $t \in$ which field?

Composite Fields

- Pick $P_m(X)$ as a primitive polynomial of degree m, $P_m(\beta) = 0$
- Pick $P_n(X)$ as another primitive polynomial of degree n, $P_n(\gamma) = 0$
- Compute $k = LCM(m, n)$, pick $P_k(X)$ as another primitive polynomial of degree k, $P_k(\alpha) = 0$

$$\alpha^{2^k-1} = \beta^{2^m-1}$$

$$\beta = \alpha^{\frac{2^k-1}{2^m-1}} \tag{2}$$

$$\alpha^{2^k-1} = \gamma^{2^n-1}$$

$$\gamma = \alpha^{\frac{2^k-1}{2^n-1}} \tag{3}$$

Composite Fields

- Example: $m = 3, n = 2, k = LCM(3, 2) = 6$
- From Eqns. (2)-(3) on previous slides: $\beta = \alpha^9, \gamma = \alpha^{21}$
- $A \in \mathbb{F}_{2^3} : A = a_0 + a_1\beta + a_2\beta^2 = a_0 + a_1\alpha^9 + a_2\alpha^{18}$
- $X = x_0 + x_1\gamma = x_0 + x_1\alpha^{21}$, same for Y
- All the bit-level variables in $\mathbb{F}_2 \subset \mathbb{F}_{2^k}$
- Ideals J_1, J_2 = polynomials for the gates in the design
- Ideal of vanishing polynomials:
  $J_0 = \langle A^{2^m} - A, X^{2^n} - X, Y^{2^n} - Y, t^{2^n} - t, x_i^2 - x_i : x_i \in \text{bit-level}\rangle$
- $J = J_1 + J_2 + \langle f_m \rangle = \langle f_1, \dots, f_s, h_1, \dots, h_r, f_m \rangle$
- Compute $G = GB(J + J_0) = \{1\}$ in $\mathbb{F}_{2^k}[A, X, Y, t, x_i]$?

[1] M. Clegg, J. Edmonds, and R. Impagliazzo, “Using the Gröbner Basis Algorithm to Find Proofs of Unsatisfiability,” in *ACM Symposium on Theory of Computing*, 1996, pp. 174–183.

[2] C. Condrat and P. Kalla, “A Gröbner Basis Approach to CNF formulae Preprocessing,” in *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, 2007, pp. 618–631.

[3] D. Cox, J. Little, and D. O’Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 2007.

[4] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*. American Mathematical Society, 1994.

[5] S. Gao, “Counting Zeros over Finite Fields with Gröbner Bases,” Master’s thesis, Carnegie Mellon University, 2009.