Nullstellensatz and Boolean Satisfiability

Application of Gröbner Bases for SAT

Priyank Kalla

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

October 8, 20, 2014

Agenda

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

Recall the SAT problem

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

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

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

Weak Nullstellensatz

- 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 $J \subset \overline{\mathbb{F}}[x_1, \dots, x_n]$, $V_{\overline{\mathbb{F}}}(J) = \emptyset \iff J = \overline{\mathbb{F}}[x_1, \dots, x_n]$.

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 $J \subset \mathbb{F}[x_1, \ldots, x_n]$, $V_{\overline{\mathbb{F}}}(J) = \emptyset \iff 1 \in J \iff reducedGB(J) = \{1\}$.

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 $J \subset \mathbb{F}[x_1, \ldots, x_n]$, $V_{\overline{\mathbb{F}}}(J) = \emptyset \iff 1 \in J \iff reducedGB(J) = \{1\}$.

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 $G \neq 1$?

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 $J \subset \mathbb{F}[x_1, \dots, x_n]$, $V_{\overline{\mathbb{F}}}(J) = \emptyset \iff 1 \in J \iff reducedGB(J) = \{1\}$.

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

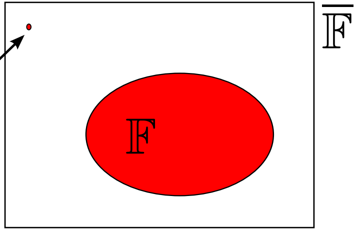
No solution over the closure $\overline{\mathbb{F}}$ implies no solution over $\mathbb{F}$ itself.

SAT/UNSAT Checking

Compute reduced $G = GB(f_1, \dots, f_s) = GB(J)$ 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 $V_{\overline{\mathbb{F}}}(J) \neq \emptyset$



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 $GB(J + J_0) = GB(f_1, \ldots, f_s,\ x_1^2 - x_1, \ldots, x_n^2 - x_n) = \{1\}$.

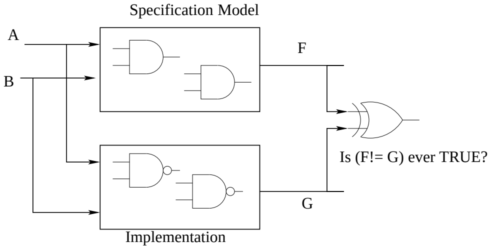
If $GB(J + J_0) = \{1\}$ then the problem is UNSAT.

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 $J_1 + J_2 = \langle f_1, \ldots, f_s,\ g_1, \ldots, g_t \rangle$

Weak Nullstellensatz to Equivalence Checking

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

Ideal J:

$$\begin{aligned} x_1 = a \vee (\neg a \wedge b) &\mapsto x_1 + a + b \cdot (a+1) + a \cdot b \cdot (a+1) \pmod 2 \\ y_1 = a \vee b &\mapsto y_1 + a + b + a \cdot b \pmod 2 \\ x_1 \neq y_1 &\mapsto x_1 + y_1 + 1 \pmod 2 \end{aligned}$$

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

$$\begin{aligned} a^2 \cdot b + a \cdot b + 1 \\ y_1 + a \cdot b + a + b \\ x_1 + a \cdot b + a + b + 1 \end{aligned}$$

$G \neq 1$, 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.
Correct formulation: Compute $G = GB(J + J_0) = \{1\}$; where $J_0 = \{x_1^2 - x_1, y_1^2 - y_1, a^2 - a, b^2 - b\}$.

Weak Nullstellensatz over Boolean: Conclusion

Theorem (Weak Nullstellensatz over Boolean Rings)

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

[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.