Computer Algebra for Computer Engineers

*Hilbert’s Nullstellensatz + $I(V(I))$*

Priyank Kalla

*Department of Electrical and Computer Engineering*

*University of Utah, Salt Lake City*
Ideal-Variety Correspondence

- When $I_1 = I_2$ we have $V(I_1) = V(I_2)$.
- What happens to varieties when $I_1 \neq I_2$?
- It depends on which fields we are working on, and algebraic closure plays an important role.
- Let's take some examples....
- In $R[x]$, $I_1 = \langle 1 \rangle$, $I_2 = \langle x^2 + 1 \rangle$, $I_3 = \langle 1 + x^2 + x^4 \rangle$
- Also in $k[x]$, $I_1 = \langle x \rangle$; $I_2 = \langle x^2 \rangle$, $V(I_1) = V(I_2) = \{0\}$
- What about $V_R(x^2 + y^2 + 1)$ and $V_C(x^2 + y^2 + 1)$?
- What about $V(x^2 + y^2) \cap V(x, y)$ over $R, C$?
Weak Nullstellensatz

- Does the problem of having different ideals represent the empty variety go away if $k$ is algebraically closed?

- Yes, it does in $k[x]$ and also in $k[x_1, \ldots, x_n]$

- In any polynomial ring, algebraic closure is enough to guarantee that the only ideal which represents the empty variety is the entire polynomial ring itself!

(Weak Nullstellensatz) Let $k$ be an algebraically closed field and let $I \subset k[x_1, \ldots, x_n]$ be an ideal such that $V(I) = \emptyset$. Then $I = k[x_1, \ldots, x_n]$. 
Weak Nullstellensatz and G.B.

- Given polynomial system: $f_1 = f_2 = \cdots = f_s = 0$
- Do they have a common zero?
- No common zero ($V(f_1, \ldots, f_s) = \emptyset$) $\iff$ $1 \in \text{G.B.}$
- But this is true only over algebraically closed fields!

(Weak Nullstellensatz) Let $k$ be an algebraically closed field and let $I \subset k[x_1, \ldots, x_n]$ be an ideal such that $V(I) = \emptyset$. Then $I = k[x_1, \ldots, x_n]$. 
What if $k$ isn’t closed?

- Let $\overline{k}$ be the algebraic closure of $k$.

- Every field $k$ is contained in $\overline{k}$, which is algebraically closed. Every element of $\overline{k}$ is the root of a non-zero $f \in k[x]$.

- Let $I = \langle f_1, \ldots, f_s \rangle \in k[x_1, \ldots, x_n]$. Denote variety over extension field

$$V_{\overline{k}}(I) = \{(a_1, \ldots, a_n) \in \overline{k}^n \mid f_i(a_1, \ldots, a_n) = 0\}.$$

- Note: Ideal in $k$ and variety in $\overline{k}$.

(Another “weak” nullsatz) Let $I$ be an ideal in $k[x_1, \ldots, x_n]$. Then $V_{\overline{k}}(I) = \emptyset$ if and only if $I = k[x_1, \ldots, x_n]$. 
Application: Equivalence Check in $F_2$

- Given: $F, G$ as polynomials in $F_2$
- Prove (or disprove) that $F \equiv G$ over $F_2$
- If $F \equiv G$, then $F \neq G$ has no solution
- Formulate as Groebner bases/Nullstellensatz
- $F \neq G$ modeled as $t(F - G) = 1$, where $t$ is inverse of $F - G$. 
Application: Equivalence Check in $F_2$

- But, Nullsatz works over algebraic closure of $F_2$
- Trick: Ideal = $J = \langle I, Z \rangle$, $Z = \{x_i^2 + x_i, \forall x_i\}$
- $Z$ is the set of all vanishing polynomials in $F_2$
- $\overline{V}(Z) = V(Z) = F_2^n$. So, we want $\overline{V}(J) = \overline{V}(I) \cap \overline{V}(Z) = V(J)$.
- $V(I) \cap V(Z) = V(\langle I, Z \rangle)$
Ideal-Variety Correspondence

- Given $I$, we have $V(I)$ and the G.B. theory
- Now think about a set of points in $k^n$ (given Variety)
- $I(V) = \{ f \in k[x_1, \ldots, x_n] | f(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_n) \in V \}$
- $I(V)$ is an ideal!
- How is $I$ related to $I(V(I))$? $I \subseteq I(V(I))$ in general.
Let $k$ = algebraically closed field. Let $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, such that $f \in I(V(f_1, \ldots, f_s))$, then $f^e \in \langle f_1, \ldots, f_s \rangle$ for some $e \geq 1$; and conversly.

This is the “regular” Nullstellensatz.

The only reason different ideals can give the same variety is that if $f$ vanishes on $V(I)$, then $f^e$ must be in $I$. (Of course, over ACF!)

$I_1 = \langle x^2, y^3 \rangle$, $I_2 = \langle x, y \rangle$, $I_1 \neq I_2$. $V(I_1) = V(I_2)$

$x \in I_2 = I(V(I_1))$ and $x^2 \in I_1$
Radical Ideals

- Let \( V \) be a variety. If \( f^e \in I(V) \) then \( f \in I(V) \).
- An ideal \( I \) is called a radical ideal if \( f^e \in I \), for some \( e \geq 1 \), implies \( f \in I \).
- Let \( I \) be an ideal in \( k[x_1, \ldots, x_n] \). Radical of \( I \), denoted \( \sqrt{I} \), is
\[
\sqrt{I} = \{ f \in k[x_1, \ldots, x_n] \mid \exists e \in \mathbb{N}, f^e \in I \}.
\]
- \( I(V(I)) \) is a radical ideal.
- \( \sqrt{I} \) is an ideal, and ideals and their radicals give rise to the same variety over \( \overline{k} \): \( V_{\overline{k}}(I) = V_{\overline{k}}(\sqrt{I}) \).
- \( \sqrt{I} \supset I \)
Putting it all together

**Strong Nullstellensatz:** \( I(V_k(I)) = \sqrt{I} \) for all ideals \( I \) in \( k[x_1, \ldots, x_n] \).

Given two ideals, \( I, J \), \( V_k(I) = V_k(J) \iff \sqrt{I} = \sqrt{J} \).

**Radical Membership:** Let \( k \) be a field, \( I = \langle f_1, \ldots, f_s \rangle \) be an ideal. Then \( f \in \sqrt{I} \) if and only if \( 1 \in J \), where \( J = \langle f_1, \ldots, f_s, 1 - yf \rangle \).

Radical membership application: Model Checking! (See Avrunin’s CAV paper)