Radical Ideals and their Varieties

The Strong Nullstellensatz

Priyank Kalla

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

Nov 6, 2017 - onwards

Agenda

- Study (strong/exact) relationships between ideals and varieties
  - Based on the Regular and Strong Nullstellensatz result
- These results are needed for word-level verification of circuits
- The remaining concepts that enable complete hardware verification:
  - Study Nullstellensatz over algebraically closed fields
  - Then study Nullstellensatz over Galois fields $\mathbb{F}_{2^k}$ and hardware design (I'll give you my textbook chapters)
  - Then apply Nullstellensatz specifically over $\mathbb{F}_{2^k}$ to verify digital circuits
- We should be able to study these basic concepts in the next 3-4 lectures and then apply these concepts to practical datapath circuits.

Some more concepts about Varieties

- Let $\mathbb{F}$ be a field and $\mathbf{a} \in \mathbb{F}$ be an arbitrary point

Some more concepts about Varieties

- Let $\mathbb{F}$ be a field and $\mathbf{a} \in \mathbb{F}$ be an arbitrary point
- $\mathbf{a}$ is a variety of some ideal: find J s.t. $V(J) = \{a\}$

Before we get to Strong Nullstellensatz...

Some more concepts about Varieties

- Let $\mathbb{F}$ be a field and $\mathbf{a} \in \mathbb{F}$ be an arbitrary point
- $\mathbf{a}$ is a variety of some ideal: find J s.t. $V(J) = \{a\}$
- $J = \langle x - a \rangle$

Before we get to Strong Nullstellensatz...

Some more concepts about Varieties

- Let $\mathbb{F}$ be a field and $\mathbf{a} \in \mathbb{F}$ be an arbitrary point
- $\mathbf{a}$ is a variety of some ideal: find J s.t. $V(J) = \{a\}$
- $J = \langle x - a \rangle$

Before we get to Strong Nullstellensatz...

Some more concepts about Varieties

- Let $\mathbb{F}$ be a field and $\mathbf{a} \in \mathbb{F}$ be an arbitrary point
- $\mathbf{a}$ is a variety of some ideal: find J s.t. $V(J) = \{a\}$
- $J = \langle x - a \rangle$

$V_1 \cup V_2$ and $V_1 \cap V_2$

Finite unions and intersections of varieties are also varieties. Let $V_1 = V(f_1, \ldots, f_s)$ and $V_2 = V(g_1, \ldots, g_t)$:

- $V_1 \cap V_2 = V(f_1, \ldots, f_s,\ g_1, \ldots, g_t)$
- $V_1 \cup V_2 = V(f_i \cdot g_j : 1 \leq i \leq s, 1 \leq j \leq t)$

Example: Consider the union of the (x, y)-plane and the z-axis. Then: $V(z) \cup V(x, y) = V(zx, zy)$

Consequently...

- Every finite set of points is a variety of some ideal $V(J)$
- Prove it!
- Example:
  - The Galois field $\mathbb{F}_2 = \mathbb{Z}_2$ is a finite set of points (2)
  - $\mathbb{F}_2 = V(J_0)$, where $J_0 = \langle x^2 - x \rangle$ the ideal of vanishing polynomial

Other notations:

- Let ideal $I = \langle f_1, \ldots, f_r \rangle$, $J = \langle g_1, \ldots, g_s \rangle$, then:
  - $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$, and $V(I + J) = V(I) \cap V(J)$
  - $I \cdot J = \langle f_i \cdot g_j : 1 \leq i \leq r, 1 \leq j \leq s \rangle$, and $V(I \cdot J) = V(I) \cup V(J)$

Now some fun stuff for Nullstellensatz

- If ideals $I_1 = I_2$, is $V(I_1) = V(I_2)$?

Now some fun stuff for Nullstellensatz

- If ideals $I_1 = I_2$, is $V(I_1) = V(I_2)$?
- Yes, of course!

Now some fun stuff for Nullstellensatz

- If ideals $I_1 = I_2$, is $V(I_1) = V(I_2)$?
- Yes, of course!
- If $V(I_1) = V(I_2)$, is $I_1 = I_2$?

Now some fun stuff for Nullstellensatz

- If ideals $I_1 = I_2$, is $V(I_1) = V(I_2)$?
- Yes, of course!
- If $V(I_1) = V(I_2)$, is $I_1 = I_2$?
- No! Not always. Maybe $I_1 = I_2$, but not always.

Now some fun stuff for Nullstellensatz

- If ideals $I_1 = I_2$, is $V(I_1) = V(I_2)$?
- Yes, of course!
- If $V(I_1) = V(I_2)$, is $I_1 = I_2$?
- No! Not always. Maybe $I_1 = I_2$, but not always.
- Example:

Now some fun stuff for Nullstellensatz

- If ideals $I_1 = I_2$, is $V(I_1) = V(I_2)$?
- Yes, of course!
- If $V(I_1) = V(I_2)$, is $I_1 = I_2$?
- No! Not always. Maybe $I_1 = I_2$, but not always.
- Example:
  - $I_1 = \langle x^2, y^2 \rangle, \quad I_2 = \langle x, y \rangle$

Now some fun stuff for Nullstellensatz

- If ideals $I_1 = I_2$, is $V(I_1) = V(I_2)$?
- Yes, of course!
- If $V(I_1) = V(I_2)$, is $I_1 = I_2$?
- No! Not always. Maybe $I_1 = I_2$, but not always.
- Example:
  - $I_1 = \langle x^2, y^2 \rangle, \quad I_2 = \langle x, y \rangle$
  - $V(I_1) = V(I_2) = \{(0,0)\}$, but $I_1 \neq I_2, (I_1 \subset I_2)$

Now some fun stuff for Nullstellensatz

- If ideals $I_1 = I_2$, is $V(I_1) = V(I_2)$?
- Yes, of course!
- If $V(I_1) = V(I_2)$, is $I_1 = I_2$?
- No! Not always. Maybe $I_1 = I_2$, but not always.
- Example:
  - $I_1 = \langle x^2, y^2 \rangle, \quad I_2 = \langle x, y \rangle$
  - $V(I_1) = V(I_2) = \{(0,0)\}$, but $I_1 \neq I_2, (I_1 \subset I_2)$
- Different ideals can have the same variety!

Now some fun stuff for Nullstellensatz

- If ideals $I_1 = I_2$, is $V(I_1) = V(I_2)$?
- Yes, of course!
- If $V(I_1) = V(I_2)$, is $I_1 = I_2$?
- No! Not always. Maybe $I_1 = I_2$, but not always.
- Example:
  - $I_1 = \langle x^2, y^2 \rangle, \quad I_2 = \langle x, y \rangle$
  - $V(I_1) = V(I_2) = \{(0,0)\}$, but $I_1 \neq I_2, (I_1 \subset I_2)$
- Different ideals can have the same variety!
- But I_1 and I_2 are somehow related....

- If ideals $I_1 = I_2$, is $V(I_1) = V(I_2)$?
- Yes, of course!
- If $V(I_1) = V(I_2)$, is $I_1 = I_2$?
- No! Not always. Maybe $I_1 = I_2$, but not always.
- Example:
  - $I_1 = \langle x^2, y^2 \rangle, \quad I_2 = \langle x, y \rangle$
  - $V(I_1) = V(I_2) = \{(0,0)\}$, but $I_1 \neq I_2, (I_1 \subset I_2)$
- Different ideals can have the same variety!
- But I_1 and I_2 are somehow related....
- Nullstellensatz describes these relationships exactly

$I(V(J))$: Ideal of polynomials that vanishes on the variety $V(J)$

$I(V)$

Let $J = \langle f_1, \ldots, f_s \rangle \subset \mathbb{F}[x_1, \ldots, x_n]$. Then:
$I(V(J)) = \{f \in \mathbb{F}[x_1, \ldots, x_n] : f(\mathbf{a}) = 0 \ \forall \mathbf{a} \in V(J)\}$

- $I(V(J))$ is the set of all polynomials that vanish on $V(J)$
- If f vanishes on $V(J)$, then $f \in I(V(J))$
- Can you prove that $I(V(J))$ is indeed an ideal?
- Example:
  - $J = \langle x^2, y^2 \rangle, \ f = x, f \notin J, f \in I(V(J))$
- In a general setting: given generators of $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, not easy to find generators of $I(V(J))$
- Over algebraically closed fields, $I(V(J))$ is related to J via $\sqrt{J}$ [details in the next few slides]

Some more about $I(V(J))$

- Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, then $J \subseteq I(V(J))$, but equality may not occur

Some more about $I(V(J))$

- Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, then $J \subseteq I(V(J))$, but equality may not occur
  - $J = \langle x^2, y^2 \rangle, I(V(J)) = \langle x, y \rangle$ which shows $J \subset I(V(J))$

Some more about $I(V(J))$

- Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, then $J \subseteq I(V(J))$, but equality may not occur
  - $J = \langle x^2, y^2 \rangle, I(V(J)) = \langle x, y \rangle$ which shows $J \subset I(V(J))$
  - $J = \langle x, y \rangle, I(V(J)) = J$; equality holds in this case

Some more about $I(V(J))$

- Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, then $J \subseteq I(V(J))$, but equality may not occur
  - $J = \langle x^2, y^2 \rangle, I(V(J)) = \langle x, y \rangle$ which shows $J \subset I(V(J))$
  - $J = \langle x, y \rangle, I(V(J)) = J$; equality holds in this case
  - $J = \langle x^2 + 1 \rangle, V_{\mathbb{R}}(J) = \emptyset, I(V(J)) = I(\text{empty}) = \mathbb{R}[x]$; here $J \subset I(V(J))$

Some more about $I(V(J))$

- Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, then $J \subseteq I(V(J))$, but equality may not occur
  - $J = \langle x^2, y^2 \rangle, I(V(J)) = \langle x, y \rangle$ which shows $J \subset I(V(J))$
  - $J = \langle x, y \rangle, I(V(J)) = J$; equality holds in this case
  - $J = \langle x^2 + 1 \rangle, V_{\mathbb{R}}(J) = \emptyset, I(V(J)) = I(\text{empty}) = \mathbb{R}[x]$; here $J \subset I(V(J))$
- Over Galois fields $\mathbb{F}_q$, let $J_0 = \langle x^q - x \rangle$

Some more about $I(V(J))$

- Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, then $J \subseteq I(V(J))$, but equality may not occur
  - $J = \langle x^2, y^2 \rangle, I(V(J)) = \langle x, y \rangle$ which shows $J \subset I(V(J))$
  - $J = \langle x, y \rangle, I(V(J)) = J$; equality holds in this case
  - $J = \langle x^2 + 1 \rangle, V_{\mathbb{R}}(J) = \emptyset, I(V(J)) = I(\text{empty}) = \mathbb{R}[x]$; here $J \subset I(V(J))$
- Over Galois fields $\mathbb{F}_q$, let $J_0 = \langle x^q - x \rangle$
- What is $I(V_{\mathbb{F}_q}(J_0))$? $I(V_{\overline{\mathbb{F}_q}}(J_0))$?

Some more about $I(V(J))$

- Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, then $J \subseteq I(V(J))$, but equality may not occur
  - $J = \langle x^2, y^2 \rangle, I(V(J)) = \langle x, y \rangle$ which shows $J \subset I(V(J))$
  - $J = \langle x, y \rangle, I(V(J)) = J$; equality holds in this case
  - $J = \langle x^2 + 1 \rangle, V_{\mathbb{R}}(J) = \emptyset, I(V(J)) = I(\text{empty}) = \mathbb{R}[x]$; here $J \subset I(V(J))$
- Over Galois fields $\mathbb{F}_q$, let $J_0 = \langle x^q - x \rangle$
- What is $I(V_{\mathbb{F}_q}(J_0))$? $I(V_{\overline{\mathbb{F}_q}}(J_0))$?
- $I(V(J_0)) = J_0$ itself! We will prove it shortly...

Some more about $I(V(J))$

- Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, then $J \subseteq I(V(J))$, but equality may not occur
  - $J = \langle x^2, y^2 \rangle, I(V(J)) = \langle x, y \rangle$ which shows $J \subset I(V(J))$
  - $J = \langle x, y \rangle, I(V(J)) = J$; equality holds in this case
  - $J = \langle x^2 + 1 \rangle, V_{\mathbb{R}}(J) = \emptyset, I(V(J)) = I(\text{empty}) = \mathbb{R}[x]$; here $J \subset I(V(J))$
- Over Galois fields $\mathbb{F}_q$, let $J_0 = \langle x^q - x \rangle$
- What is $I(V_{\mathbb{F}_q}(J_0))$? $I(V_{\overline{\mathbb{F}_q}}(J_0))$?
- $I(V(J_0)) = J_0$ itself! We will prove it shortly...
- Is $V(J) = V(I(V(J)))$? Yes, it is!

Some more about $I(V(J))$

- Given ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, then $J \subseteq I(V(J))$, but equality may not occur
  - $J = \langle x^2, y^2 \rangle, I(V(J)) = \langle x, y \rangle$ which shows $J \subset I(V(J))$
  - $J = \langle x, y \rangle, I(V(J)) = J$; equality holds in this case
  - $J = \langle x^2 + 1 \rangle, V_{\mathbb{R}}(J) = \emptyset, I(V(J)) = I(\text{empty}) = \mathbb{R}[x]$; here $J \subset I(V(J))$
- Over Galois fields $\mathbb{F}_q$, let $J_0 = \langle x^q - x \rangle$
- What is $I(V_{\mathbb{F}_q}(J_0))$? $I(V_{\overline{\mathbb{F}_q}}(J_0))$?
- $I(V(J_0)) = J_0$ itself! We will prove it shortly...
- Is $V(J) = V(I(V(J)))$? Yes, it is!
- Always remember that $V(J)$ is always taken over an ACF unless specified otherwise

Still some more about $I(V(J))$

- Prove that $I(V(J))$ is an ideal
- Show that:
  - $0 \in I(V(J)$ (The zero element of the ring is in I(V(J)))
  - For $f, g \in I(V(J)) \implies f + g \in I(V(J))$
  - For $f \in I(V(J)), h \in \mathbb{F}[x_1, \ldots, x_n]$, then $f \cdot h \in I(V(J))$
- The concept of $I(V(J))$ is valid over any ring (not necessarily algebraically closed)
- Finally, some more examples: $J = \langle x^2, y^2 \rangle$
- $f_1 = x + y,\; f_2 = x \cdot y;\; f_1, f_2 \notin J,\; f_1, f_2 \in I(V(J))$
- $f_3 = x(x + y^2) = x^2 + xy^2;\; f_3 \in J$ and so obviously $f_3 \in I(V(J))$

Regular Nullstellensatz

- Previous examples show that the reason why different ideals can have the same variety is that: for $a \in V(J)$, $f(a) = 0$ as well as $f^m(a) = 0$ but $(I_1 = \langle f \rangle) \neq (I_2 = \langle f^m \rangle)$

Theorem (Regular Nullstellensatz)

Let $\overline{\mathbb{F}}$ be an algebraically closed field. Let $J = \langle f_1, \ldots, f_s \rangle \subset \overline{\mathbb{F}}[x_1, \ldots, x_n]$. Let another polynomial f **vanish** *on $V_{\overline{\mathbb{F}}}(J)$, so $f \in I(V_{\overline{\mathbb{F}}}(J))$. Then, $\exists m \in \mathbb{Z}_{\geq 1}$ s.t.*

$$f^m \in J,$$

and conversely.

Its proof is very interesting and important. Described very well in [Cox/Little/O'Shea]. Proof covered in class.

Decipher the following from the proof of Regular Nullstellensatz

Given $\mathbb{F} = $ ACF, $J = \langle f_1, \dots, f_s \rangle \subseteq \mathbb{F}[x_1, \dots, x_n]$ such that f vanishes on $V(J)$, then the following statements are equivalent (i.e. implications $\iff$ work both ways)

- $f \in I(V(J))$

Decipher the following from the proof of Regular Nullstellensatz

Given $\mathbb{F} = \text{ACF}$, $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$ such that f vanishes on $V(J)$, then the following statements are equivalent (i.e. implications $\iff$ work both ways)

- $f \in I(V(J))$
- $f^m \in J$ for some integer $m \geq 1$

Decipher the following from the proof of Regular Nullstellensatz

Given $\mathbb{F} = \text{ACF}$, $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$ such that f vanishes on $V(J)$, then the following statements are equivalent (i.e. implications $\iff$ work both ways)

- $f \in I(V(J))$
- $f^m \in J$ for some integer $m \geq 1$
- $V(J') = \emptyset$ for the ideal $J' = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n, y]$

Decipher the following from the proof of Regular Nullstellensatz

Given $\mathbb{F} = \text{ACF}$, $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$ such that f vanishes on $V(J)$, then the following statements are equivalent (i.e. implications $\iff$ work both ways)

- $f \in I(V(J))$
- $f^m \in J$ for some integer $m \geq 1$
- $V(J') = \emptyset$ for the ideal $J' = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n, y]$
- Given J, can you think of an approach to test if $f \in I(V(J))$? Note, you're given generators of J, not the generators of $I(V(J))$

Decipher the following from the proof of Regular Nullstellensatz

Given $\mathbb{F} = \text{ACF}$, $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$ such that f vanishes on $V(J)$, then the following statements are equivalent (i.e. implications $\iff$ work both ways)

- $f \in I(V(J))$
- $f^m \in J$ for some integer $m \geq 1$
- $V(J') = \emptyset$ for the ideal $J' = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n, y]$
- Given J, can you think of an approach to test if $f \in I(V(J))$? Note, you're given generators of J, not the generators of $I(V(J))$
- $f \in I(V(J)) \iff V(J') = \emptyset \iff 1 \in J' \iff$ reduced $\text{GB}(J') = \{1\}$

Decipher the following from the proof of Regular Nullstellensatz

Given $\mathbb{F} =$ ACF, $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$ such that f vanishes on $V(J)$, then the following statements are equivalent (i.e. implications $\iff$ work both ways)

- $f \in I(V(J))$
- $f^m \in J$ for some integer $m \geq 1$
- $V(J') = \emptyset$ for the ideal $J' = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n, y]$
- Given J, can you think of an approach to test if $f \in I(V(J))$? Note, you're given generators of J, not the generators of $I(V(J))$
- $f \in I(V(J)) \iff V(J') = \emptyset \iff 1 \in J' \iff$ reduced GB$(J') = \{1\}$
- Careful: $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$ whereas $J' = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n, y]$

Radical Ideals: Ideals with some special properties

We need to study one more type of ideal, called a radical ideal $\sqrt{J}$, that is related to J:

- In a general setting: $J \subset \sqrt{J} \subset I(V(J))$
- Over an ACF: $I(V(J)) = \sqrt{J}$ (This is the Strong Nullstellensatz)

Lemma

If $f^m \in I(V(J))$ then $f \in I(V(J))$

Definition

An ideal I is **radical** if $f^m \in I$ (for some $m \geq 1$) implies that $f \in I$

Lemma

From the Lemma and Definition above, it follows that the ideal $I(V(J))$ is radical.

How to find out whether an ideal is radical?

- For any (and all) polynomials f, such that $f^m \in J$ for some $m \geq 1$
  - If $f^m \in J$ implies that $f \in J$
  - Then the ideal J has the property that it is radical
- If you find a counter-example polynomial f with no m such that $f^m \in J$ implying $f \in J$, then J is not radical

Example (Counter-example for Radical Ideal)

Let $J = \langle x^3 \rangle$. Pick $f = x$. Does there exist some m, s.t. $f^m \in J$ while also implies that $f \in J$? No. E.g., consider $m = 3$ such that $f^3 = x^3 \in J$. But that does not imply $f \in J$. This is true for all $m \geq 3$. Ideal J is NOT radical.

Now consider the example on the next slide

How to find out whether an ideal is radical?

Example

Let $J = \langle x^2, x^4 - x \rangle \subset \mathbb{F}_4[x]$. Note $x^4 - x$ is a vanishing polynomial in $\mathbb{F}_4[x]$.

- Pick any polynomial f such that $f^m \in J$ for some $m \geq 1$
- Say, $f = x$, then for $m = 2$, we have $f^2 = x^2 \in J$:
- But this also implies that $f \in J$:
  - $f = x = x^2 \cdot (x^2) - 1 \cdot (x^4 - x)$; so $f \in J$
- Similarly, pick $f = \alpha x^2 + \alpha^2 x$ for $\alpha \in \mathbb{F}_4$
- $\exists m = 2 \ : \ f^m = f^2 = \alpha^2 x^4 + \alpha^4 x^2$, so $f^m \in J$ for some m
- Notice that $f^m \in J$ implies that $f \in J$
- $f = \alpha x^2 + \alpha^2 x = \alpha x^2 + \alpha^2 \cdot (x^2 \cdot x^2 - (x^4 - x))$ so $f \in J$
- The argument can be shown to hold for all f that $\exists m : f^m \in J \implies f \in J$
- Clearly the ideal $J = \langle x^2, x^4 - x \rangle \subset \mathbb{F}_4[x]$ is radical!

Radical Tests?

- Given an ideal J, is there an algorithm to find if it is radical?
- In theory, yes, but in practice this is infeasible
- An ideal may or may not be radical
- If an ideal J is NOT radical, then one can compute the Radical of J
- Radical of J is denoted as $\sqrt{J}$, where $\sqrt{\cdot}$ is just a "symbol"
- If the ideal J is itself radical, then computing the "radical of J" gives J itself, i.e. $\sqrt{J} = J$
- Definition of $\sqrt{J}$?

Please read and understand the following two concepts

From Cox/Little/O'Shea:

An ideal $\mathbf{I} = I(V(J))$ consisting of all polynomials that vanish on $V(J)$, has the property that if $f^m \in \mathbf{I} = I(V(J))$ then it implies that $f \in \mathbf{I} = I(V(J))$.

But that is the definition of a radical ideal: so $\mathbf{I} = I(V(J))$ is also a radical ideal

$\sqrt{J}$: The Radical of J

Let $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be an ideal. The radical of J, denoted $\sqrt{J}$ is the set:

$$\sqrt{J} = \{f \ : \ f^m \in J, \text{ for some } m \geq 1\}$$

An ideal is radical when $J = \sqrt{J}$.
Explain with Examples!

Examples for $J, \sqrt{J}$

The Radical of J is the smallest ideal containing J, which is also radical. It is possible to have $J \subset \sqrt{J} \subset J_1$ where J_1 is a radical ideal but it is different from the Radical of J.

Example

Let $J = \langle x^2 \rangle$

i) $\sqrt{J} = \langle x \rangle$

ii) $J_1 = \langle x, y \rangle$ is a radical ideal, but $J_1 \neq \sqrt{J}$

iii) $J \subset \sqrt{J} \subset J_1$

iv) $J_1 = \sqrt{J_1}$, since J_1 is a radical ideal too

Given J, SINGULAR provides a library function to compute the Radical of J (OK for small problems). See the SINGULAR file uploaded along with these slides. The procedure `radical(J)` is available through LIB "primdec.lib" in SINGULAR.

The Strong Nullstellensatz

Theorem (The Strong Nullstellensatz)

Over an algebraically closed field $I(V(J)) = \sqrt{J}$

To prove $I(V(J)) = \sqrt{J}$:

- Prove that $\sqrt{J} \subset I(V(J))$
  - Take an arbitrary polynomial $f \in \sqrt{J}$. This implies $f^m \in J$ (definition of a radical ideal)
  - Then f^m vanishes on $V(J)$, so f vanishes on $V(J)$
  - So, $f \in I(V(J))$. Therefore, $\sqrt{J} \subset I(V(J))$
- Prove that $\sqrt{J} \supset I(V(J))$
  - Let $f \in I(V(J))$. Then $f^m \in J$ (Regular Nullstellensatz)
  - If $f^m \in J$ then $f \in \sqrt{J}$
- Since both $I(V(J))$ and $\sqrt{J}$ contain each other, they are equal

Radical Membership Testing

Given generators of J, it is not always computationally feasible to identify generators of $\sqrt{J}$. But, it is possible to test for membership in $\sqrt{J}$, given J.

Theorem (Radical Membership)

Let $\mathbb{F}$ be a arbitrary field. Let $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be an ideal. Then a polynomial $f \in \sqrt{J} \iff 1 \in J' \iff reducedGB(J') = \{1\}$ where:

$$J' = \langle f_1, \ldots, f_s, 1 - y \cdot f \rangle \subset \mathbb{F}[x_1, \ldots, x_n, y],$$

and y is a new variable.

Consolidating the results

- Associated with an ideal J, there are two more ideals $\sqrt{J}, I(V(J))$
- In general: $J \subset \sqrt{J} \subset I(V(J))$
- Over ACF: $\sqrt{J} = I(V(J))$
- They have same solutions: $V(J) = V(\sqrt{J}) = V(I(V(J)))$ over ACF
- If f vanishes on $V(J)$, then $f \in I(V(J)) = \sqrt{J}$
- If J is radical, then $J = \sqrt{J} = I(V(J))$
- Given J, we cannot easily find generators of $\sqrt{J}$
- But we can test for membership in $\sqrt{J}$
  - $f \in \sqrt{J} \iff \text{reducedGB}(J + \langle 1 - y \cdot f \rangle) = \{1\}$
- $V(J_1) = V(J_2) \iff \sqrt{J_1} = \sqrt{J_2}$

Intuitively: Proving equality of circuits may not imply equality of ideal, but rather equality of their radicals!

Nullstellensatz over Galois fields $\mathbb{F}_q$

Given an ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$, and let $J_0 = \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle$

- $I(V_{\mathbb{F}_q}(J_0)) = I(V_{\overline{\mathbb{F}_q}}(J_0)) = J_0$

Nullstellensatz over Galois fields $\mathbb{F}_q$

Given an ideal $J = \langle f_1, \dots, f_s \rangle \subseteq \mathbb{F}_q[x_1, \dots, x_n]$, and let $J_0 = \langle x_1^q - x_1, \dots, x_n^q - x_n \rangle$

- $I(V_{\mathbb{F}_q}(J_0)) = I(V_{\overline{\mathbb{F}_q}}(J_0)) = J_0$
- What is $\sqrt{J_0}$?

Nullstellensatz over Galois fields $\mathbb{F}_q$

Given an ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$, and let $J_0 = \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle$

- $I(V_{\mathbb{F}_q}(J_0)) = I(V_{\overline{\mathbb{F}_q}}(J_0)) = J_0$
- What is $\sqrt{J_0}$?
- $\sqrt{J_0} = J_0$. IOW, J_0 is a radical ideal. Prove it.

Nullstellensatz over Galois fields $\mathbb{F}_q$

Given an ideal $J = \langle f_1, \dots, f_s \rangle \subseteq \mathbb{F}_q[x_1, \dots, x_n]$, and let $J_0 = \langle x_1^q - x_1, \dots, x_n^q - x_n \rangle$

- $I(V_{\mathbb{F}_q}(J_0)) = I(V_{\overline{\mathbb{F}_q}}(J_0)) = J_0$
- What is $\sqrt{J_0}$?
- $\sqrt{J_0} = J_0$. IOW, J_0 is a radical ideal. Prove it.
- $I(V(J_0)) = \sqrt{J_0} = J_0$

Nullstellensatz over Galois fields $\mathbb{F}_q$

Given an ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$, and let $J_0 = \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle$

- $I(V_{\mathbb{F}_q}(J_0)) = I(V_{\overline{\mathbb{F}_q}}(J_0)) = J_0$
- What is $\sqrt{J_0}$?
- $\sqrt{J_0} = J_0$. IOW, J_0 is a radical ideal. Prove it.
- $I(V(J_0)) = \sqrt{J_0} = J_0$

Nullstellensatz over Galois fields $\mathbb{F}_q$

Given an ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$, and let $J_0 = \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle$

- $I(V_{\mathbb{F}_q}(J_0)) = I(V_{\overline{\mathbb{F}_q}}(J_0)) = J_0$
- What is $\sqrt{J_0}$?
- $\sqrt{J_0} = J_0$. IOW, J_0 is a radical ideal. Prove it.
- $I(V(J_0)) = \sqrt{J_0} = J_0$

Proof: $J_0 = I(V(J_0)) = \sqrt{J_0}$

Take an arbitrary $f \in J_0$, so f is a vanishing polynomial over $\mathbb{F}_q$. It vanishes everywhere, so it vanishes on $V(J_0)$ too. Hence, $f \in I(V(J_0))$. Conversely, take $f \in I(V(J_0))$, then $f^m \in J_0$ (Regular Nullstellensatz). Which means f^m is a vanishing polynomial. $f^m = 0$ everywhere $\iff f = 0$ everywhere. This means $f \in J_0$. This proves $J_0 = I(V(J_0))$.

Since $V_{\mathbb{F}_q}(J_0) = V_{\overline{\mathbb{F}_q}}(J_0)$, we have: $J_0 = I(V_{\mathbb{F}_q}(J_0)) = I(V_{\overline{\mathbb{F}_q}}(J_0)) = \sqrt{J_0}$

Life is easy over Galois fields $\mathbb{F}_q$

Theorem ($J + J_0$ is radical)

Over Galois fields $\sqrt{J + J_0} = J + J_0$, i.e. $J + J_0$ is a radical ideal.

Note: J is an arbitrary ideal, and J_0 is the ideal of all vanishing polynomials. J_0 is radical, J may or may not be radical, but $J + J_0$ becomes radical! Proof is attached separately.

Example

I showed you on previous slides that $J = \langle x^2 \rangle$ and $J_0 = \langle x^4 - x \rangle$, then $J + J_0 = \langle x^2, x^4 - x \rangle \subset \mathbb{F}_4[x]$ is radical, i.e. $J + J_0 = \sqrt{J + J_0}$

Theorem (Strong Nullstellensatz over $\mathbb{F}_q$)

$$I(V_{\mathbb{F}_q}(J)) = I(V_{\overline{\mathbb{F}_q}}(J + J_0)) = \sqrt{J + J_0} = J + J_0$$

Apply Strong Nullstellensatz to Circuit Verification

- Now we will apply the Strong Nullstellensatz over $\mathbb{F}_q$ to verify circuits
- Formulate as f vanishes on $V(J)$
- So $f \in I(V(J))$
- We know that over Galois fields, $I(V(J)) = J + J_0$
- So test if $f \in J + J_0$ or test of $f \xrightarrow{GB(J+J_0)}_+ 0$?
- The challenge is to do this verification in a scalable fashion
- Next set of slides...