Nov 17: To recap:

Given an ideal \( J = \langle f_1, \ldots, f_s \rangle \), their variety \( \text{V}(J) \), there exists another ideal \( I(\text{V}(J)) = \) the ideal of all polynomials that vanish on \( \text{V}(J) \).

Result: If \( f \) vanishes on \( \text{V}(J) \), then \( f \in I(\text{V}(J)) \).

\[ J \subseteq I(\text{V}(J)) \]

Example:

\[ J = \langle x^2, y^2 \rangle \]
\[ I(\text{V}(J)) = \langle x, y \rangle \]
\[ f = x + y \]
\[ \text{V}(J) = \{ (0,0) \} \]
\[ f(x=0, y=0) = 0 \]
\[ f \in I(\text{V}(J)) \]
In general, we are always given \( \langle f_1, \ldots, f_s \rangle \) generators of \( J \).

But we are not given generators of \( \operatorname{I}(\mathcal{V}(\mathcal{S})) \).

Given \( J \), can we easily find the generators of \( \operatorname{I}(\mathcal{V}(\mathcal{S})) \)? \( \boxed{\text{NO! Not easy}} \)

**BUT**: Over finite fields.

\[ F_q [x_1, \ldots, x_n]. \]

\[ \operatorname{I}(\mathcal{V}(\mathcal{S})) = J + J_0 \]

\[ J_0 = \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle \]

\( J = \langle f_1, \ldots, f_s \rangle = \text{arbitrary} \).
Application to verification:

Given a circuit \( \mathcal{C} \), and a specification polynomial \( f \in \mathbb{F}_q[x_1, \ldots, x_n] \).

Does \( \mathcal{C} \) implement \( f \)?

**Answer:** \( \mathcal{C} \equiv f \iff f \) agrees with all evaluations of \( \mathcal{C} \)

\[ \iff f \) agrees with the truth-table of \( \mathcal{C} \)

1. Model \( \mathcal{C} \) with polynomials. \( \langle f_1, \ldots, f_s \rangle = \)

\[ \iff \) vanishes on \( \mathbb{V}(\mathcal{C}) \).

\[ \iff f \in \mathbb{I}(\mathbb{V}(\mathcal{C})) = \mathcal{J} + \mathcal{J}_0. \]

\[ \iff f \in \mathcal{J} + \mathcal{J}_0. \) [Ideal membership].

\[ \iff \) Compute \( G = \text{GB}(\mathcal{J} + \mathcal{J}_0) = \{ g_1, \ldots, g_t \} \)

\[ \iff f \) \begin{array}{c} \in \{ g_1, \ldots, g_t \} \\ + r = 0? \end{array} 

If \( r = 0 \), \( f \equiv \mathcal{C} \)

\( r \neq 0 \), \( f \neq \mathcal{C} \) [Bug in the design].
How do we know that over $F_q[x_1 \ldots x_n]$, $I(\mathcal{V}(f)) = J + J_0$?

* Study Radical ideals.
* Strong Nullstellensatz.

Radical Ideals: Ideals with special properties:

An ideal $I$ is radical if:
1. Take an arbitrary polynomial $f$.
2. There exists some integer $m > 1$
3. $f^m \in I$
4. and it also makes $f \in I$.

Not every ideal has the property that it is radical, but some ideals do.

* When $I \neq \text{radical}$, you can compute it's radical: $\sqrt{I}$
* When $I$ is radical, $I = \sqrt{I}$
In the slides, I have given 2 examples

1. $F_q[x]$. $\langle x^2, x^4-x \rangle = \text{radical}$

2. $F_q[x]$. $\langle x^3 \rangle$, is not radical

Ex. $J = \langle x^3 \rangle$, $\sqrt{J} = \langle x \rangle$

Ex. $J + J_0 = \langle x^3, x^4-x \rangle$, $\sqrt{J + J_0} = \langle x^2, x^4-x \rangle$

I. $\sqrt{J + J_0} = J + J_0$
The strong Nullstellensatz (SNS)

Over an algebraically closed field $\overline{F}$

\[ I(V_F(J)) = \sqrt{J} \]

\[ \sqrt{J} = I(V(J)) \]

Note: \[ J = \langle f_1, \ldots, f_s \rangle = \text{given} \rightarrow \text{known}. \]
\[ I(V(J)) = \langle h_1, \ldots, h_r \rangle = \sqrt{J} \]
\[ \text{not easy to compute.} \]

But over Finite fields

\[ I(V(J)) = J + J_0 \rightarrow \text{vanishing poly} \]
\[ \langle x^9 - x \rangle \]

How?

& why?
Strong Nullstellensatz over finite fields.

Let \( F_q[x_1, \ldots, x_n] \) be a polynomial ring.

Let \( J = \langle f_1, \ldots, f_s \rangle \) be an ideal.

\[
I(V_{F_q}(J)) = J + J_0
\]

**Proof:**

\[
V_{F_q}(J) = V_{F_q}(J + J_0)
\]

\[
\Rightarrow I(V_{F_q}(J)) = I(V_{F_q}(J + J_0))
\]

\[
= \sqrt{J + J_0} \quad [\text{SNS}]
\]

\[
= J + J_0 \quad [\text{radical}]
\]

So to check if \( f \in I(V_{F_q}(J)) \)

\[
\iff f \in J + J_0
\]

Apply this to ckt verification.
An intuitive explanation of why
\[ J + J_0 \subset F_q[x_1, \ldots, x_n] \] is radical.

**Radical**: An ideal is radical if
\[ \exists m \text{ s.t. } f^m \in J \quad \Rightarrow \quad f \in J. \]

Over \( F_q \), \( x^9 = x \) or \( f^9 = f \)
\[ \Rightarrow x^9 - x = 0 \quad \text{or} \quad f^9 - f = 0 \]
\[ \in J_0 \quad \text{or} \quad \in J_0. \]

So, \( \exists m = 9 \quad f^9 \in J \)
\[ \Rightarrow f \in J \]

How do you "tell" an ideal that \( x^9 = x \)?
\[ \Rightarrow \text{ include } \langle x^9 - x \rangle \text{ in your ideal} \]
\[ \text{or} \Rightarrow \text{ include } J_0. \]
\[ \Rightarrow J + J_0 = \sqrt{J + J_0} \]
Special Case

\[ J_0 = \langle x^9 - x, \ldots, x^9 - x \rangle \subseteq \mathbb{F}_9[x, \ldots, x_9] \]

\[ J_0 \subseteq \mathbb{F}_9 \]

\[ I(x(x_{50})) = 0 \quad \sqrt{J_0} = J_0 \]

\[ x + J_0 = \sqrt{x + J_0} \]

\[ I(x(x_{50})) = I(x(x_{50})) = J_0 \]

\[ I(x^9(x_{55})) = I(x^9(x_{55})) = J_0 \]

\[ x^9 = x \]

\[ x^9 - x = 0 \]

\[ J_0 = 9 \]
Finally, $J_1 = \langle h_1, \ldots, h_s \rangle$, $J_2 = \langle h_1, \ldots, h_r \rangle$

$V(J_1)$

if $V(J_1) = V(J_2)$

then $J_1$ may or may not be equal to $J_2$

But $V(J_1) = V(J_2)$

$\iff$

$\sqrt{J_1} = \sqrt{J_2}$

Apply to circuits. → next page.
\[
\sqrt{\mathfrak{J}_1 + \mathfrak{J}_0} = \sqrt{\mathfrak{J}_2 + \mathfrak{J}_0}
\]

Two varieties are the same if and only if their radical ideals are the same.

\[
\mathfrak{V}_{f_q}(\mathfrak{J}_1) = \mathfrak{V}_{f_q}(\mathfrak{J}_2) \implies \mathfrak{V}_{f_q}(\mathfrak{J}_1 + \mathfrak{J}_0) = \mathfrak{V}_{f_q}(\mathfrak{J}_2 + \mathfrak{J}_0)
\]

As these ideals are radical.