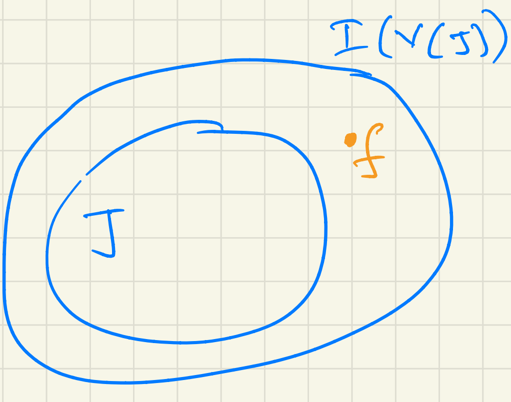
Nov 17:

To recap:

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

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

$$J \subseteq I(V(J))$$



Example:

$J = \langle x^2, y^2 \rangle$; $I(V(J)) = \langle x, y \rangle$

$f = x + y$.

$V(J) = \{(0,0)\}$

$f(x=0, y=0) = 0$

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

In general, we are always given $\underbrace{\langle f_1 \ldots f_s \rangle}_{\text{generators of } J}$

$$J = \langle f_1 \ldots f_s \rangle.$$

generators of J

But we are **not** given generators of $I(V(J))$

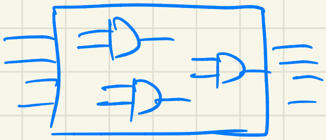
Given J, can we easily find the generators of $I(V(J))$? $\boxed{\text{NO! Not easy}}$

BUT: Over finite fields.

$$\mathbb{F}_q[x_1 \ldots x_n].$$

$$\boxed{\begin{aligned} I(V(J)) &= J + J_0 \\ J_0 &= \langle x_1^q - x_1, \ldots \ldots, x_n^q - x_n \rangle \\ J = \langle f_1 \ldots f_s \rangle &= \text{arbitrary} \end{aligned}}$$

Application to verification:



Circuit C

Given a ckt C, and a specification polynomial f $\mathbb{F}_q[x_1 \dots x_n]$.

Does C implement f?

Answer: $C \equiv f \iff f$ agrees with all evaluations of C

$\iff f$ agrees with the truth-table of C

1 Model C with polynomials. $\langle f_1 \dots f_s \rangle = J$

f vanishes on $V_{\mathbb{F}_q}(J)$.

$\iff f \in I(V(J)) = J + J_0$.

$\iff f \in J + J_0$ [Ideal membership].

2. Compute $G = GB(J + J_0) = \{g_1 \dots g_t\}$

$\iff f \xrightarrow{\{g_1 \dots g_t\}}_+ r = 0$?

If $r = 0$, $f \equiv C$

$r \neq 0$, $f \not\equiv C$ [BUG in the design]

Q How do we know that over $\mathbb{F}_q[x_1 \cdots x_n]$, $I(V(J)) = J + J_0$?

* Study Radical ideals.
* Strong Nullstellensatz.

———x———x———

Radical Ideals: Ideals with special properties:

An ideal 'I' is radical if:

1. Take an arbitrary polynomial f
2. There exists some integer $m \geq 1$
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 $I \neq$ 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. $\mathbb{F}_q[x]$. $\langle x^2, x^4 - x\rangle = \text{radical}$

$J + J_0$

2. $\mathbb{F}_q[x]$. $\langle x^3\rangle$, is not radical

Ex 1 $J = \langle x^3\rangle$, $\sqrt{J} = \langle x\rangle$

$\neq$

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

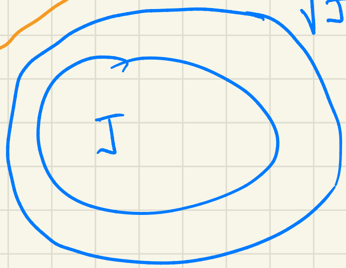
$\sqrt{J+J_0} = J + J_0$

The Strong Nullstellensatz. (SNS)

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

$$\boxed{I(V_{\overline{F}}(J)) = \sqrt{J}}$$

$\sqrt{J} = I(V(J))$



Note: $J = \langle f_1 \dots f_s \rangle$ = given

→ Known.

$$I(V(J)) = \langle h_1 \dots h_r \rangle = \sqrt{J}$$

→ not easy to compute.

But over Finite fields

$$I(V(J)) = J + J_0$$

→ vanishing poly

$\langle x^q - x \rangle$

How?

& why?

Strong Nullstellensatz over finite fields.

Let $\mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial ring.

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

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

Proof: $V_{\mathbb{F}_q}(J) = V_{\mathbb{F}_q}(J + J_0)$

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

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

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

So to check if $f \in I(V_{\mathbb{F}_q}(J))$

$$\Longleftrightarrow f \in J + J_0$$

Apply this to ckt verification.

An intuitive explanation of why

$J + J_0 \subset \mathbb{F}_q[x_1, \dots x_n]$ is radical.

Radical: An ideal is radical if

$\exists m$ s.t. $f^m \in J$

$\Rightarrow f \in J.$

Over $\mathbb{F}_q$ $x^q = x.$ or $f^q = f$

$\Rightarrow \underbrace{x^q - x}_{\in J_0} = 0$ or $\underbrace{f^q - f}_{\in J_0.} = 0$

So $\exists m = q,$ $f^q \in J$

$\Rightarrow f \in J$

How do you "tell" an ideal that $x^q = x$?

$\Rightarrow$ include $\langle x^q - x \rangle$ in your ideal

or $\Rightarrow$ include J_0.

$\Rightarrow J + J_0 = \sqrt{J + J_0}$

Special cases.

$$J_0 = \langle x_1^q - x_1, \dots, x_n^q - x_n \rangle$$
$$\subseteq \mathbb{F}_q[x_1, \dots, x_n]$$

$$I(V(J_0)) = ? \ \sqrt{J_0} = J_0$$

J_0

$$\cancel{f} + J_0 = \sqrt{\cancel{f} + J_0}$$

$$I(V(\underline{J_0})) = I(\mathbb{F}_q) = J_0$$

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

$$x^q = x$$

$$= \sqrt{J_0}$$

$$x^q - x = 0$$

$$\#m = q$$

$$= J_0$$

Finally, $J_1 = \langle f_1 \dots f_s \rangle$, $J_2 = \langle h_1, \dots h_r \rangle$

$V(J_1)$ $\qquad$ $V(J_2)$.

If $V(J_1) = V(J_2)$

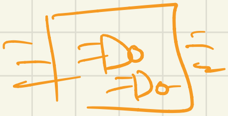
then J_1 may or may not be equal to J_2

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

$$\Longleftrightarrow$$

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

Apply to circuits. $\longrightarrow$ next page.



CKT C_1

$J_1 = \langle f_1 \ldots f_s \rangle$

CKT C_2.

$J_2 = \langle h_1, \ldots h_r \rangle$.

Truth table of C_1 $\equiv$ truth table of C_2

$V_{\mathbb{F}_q}(J_1) \equiv V_{\mathbb{F}_q}(J_2)$

$\Rightarrow V_{\overline{\mathbb{F}_q}}(J_1 + J_0) \equiv V_{\overline{\mathbb{F}_q}}(J_2 + J_0)$

Two varieties are the same

implies $\Rightarrow$ their radical ideals are the same

$\sqrt{J_1 + J_0} \equiv \sqrt{J_2 + J_0}$

$\Rightarrow J_1 + J_0 \equiv J_2 + J_0$

(as these ideals are radical).