Nov. 15

When two ideals are the Same, their varieties are too.

$I_1 = \langle f_1, \dots, f_s \rangle$, $I_2 = \langle h_1, \dots, h_r \rangle$

If $I_1 = I_2$, then

$$V(I_1) = V(I_2)$$

But the converse is not true: Given I_1 & I_2

If $V(I_1) = V(I_2)$

then

I_1 may NOT be equal to I_2.

But I_1 and I_2 are related.

Example $I(V(I_2)) = I_1$

$I_1 = \langle x, y \rangle$

$I_2 = \langle x^2, y^2 \rangle$

$V(I_1) = \{(0,0)\}$

Soln. to $x = 0$ & $y = 0$

$V(I_2) = \{(0,0)\}$

Soln. to $x^2 = 0$, $y^2 = 0$

$\sqrt{I_2} = I_1$

$V(I_1) = V(I_2)$

But $I_1 \neq I_2$.

$\sqrt{I_1} = \sqrt{I_2}$

$I_1 \qquad I_1$

$x \in I_1$

$x + y \in I_1$

$(x+y)^2 \in I_1$

$\underbrace{x^2 + y^2 + 2xy}_{\in I_1}$

$x \notin I_2$

$(x+y) \notin I_2$

$(x+y)^2 =$

$x^2 + y^2 + 2xy$

$\in I_2 \qquad \in I_2 \qquad \notin I_2?$

But $\langle x, y \rangle \leftrightsquigarrow \langle x^2, y^2 \rangle$

related by "powers"

Mystery?: Variety depends on the ideals, but it is not uniquely defined by the ideals.

Variety is uniquely defined by "radicals" → the subject of the Strong Nullstellensatz, and required for a sound & complete approach to verification.

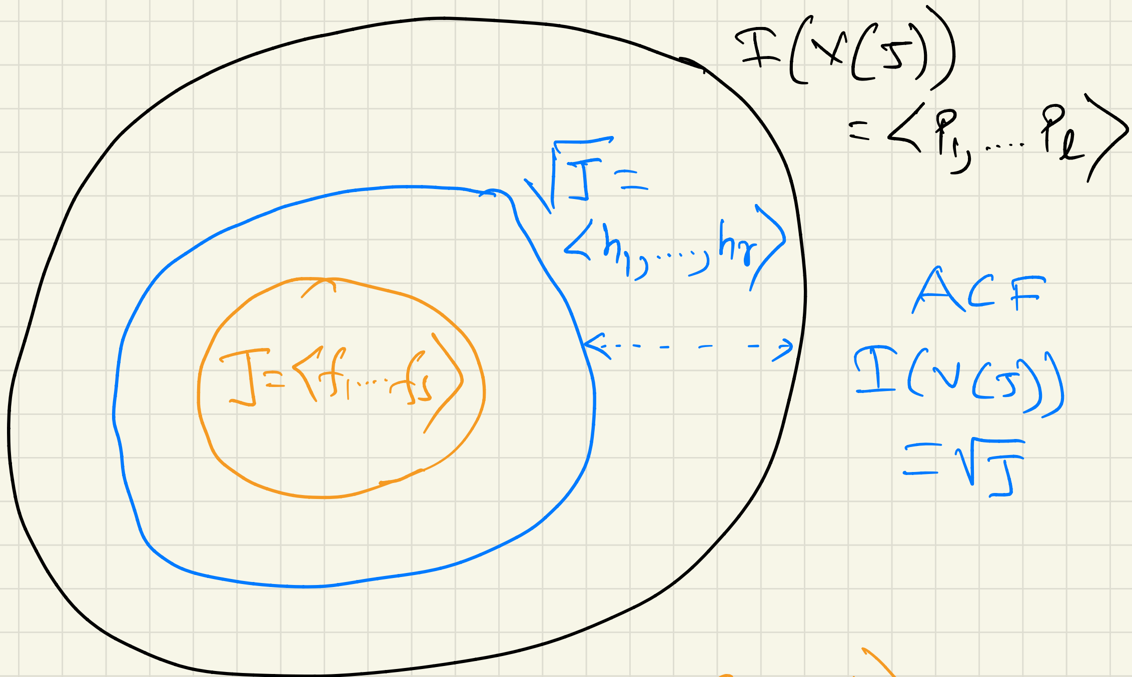
(also scalable/efficient procedure)

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

Associated with ideal J, there are two other ideals:

① $\sqrt{J}$ = radical of J

② $I(V(J))$



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

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

First, we study $I(V(J))$

$=$ Ideal of polynomials that vanish $(=0)$ on a variety

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

$J = \langle x^2, y^2 \rangle$ $\qquad g = xy$

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

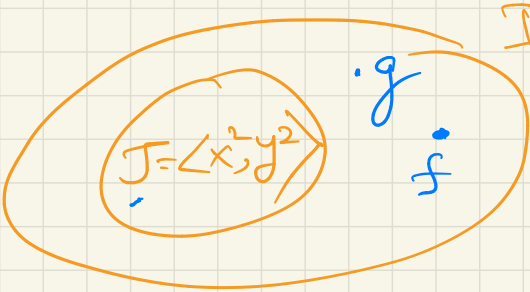
$f = x + y$. $\qquad f \notin J$,

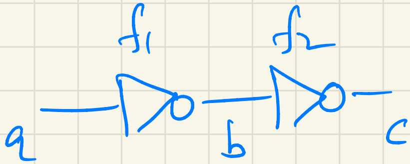
$f(x=0, y=0) = 0$.

<u>Note</u>. $f \notin J$. But f vanishes on $V(J)$.

So $f \in I(V(J))$, $g \in I(V(J))$

$I(V(J))$





$\mathbb{F}_2[a,b,c]$

$f_1: b = 1 + a$

or $b + a + 1$

$J = \langle f_1, f_2 \rangle$

$f_2: c + b + 1$

$f: c + a$ [modeling $c = a$]

$$V_{\mathbb{F}_2}(J) = \left\{ \begin{array}{ccc} a & b & c \\ (0 & 1 & 0) \\ (1 & 0 & 1) \end{array} \right\}$$

$f(a=0, c=0) = 0$

$f(a=1, c=1) = 0$

so f vanishes on $V(J)$.

Does f vanish on $V(J)$? $\Longleftrightarrow$

Does f agree with all evaluations of the circuit?

$f(a=0, c=0) = 0$; $f(a=1, c=1) = 0$.

$\Rightarrow$ f does vanish on $V_{\mathbb{F}_2}(J)$

$f \in \underbrace{I(V(J))}_{\langle h_1 \dots h_r \rangle}$? $\quad f \xrightarrow{GB(h_1 \cdots h_r)}_{+} 0$?

$J = \langle f_1, \dots, f_s \rangle$

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

$\langle f_1, f_2 \rangle + \langle a^2 - a,\ b^2 - b,\ c^2 - c \rangle$

$c + a \in J + J_0$

In general, given generators of J.

$$J = \langle f_1, \dots, f_s \rangle$$

not possible to find generators of $I(V(J))$

$$I(V(J)) = \langle \underbrace{h_1, \dots, h_r}_{??} \rangle$$

But over $\mathbb{F}_q[x_1, \dots, x_n]$

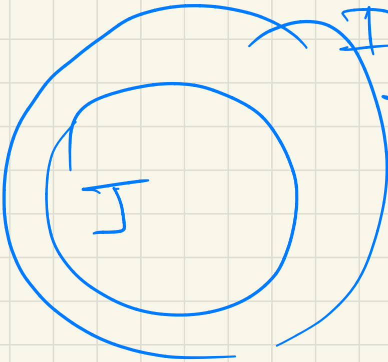
$$\boxed{I(V(J)) = J + J_0}$$

$$J_0 = \langle x_1^q - x_1,\ x_2^q - x_2,\ \dots,\ x_n^q - x_n \rangle$$

why? . . . .

$\mathbb{F}_2[a,b] \to f_1, f$

$\underline{J} = \langle f_1, f_2, \underbrace{\cancel{a^2-a}, \cancel{b^2-b}}_{J_0} \rangle$



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

$J = J + J_0$

$J \subseteq J + J_0$

$\subset J_0$

SNS over ACF.

$$I(V(J_1)) = \sqrt{J_1}$$

over F_q.

$$I(V_{F_q}(J)) = I\left(V_{F_q}(\underbrace{J+J_0}_{J_1})\right)$$

test $f \in$

$$= \sqrt{J_1}$$

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

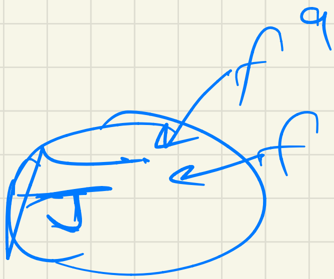
$f \in$ $$= J+J_0$$

$\exists\, m$ if $f^m \in J$

$\Rightarrow f \in J$

$m = q$

$J = \langle f_1, \dots, f_s \rangle$



$f^q \in J \overset{?}{\Longrightarrow} f \in J$

$x^q = x$

$f^q = f$

$J =$ radical