$$\mathbb{F}_{2^k} = \mathbb{F}_2[x] \pmod{P(x)}$$

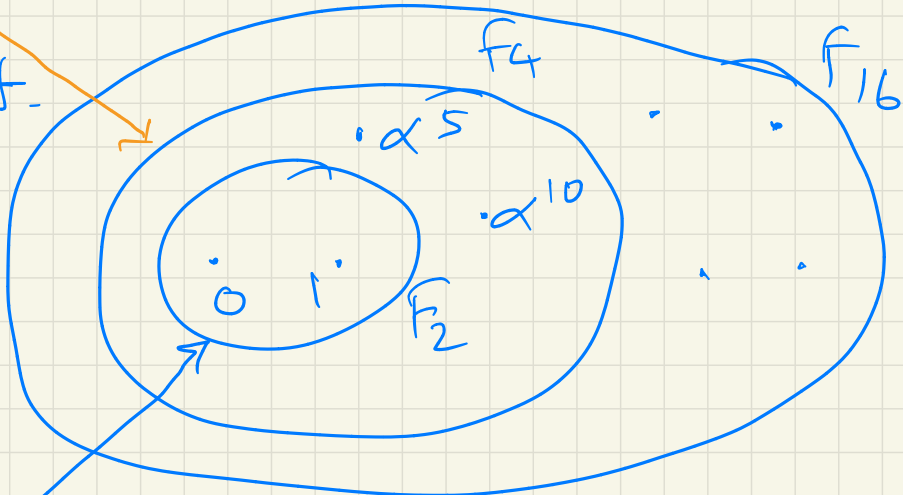
$$P(\beta) = 0.$$

Every $\mathbb{F}_2 = \{0,1\} \subset \mathbb{F}_{2^k}$

$k > 1$

$x^4 - x$

$J = \langle f_1 f_-$



$\underline{x^2 - x = 0}$ $\quad 0^2 - 0 = 0, \quad 1^2 - 1 = 0.$

$\mathbb{F}_2 = \{0,1\}.$

$V(x^2 - x) = \{0,1\} = \mathbb{F}_2.$

$\mathbb{F}_4 = \{0,1,\beta,\beta^2\}$ $\quad x^4 - x = 0$

$$\mathbb{F}_4 = \mathbb{F}_2[x] \pmod{P(x)}$$

$$P(x) = x^2 + x + 1 \quad \beta$$

$$P(\beta) = 0$$

$$\beta^2 + \beta + 1 = 0 \quad \text{or} \quad \beta^2 = \beta + 1$$

$$\mathbb{F}_4 = \{0, 1, \beta, \beta^2 = \beta + 1\}$$

$$x^4 - x = 0. \qquad 0^4 - 0 = 0$$

$$1^4 - 1 = 0$$

$$\beta^4 - \beta = 0.$$

$$(\beta^2)(\beta^2) - \beta = 0$$

$$(\beta+1)(\beta+1) - \beta = 0$$

$$\beta^2 + \cancel{2\beta} + 1 - \beta = 0$$

$$(\beta + 1) + 1 - \beta = 0$$

$$0 = 0.$$

$$(\beta^2)^4 - \beta = 0$$

$$V(x^4 - x) = \{0, 1, \beta, \beta^2\} = \mathbb{F}_4$$

$\beta^2 - \beta = (\beta+1) + \beta = 1 = 0$?

$x^2 - x$

Any $\mathbb{F}_q$. $x^q = x$

$x^q - x = 0$.

$(x^q - x)$ = Vanishing polynomial of $\mathbb{F}_q$.

let $J_0 = \langle x^q - x \rangle \subset \mathbb{F}_q[x]$.

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

$= \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}, \alpha^{q-1} = 1\}$

J_0 = ideal of ALL vanishing polynomials.

$$R = \mathbb{F}_q[x_1, \dots, x_n]$$

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

$\mathbb{F}_{2^k} \subset \mathbb{F}_{2^n}$.
$k \mid n$

$$\underline{V_{\mathbb{F}_q}(J_0)} = (\mathbb{F}_q)^n = \mathbb{F}_q^n$$

$$V_{\overline{\mathbb{F}_q}}(J_0) = (\mathbb{F}_q)^n.$$

$$\boxed{V(J_0) = \underline{V_{\mathbb{F}_q}(J_0) = V_{\overline{\mathbb{F}_q}}(J_0)}}$$

$$= (\mathbb{F}_q)^n = \mathbb{F}_q^n$$

$$1 \in \langle f_1, \dots, f_s \rangle$$

$$1 \xrightarrow{GB(f_1, \dots, f_s) = \{g_1, \dots, g_t\}}_{+} 0 \ ?$$

$$1 \xrightarrow{g_1, \dots, g_t} 0 \ \checkmark$$

$$g_1 \overline{\big) \ \underline{1 = f}}$$

$$g_1 = LT(g_1) + T$$

$$r = f - \frac{LT(f)}{LT(g)} \cdot g$$

$$= 1 - \boxed{\frac{1}{LT(g)}} \cdot g$$

$$\underline{g = 1}$$

$\{g_1, \dots, g_t\}$

$\{g_1 = 1, \cancel{g_2}, \cancel{g_3}, \dots, \cancel{g_t}\}$

is $lm(g_1) \mid lm(g_2)$ ✓

$\cancel{g_3}$

$\rightarrow \{g_1 = 1\}$

$R = \cancel{\mathbb{Q}}[x] \qquad I = \langle x^2+1 \rangle$

$GB(x^2+1) = \{g_1 = x^2+1\}$

$V_C(x^2+1) \neq \phi$?

$I = \langle f_1, f_2 \rangle$
$\subset \mathbb{F}_2[x,y]$

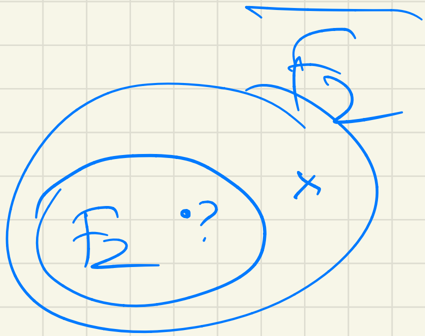
$V_{\mathbb{F}_2}(\underline{f_1, f_2}) = \emptyset ?$

GB

$V_{\overline{\mathbb{F}_2}}(\underline{g_1, g_2}) = \emptyset ?$

$\neq \{1\}$

$(f_1, f_2, x^2 - x, y^2 - y)$



November 10

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

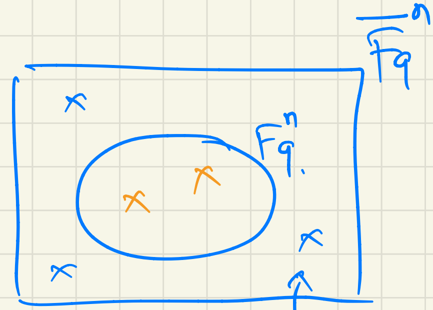
$$V(J) = V_{\overline{\mathbb{F}_q}}(J).$$

We need to analyze variety over $\mathbb{F}_q$ itself, not over the closure $\overline{\mathbb{F}_q}$.

[the circuit works over $\mathbb{F}_q$, not $\overline{\mathbb{F}_q}$].

$$V_{\mathbb{F}_q}(J) = V_{\overline{\mathbb{F}_q}}(J) \cap \mathbb{F}_q^n$$

2 pts.   5 pts. $\cap\, \mathbb{F}_q^n$



$$V(J) \subset \overline{\mathbb{F}_q}^n$$

Significance of J_0:

Equivalence chk example

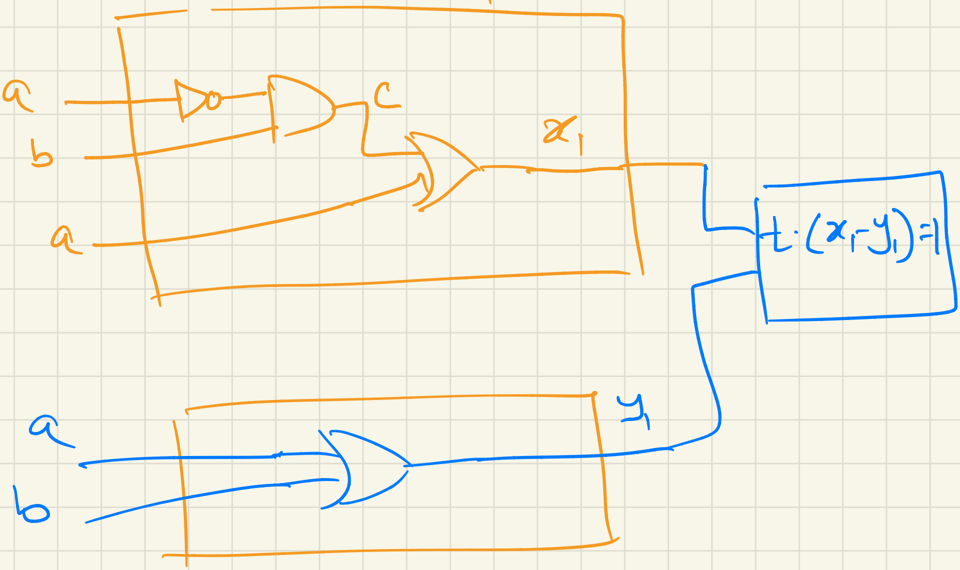
$x_1 = y_1$

spec: $a \vee \bar{a} b = x_1$

Impl: $a \vee b = y_1$

F_2

spec.



Impl.

$f_1: (1-a) \cdot b + c = 0.$

$f_2: c + a + c \cdot a + x_1 = 0$

$f_3: a + b + a \cdot b + y_1 = 0.$

$f_m: t \cdot (x_1 - y_1) + 1 = 0.$

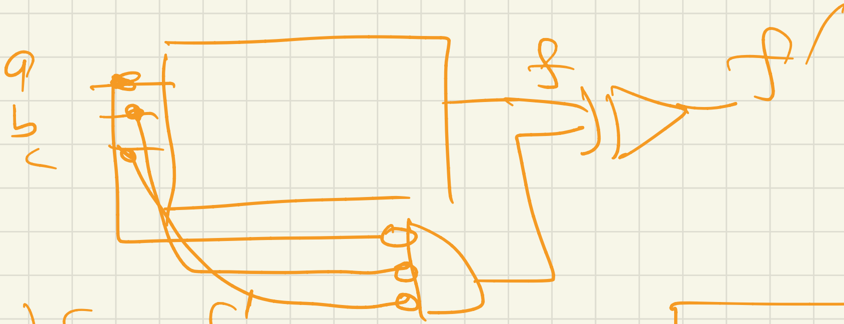
$J = \langle f_1, f_2, f_3, f_m \rangle$

$J_0 = \langle a^2 - a, b^2 - b, \dots \dots t^2 - t \rangle$

$GB(J) \neq \{1\}$

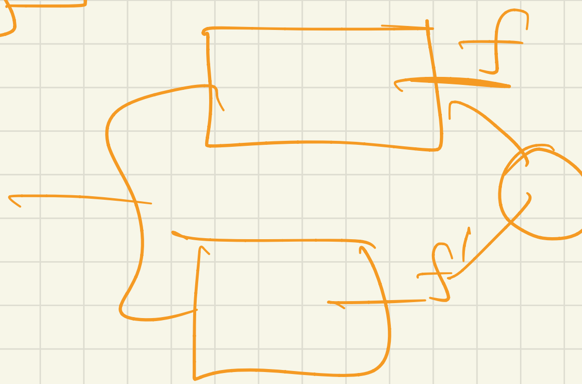
$GB(J + J_0) = \{1\}$

See the file "f2.sing" on class website.



abc	f	f'
000	0	1
	0	
	0	
	0	

Spec Imp.



$$GB(J + J_0) = \{1\}$$

$$SM = \{1\}$$

How to generate a circuit f' from f, such that f agrees with f' everywhere except at 1 point.