

**Definition :** We define a class  $\mathcal{C}$  in  $\mathbb{F}[x_1, x_2, \dots]$  as follows :

1.  $x_i \in \mathcal{C}$ .
2. If  $p \in \mathbb{F}[x_1, \dots, x_n], q \in \mathbb{F}[y_1, \dots, y_m]$  and  $\text{Var}(p) \cap \text{Var}(q) = \emptyset$  then
  - (a)  $p + q \in \mathcal{C}$ .
  - (b)  $p \times q \in \mathcal{C}$ .
  - (c)  $\forall m \geq 1 : p^m \in \mathcal{C}$ .

**Definition :** If  $p \in \mathbb{F}[x_1, \dots, x_n]$  then

$$\text{Jacob}(p) \equiv \left\langle \frac{\partial p}{\partial x_i} \mid x_i \in \text{Var}(p) \right\rangle$$

**Theorem :** If  $p \in \mathcal{C}$ , then  $\text{Gröbner}(\text{Jacob}(p)) = \text{Jacob}(p)$ .

**Proof :** The proof is by induction on the structure of the polynomials in  $\mathcal{C}$ .

**[Basis]**

If  $p \in \mathcal{C}$  and  $p = x_i$  then  $\frac{\partial p}{\partial x_j} = 0$ , if  $i \neq j$ ,  $\frac{\partial p}{\partial x_i} = 1$ , if  $i = j$ . Clearly  $\text{Jacob}(p) = \langle 1 \rangle$ , which is a Gröbner basis. So the basis case holds.

**[Additive Case]**

If  $p, q \in \mathcal{C}$  and  $\text{Var}(p) \cap \text{Var}(q) = \emptyset$ , then if  $R = p + q$ ,

$$\begin{aligned} \frac{\partial R}{\partial x_i} &= \frac{\partial P}{\partial x_i}, \text{ if } x_i \in \text{Var}(p) \\ \frac{\partial R}{\partial x_i} &= \frac{\partial P}{\partial x_i}, \text{ if } x_i \in \text{Var}(q) \end{aligned}$$

$$\overline{S\left(\frac{\partial p}{\partial x_i}, \frac{\partial p}{\partial x_j}\right)}^{\text{Jacob}(p+q)} = 0$$

by Induction Hypothesis as the entries of  $\text{Jacob}(p)$  are in the basis.

$$\text{Similarly } \overline{S\left(\frac{\partial q}{\partial x_i}, \frac{\partial q}{\partial x_j}\right)}^{\text{Jacob}(p+q)} = 0$$

$$\text{Further } \text{LM}\left(\frac{\partial p}{\partial x_i}\right) \perp \text{LM}\left(\frac{\partial q}{\partial x_j}\right) \text{ as } \text{Var}(p) \cap \text{Var}(q) = \emptyset$$

So  $\langle \text{Jacob}(p), \text{Jacob}(q) \rangle = \langle \text{Jacob}(R) \rangle$  is a Gröbner basis.

We split the multiplicative case into two analyses as follows :

**[Monomial Case]**

If  $R = x_1^{a_1} \cdots x_n^{a_n}$  then the S-Poly is always zero. Hence  $\text{Jacob}(R)$  forms a Gröbner basis.

**[Multiplicative Case]**

If  $R \in \mathcal{C}$  is not a monomial then we can express it as one of the following :

$$\begin{aligned} R &= (f + g) \times h \text{ The Var sets are mutually disjoint} \\ R &= h \times (f + g) \end{aligned}$$

Let  $f_i = \frac{\partial f}{\partial x_i}$ ,  $h_j = \frac{\partial h}{\partial x_j}$ . We assume that through the induction the following invariant is also maintained for the S-Poly.

$$\begin{aligned} S(f_i h, f h_j) &= \frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(f h_j))}{\text{LT}(f_i h)} f_i h - \frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(f h_j))}{\text{LT}(f h_j)} f h_j \\ &= \alpha_1 f_1 h + \alpha_2 f_2 h + \cdots + \alpha_k f_k h + \beta_1 f h_1 + \beta_2 f h_2 + \cdots + \beta_l f h_l \end{aligned}$$

Such that

$$\frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(f h_j))}{\text{LT}(f h_j)} f h_j = \beta_1 f h_1 + \beta_2 f h_2 + \cdots + \beta_l f h_l$$

We assume  $R = (f + g) \times h$ ,

$$\begin{aligned} \frac{\partial R}{\partial x_i} &= f_i h, \text{ if } x_i \in \text{Var}(f) \\ \frac{\partial R}{\partial x_i} &= g_i h, \text{ if } x_i \in \text{Var}(g) \\ \frac{\partial R}{\partial x_i} &= (f + g)h, \text{ if } x_i \in \text{Var}(h) \end{aligned}$$

Note that these are the entries in  $\text{Jacob}(R)$ , and we have to show they form a Gröbner basis.

Now consider  $S(f_i h, (f + g)h_j)$ , as  $\text{Var}(p) \cap \text{Var}(q) = \emptyset$ , either  $\text{LT}(f) \prec \text{LT}(g)$  or  $\text{LT}(f) \succ \text{LT}(g)$ . We assume that  $\text{LT}(f) \succ \text{LT}(g)$  in the following.

$$\begin{aligned} S(f_i h, (f + g)h_j) &= \frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(f h_j))}{\text{LT}(f_i h)} f_i h - \frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(f h_j))}{\text{LT}(f h_j)} (f + g)h_j, \\ (\text{as } \text{LM}((f + g)h_j) &= \text{LM}(f h_j)) \\ &= \frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(f h_j))}{\text{LT}(f_i h)} f_i h - \frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(f h_j))}{\text{LT}(f h_j)} f h_j - \frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(f h_j))}{\text{LT}(f h_j)} g h_j \end{aligned}$$

By Inductive Hypothesis

$$\frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(f h_j))}{\text{LT}(f h_j)} f h_j = \beta_1 f h_1 + \beta_2 f h_2 + \cdots + \beta_l f h_l$$

Which implies that

$$\beta_1 g h_1 + \beta_2 g h_2 + \cdots + \beta_l g h_l = \frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(f h_j))}{\text{LT}(f h_j)} g h_j$$

as  $\mathbb{F}[x_1, \dots, x_n]$  is an integral domain.

$$\text{Hence } \overline{S(f_i h, (f + g)h_j)}^{\text{Jacob}((f + g)h)} = 0.$$

$$\text{Note that } \beta_1 (f + g)h_1 + \beta_2 (f + g)h_2 + \cdots + \beta_l (f + g)h_l = \frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(f h_j))}{\text{LT}(f h_j)} (f + g)h_j$$

so the induction goes through.

Now in the case that  $LT(f) \prec LT(g)$ , we have

$$\begin{aligned}
S(f_i h, (f + g)h_j) &= \frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(g h_j))}{\text{LT}(f_i h)} f_i h - \frac{\text{lcm}(\text{LM}(f_i h), \text{LM}(g h_j))}{\text{LT}(g h_j)} (f + g)h_j \\
&= LM(f_i g) \frac{\text{lcm}(LM(h), LM(h_j))}{LT(f_i) LT(h)} f_i h - LM(f_i g) \frac{\text{lcm}(LM(h), LM(h_j))}{LT(g) LT(h_j)} (f + g)h_j \\
&= LM(g) \frac{\text{lcm}(LM(h), LM(h_j))}{LT(h)} f_i h - LM(f_i) \frac{\text{lcm}(LM(h), LM(h_j))}{LT(h_j)} (f + g)h_j
\end{aligned}$$

Assuming the polynomials are monic this is true, as  $LT(f) = LM(f)$  in that case.

*[Ken : Finally this is the case which has to be tackled. Since the other cases are symmetric.]*

**[Powering Case]** If  $R = p^m$  for some  $m \geq 1$ , we have  $\text{Jacob}(p^m) = p^{m-1}(\text{Jacob}(p))$ . Clearly if  $\langle f \rangle$  is a principal ideal and  $I$  is an ideal for which  $G_I$  is a Gröbner basis then we have  $f \times G_I = \langle f \times g \mid g \in G_I \rangle$  is also a Gröbner basis as all the S-Poly are now  $f \times S(g_i, g_j)$  where  $g_i, g_j \in G_I$  which are zero by Induction. Hence  $\text{Jacob}(p^m)$  is also a Gröbner basis.