Properties of Gröbner Bases

every ideal $I \subseteq K[x_1, \dots, x_n]$ has a GB. !!

Prop Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal, let $G = \{g_1, \dots, g_t\}$ be a GB for I. Given $f \in K[x_1, \dots, x_n]$. There $\exists$ a unique $r \in K[x_1, \dots, x_n]$ s.t.

(i) No term of r is div by any of $LT(g_1), \dots, LT(g_t)$

(ii) $\exists\ g \in I$ s.t. $f = g + r$

proof: Existance done H.B.T proof.

uniqueness: say $f = g + r = g' + r'$ satisfy (i), (ii)

$\Rightarrow r - r' = g' - g \in I$

If $r \neq r'$

$LT(g_i) \mid LT(r - r')$

but this is a contradiction of (i) ∎

Have shown:

unique remender r of div. by GB

$f = q_1 g_1 + \cdots + q_t g_t + r$ ← Normal form

$q_1, \dots, q_t$ not unique.

$\overline{f}^{G} = r$ where $G = \{g_1, \dots, g_t\}$

Cor for any ideal $I \subseteq k[x_1, \dots, x_n]$ $f \in I$ iff $\text{rem} = \bar{f}^G = 0$ of division of f by

$G = \{g_1, \dots, g_t\}$ Any Grobner basis of I.

To Solve ideal membership we just divide by GB

One way $\{f_1, \dots, f_s\}$ can fail to be a GB is if

$ax^\alpha f_i - bx^\beta f_j$ cancels some leading terms of f_i or f_j.

Def Let $f, g \in K[x_1, \dots, x_n]$

(i) $\text{multdeg}(f) = \alpha$, $\text{multdeg}(g) = \beta$

$\gamma = (\gamma_1, \dots, \gamma_n)$ $\gamma_i = \max(\alpha_i, \beta_i)$

$x^\gamma = \text{lcm}(LM(f), LM(g))$

↑ least common multiple

(ii) The S-polynomial of f and g is

$$S(f,g) = \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g.$$

Ex $f = x^3y^2 - x^2y^3 + x$, $g = 3x^4y + y^2$ (grlex)

$\gamma = (4, 2)$ $\quad x^\gamma = x^4y^2 = \text{lcm}$

$$S(f,g) = \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g$$

$$= -x^3y^3 + x^2 - \frac{y^3}{3}$$

Lemma $\quad \mathcal{F} = \sum_{i=1}^{s} p_i$, $\quad \text{multdeg}(p_i) = \delta \in \mathbb{N}^n \ \forall i$

if $\text{multdeg}(\mathcal{F}) < \delta$

$\Rightarrow$ p is a lin. combo of S-poly $S(p_j, p_k)$

Also $\quad \text{multdeg}(S(p_i, p_j)) < \delta$.

Proof: Since $\text{multdeg}(\mathcal{F}) < \delta$ but $\text{multdeg}(p_i) = \delta$

$$\sum LC(p_i) = 0$$

$$\text{lcm}(p_i, p_j) = LM(p_j)$$

$$S(p_i, p_j) = \frac{1}{LC(p_i)} p_i - \frac{1}{LC(p_j)} p_j$$

$$\text{multdeg}(S(p_i, p_j)) < \delta$$

Since $LM(p_i), LM(p_j)$ cancel

Let $d_i = LC(p_i)$

$$\sum_{i=1}^{s-1} d_i \, S(p_i, p_s) = d_1 \left(\frac{1}{d_1} p_1 - \frac{1}{d_s} p_s \right) + \cdots$$

$$= p_1 + \cdots + p_{s-1} - \frac{1}{d_s} (\underbrace{d_1 + \cdots + d_{s-1}}_{= -d_s \text{ since } \sum d_i = 0}) p_s$$

$$= p_1 + \cdots + p_{s-1} + p_s = 0 \quad \blacksquare$$

Thm (Buchberger's Criterion)

Let I be an ideal in $K[x_1, \ldots, x_n]$. A basis $G = \{g_1, \ldots, g_t\}$ of I is a Gröbner basis of I iff for all pairs $i \neq j$ the rem. of div of $S(g_i, g_j)$ by G (in any order of g_i's) is zero.

Proof:

$\Rightarrow$ if G a gb $\Rightarrow$ $S(g_i, g_j) \in I \Rightarrow$ $\overline{S(g_i, g_j)}^{G} = 0$

$\Leftarrow$

Let $f \in I$ Show $LT(f) \in (LT(g_1), \ldots, LT(g_t))$

$$f = \sum_i h_i g_i \quad \text{(polys)}$$

$$\text{mult deg}(f) \leq \max\left(\text{mult deg}(h_i g_i) \right)$$

By well ordering among all choices of h's $\exists$ a choice s.t $\delta = \max(\text{mult deg}(h_i g_i))$ is the least

$\therefore \quad \text{multdeg}(f) \leq \delta$

if $\text{multdeg}(f) = \delta \Rightarrow LT(g_i) \mid LT(f)$

$\therefore LT(f) \in (LT(g_1), \ldots, LT(g_t))$

Assume $\text{multdeg}(f) < \delta$

$\overline{S(g_i, g_j)}^{G} = c \quad i \neq j$

use this to condict δ being minimal

$$f = \underbrace{\sum_{\text{multdeg}(h_i g_i) = \delta} LT(h_i) g_i}_{= p} + \underbrace{\sum_{\text{multdeg}(h_i g_i) = \delta} (h_i - LT(h_i)) g_i + \sum_{\text{multdeg}(h_i g_i) < \delta} h_i g_i}_{\text{Both have multdeg} < \delta}$$

$p_i = LT(h_i) g_i$

So if $\text{multdeg}(f) < \delta$

$$\text{multdeg}\left(\sum p_i\right) < \delta$$

$\updownarrow$ if both true

remember our lemma $\text{multdeg}(p_i) = \delta$

So we can we write using S-poly

i.e. $p = \sum p_i$ must be a lin combo of $S(p_i, p_j)$

$$S(p_i, p_j) = X^{\delta - \gamma_{ij}} S(g_i, g_j)$$

$\gamma_{ij} = \text{lcm}(LM(g_i), LM(g_j))$ ← check

↑ p is a lin. combo of these

$$S(g_i, g_j) = \sum_{l=1}^{t} A_l g_l \quad \leftarrow \text{Poly.}$$

$$\left(\text{Since } \overline{S(g_i,g_j)}^{G} = 0 \right)$$

$$\text{multdeg}(A_l g_l) \leq \text{multdeg}(S(g_i, g_j))$$

$$x^{\delta - \gamma_{ij}} S(g_i, g_j) = \sum B_l g_l$$

$$\uparrow$$

$$x^{\delta - \gamma_{ij}} A_l$$

$$\text{multdeg}(B_l g_l) \leq \text{multdeg}(x^{\delta-\gamma_{ij}} S(g_i, g_j))$$

$S(g_i, g_j)$: S-poly reduces LT values

in particular

$$LT(S(g_i, g_j)) < \text{lcm}(LM(g_i), LM(g_j))$$

$$= x^{\gamma_{ij}}$$

$$< x^{\gamma_{ij}}$$

$$\text{multdeg}(x^{\delta-\gamma_{ij}} S(g_i, g_j)) < \delta$$

$\therefore$ All terms in $\mathcal{P} < \delta$

this is a contradiction ∎

Ex] $I = (y - x^2, z - x^3)$ is a GB in lex $y > z > x$

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3$$

$\leftarrow$ lcm

$= -z^2 + yx^3$

if we divide $S(y-x^2, z-x^3)$ by $\{y-x^2, z-x^3\}$ we get remainder zero.

Thm: 1 (Buchberger's Algorithm)

Let $I = (f_1, \ldots, f_s) \neq 0$ be a poly. ideal

A Gröbner basis for I can be constructed in a finite number of steps by the following

Input : $F = (f_1, \ldots, f_s)$

Output: a GB $G = (g_1, \ldots, g_t)$ for I, $F \subseteq G$

$G := F$

Repeat :

$G' = G$

For each pair $\{p, q\}$ in G' DO

$r = \overline{S(p,q)}^{G'}$

If $r \neq 0$ Then $G = G \cup \{r\}$

until $G = G'$

Return G

Proof: $I = (G)$ at every step since F is a basis of I and $\overline{S(p,q)}^{G} \in I$

So $G \cup \{r\} \subseteq I$

now note if $G_1 = G'$ $\Rightarrow$ $r = \overline{S(p,q)}^{G} = 0$ $\forall$ pairs $p,q \in G$

$\Rightarrow$ G is $< G$, B.

Show alg. terminates:

$(LT(G')) \subseteq (LT(G))$ since $G' \subseteq G$ ← has r added

If $G' \neq G$ $(LT(G')) \subsetneq (LT(G))$ since

$LT(r) =$ rem of div by G'

is not div by any of $LT(G')$

$\therefore LT(r) \notin (LT(G'))$

The ideals $(LT(G')) \subseteq (LT(G))$

form an ascending chain as alg runs

$\therefore$ They must stabilize at some stage

by ACC ∎

Lemma: Let G be a GB of $I \subseteq K[x_1, \ldots, x_n]$

$p \in G$ s.t $LT(p) \in (LT(G \setminus \{p\}))$ Then

$G \setminus \{p\}$ is also a GB.

minimal GB: GB G where make $LC = 1$ and remove any redundant $p \in G$.

Def A reduced Gröbner basis G of I is

a GB s.t

- $LC(p) = 1 \quad \forall p \in G$
- $\forall p \in G$ no monomial of p lies in $(LT(G \setminus \{p\}))$

This is how M2 checks equality of ideals.

Theorem | Let $I \neq \{0\}$ be a poly ideal. For a fixed monomial order I has a unique reduced Gröbner basis.