Lec 11/16

Friday, November 16, 2018 11:31

$R = K[x_1, \dots, x_n]$. $\quad x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \quad \alpha \in \underset{\text{includes } 0.}{\mathbb{N}}^n$.

fix $\leq$ total ordering on $\{x^\alpha : \alpha \in \mathbb{N}^n\}$ s.t. $x^\alpha \leq x^\beta \Rightarrow x^{\alpha+\gamma} \leq x^{\beta+\gamma} \quad \forall \gamma \in \mathbb{N}^n$.

$LT\left(\sum_\alpha^{\text{finite}} c(\alpha) x^\alpha\right) = c(\alpha_0) x^{\alpha_0}$ where $c(\alpha_0) \neq 0$ & if $c(\alpha) \neq 0$ then $x^\alpha \leq x^{\alpha_0}$

Multivariable division algorithm:

<u>Input</u>: $g_1, \dots, g_m, f \in R$

<u>output</u>: $r \in R$ s.t.

$f \equiv r \mod (g_1, \dots, g_m)$

and monomials in r are not divisible by any $LT(g_i)$

If we are given $f_1, \dots, f_s$ and asked if $f \in I = (f_1, \dots, f_s)$.

If $\{f_1, \dots, f_s\}$ is a gröbner basis then let r be the output of the MDA & we proved yesterday that $f \in I \Leftrightarrow r = 0$.

Recall: $\{g_1, \dots, g_m\} \subset I$ is a gröbner basis of I if

$$\left(LT(g_1), \dots, LT(g_m)\right) = LT(I).$$

Application: Solve simultaneous polynomial eq^{n}s.

Yesterday we saw that $\forall\, I \subset R$, a gröbner basis exists.
(uses Hilbert Basis Theorem)

Q: Given $g_1, \ldots, g_m \in I$, how to tell if $\{g_1, \ldots, g_m\}$ is a Gröbner Basis?

Buchberger's Criterion:

<u>Notation</u>: • $f \equiv r \mod G^{=\{g_1, \ldots, g_m\}}$ means r is output from MDA.

• $f_1, f_2 \in R$. $LT(f_1) = c_1 x^\alpha$, $LT(f_2) = c_2 x^\beta$

$$M = x_1^{\max\{\alpha_1, \beta_1\}} \cdots x_n^{\max\{\alpha_n, \beta_n\}}.$$

$$S(f_1, f_2) = \frac{M}{LT(f_1)} \cdot f_1 - \frac{M}{LT(f_2)} \cdot f_2$$

<u>Theorem</u>: $\{g_1, \ldots, g_m\}$ is a Gröbner basis of $(g_1, \ldots, g_m)$ iff $S(g_i, g_j) \equiv 0 \mod G$ $\forall i \neq j$

<u>Ex.</u> $f_1 = x^3y - xy^2 + 1$
$f_2 = x^2y^2 - y^3 - 1$ $\in \mathbb{Q}[x, y]$. $\leq$ = lex $(x > y)$.

$I = (f_1, f_2)$

$M = x^3y^2$. $S(f_1, f_2) = y \cdot f_1 - x \cdot f_2 = x + y \not\equiv 0 \mod \{f_1, f_2\}$.

$\Rightarrow$ $\{f_1, f_2\}$ is <u>not</u> a gröbner basis.

Continue: Let $f_3 = x + y$, so $G_2 = \{f_1, f_2, f_3\}$.

Still $(f_1, f_2, f_3) = (f_1, f_2)$. Now:

$S(f_2, f_3) = f_2 - xy^2 f_3 = -xy^3 - y^3 - 1 \equiv y^4 - y^3 - 1 \pmod{G_2}$.

Still not a Gröbner basis.

Continue: Let $f_4 = y^4 - y^3 - 1$. $G_3 = \{f_1, f_2, f_3, f_4\}$.

Exercise (for laptop): G_3 is a Gröbner basis since $S(f_i, f_j) \equiv 0 \mod G \quad \forall\, i \neq j$.

Also $\{x+y,\ y^4 - y^3 - 1\}$ is a G-B for (f_1, f_2).

since $x^3y,\ x^2y^2 \in (x)$

Buchberger's algorithm:

Input: $f_1, \dots, f_s \in K[x_1, \dots, x_n]$

Output: $G = \{g_1, \dots, g_m\} \supseteq \{f_1, \dots, f_s\}$, a G-B for $(f_1, \dots, f_s)$.

<u>Procedure:</u> initially $G = \{f_1, \dots, f_s\}$, $G_{temp} = \emptyset$.

while $G \neq G_{temp}$:

$G_{temp} = G$.

for $p \neq q \in G$:

$r \equiv S(p,q) \mod G_{temp}$

if $r \neq 0$, $G \mapsto G \cup \{r\}$

return G.

If $G = \{g_1, \dots, g_m\}$ is a G-B for a non-zero ideal $I \subset K[x_1, \dots, x_n]$ w.r.t. $\leq$ = lexicographic order generated by $x_i < x_j \Leftrightarrow i > j$.

then $G \cap K[x_i, x_{i+1}, \dots, x_n]$ is a G-B for $I \cap K[x_i, x_{i+1}, \dots, x_n]$ $\forall\, i = 1, \dots, n$.

eg
$$\begin{aligned} x^3y - xy^2 - 1 &= 0 \\ x^2y^2 - y^3 + 1 &= 0 \end{aligned} \quad \longleftrightarrow \quad \begin{aligned} x + y &= 0 \\ y^4 - y^3 - 1 &= 0 \end{aligned}$$
in $\mathbb{C}[x,y]$.

4 solns over $\mathbb{C}$.

1 soln over $\mathbb{C}$.

eg find all points $(x,y) \in \mathbb{R}^2$ s.t. $2x^2 + 2xy + y^2 - 2x - 2y = 0$ & $x^2 + y^2 = 1$.

G. B algorithm gives :

$$g_1 = 2x + 5y^3 + y^2 - 2 = 0$$

$$g_2 = 5y^4 - 4y^3 = 0 \Rightarrow \underset{\uparrow}{\overset{x=1}{y=0}} \text{ or } \underset{\uparrow}{\overset{x=\frac{3}{4}}{y=\frac{4}{5}}}$$