Shun/翔海 (@shun4midx)

GRÖBNER BASIS (II)

THEOREM 1

The Buchburger's algorithm will terminate

<u>Proof</u>

- $\langle LT(G_i)\rangle \subsetneq \langle LT(G_{i+1})\rangle$ if $G_i \neq G_{i+1}$:
  $G_i \neq G_{i+1} \Rightarrow \exists f, g \in G_i$, s.t. $\overline{S(f,g)}^{G} \neq 0 \Rightarrow \overset{\in \langle LT(G_{i+1})\rangle}{LT(\overline{S(f,g)}^{G_i})} \notin \langle LT(G_i)\rangle$
- If this algorithm doesn't terminate, then $\exists \langle LT(G_0)\rangle \subsetneq \langle LT(G_1)\rangle \subsetneq \dots$
  This contradicts the Noetherian property of $F[x_1,\dots,x_n]$ $\rightarrow\!\times\!\leftarrow$

DEFINITION

A Gröbner basis $G=\{g_1,\dots,g_m\}$ of I is said to be **minimal** if each $LT(g_i)$ is monic $\forall i$, and $\forall j$, $LT(g_j) \notin \langle LT(G\setminus\{g_j\})\rangle$

(If $LT(g_j) \in \langle LT(G\setminus\{g_j\})\rangle$, then $\langle LT(G\setminus\{g_j\})\rangle = \langle LT(G)\rangle = LT(I)$, i.e. $G\setminus\{g_j\}$ is still a Gröbner basis of I)

DEFINITION

A minimal Gröbner basis $\{g_1,\dots,g_m\}$ is said to be **reduced** if $\forall j$, no term in g_j is divisible by any $LT(g_1),\dots,\widehat{LT(g_j)},\dots,LT(g_m)$

In this case, g_j is said to be reduced for G

THEOREM 2

For a given monomial ordering, every non-zero ideal I in $F[x_1,\dots,x_n]$ has a unique reduced Gröbner basis

$\Rightarrow$ Corollary: $I, J \subseteq F[x_1,\dots,x_n]$, $I=J \Leftrightarrow I$ and J have the same reduced Gröbner basis)

<u>Proof</u>

Existence: Let G be a minimal Gröbner basis of I.

For $g\in G$, let $g' = \overline{g}^{G\setminus\{g\}}$ and set $G' = (G\setminus\{g\}) \cup \{g'\}$

Claim: G' is still a Gröbner basis of I

<u>Proof</u>

Observe that when we divide g by $G\setminus\{g\}$, $LT(g)$ goes to the remainder since $LT(g)\notin \langle LT(G\setminus\{g\})\rangle$

This implies that $LT(g') = LT(g) \Rightarrow \langle LT(G')\rangle = \langle LT(G)\rangle = LT(I)$ and G' is still a minimal Gröbner basis

Now, take other elements of G and apply the same process until they are all reduced

Uniqueness: Let G and $\tilde{G}$ be two reduced Gröbner bases of I. In particular, G and $\tilde{G}$ are minimal

Claim: $LT(G) = LT(\tilde{G})$ and thus G and $\tilde{G}$ have the same number of elements

<u>Proof</u>

$\forall LT(g) \in LT(G) \subseteq LT(I) = \langle LT(\tilde{G})\rangle$, say $LT(g) = \sum_{\tilde{g}\in\tilde{G}} h_{\tilde{g}} LT(\tilde{g}) \Rightarrow LT(\tilde{g}) \mid LT(g)$ for some $\tilde{g}\in\tilde{G}$

Similarly, $\exists g' \in G$, s.t. $LT(g') \mid LT(\tilde{g}) \Rightarrow LT(g') \mid LT(g) \Rightarrow LT(g') = LT(g) \Rightarrow LT(g) = LT(\tilde{g})$ since G is minimal.

We conclude that $\forall g\in G, \exists \tilde{g}\in\tilde{G}$ s.t. $LT(g) = LT(\tilde{g})$. By symmetry, $\forall \tilde{g}\in G, \exists g\in G$, s.t. $LT(\tilde{g}) = LT(g)$ $\square$

For $g\in G$, let $\tilde{g}\in\tilde{G}$, s.t. $LT(g) = LT(\tilde{g})$. $\because g-\tilde{g}\in I$ $\therefore \overline{g-\tilde{g}}^{G} = 0$

But $LT(g)$, $LT(\tilde{g})$ cancel in $g-\tilde{g}$ and the remaining terms are divisible by none of $LT(G) = LT(\tilde{G})$ since $G, \tilde{G}$ are reduced.

This shows that $\overline{g-\tilde{g}}^{G} = g-\tilde{g} = 0 \Rightarrow g = \tilde{g}$ $\square$

Shun/羊羽海(@shun4midx)

EXAMPLE 1

Let $I=\langle f_1=x^2+xy^5+y^4,\ f_2=xy^6-xy^3+y^5-y^2,\ f_3=xy^5-xy^2\rangle$, $x>y$

$\overline{S(f_1,f_2)}^{G_0}=0$

$\overline{S(f_1,f_3)}^{G_0}=0$

$\overline{S(f_2,f_3)}^{G_0}=y^5-y^2=f_4$

$G_1=\{f_1,f_2,f_3,f_4\}$

$\overline{S(f_3,f_4)}^{G_1}=0$, $\overline{S(f_2,f_4)}^{G_1}=0$, $\overline{S(f_1,f_4)}^{G_1}=0$

$\Rightarrow G=\{x^2+xy^5+y^4,\ \cancel{xy^6-xy^3+y^5-y^2},\ \cancel{xy^5-xy^2},\ y^5-y^2\}$

$\Rightarrow$ Reduced $=\{x^2+xy^5+y^4,\ y^5-y^2\}$

APPLICATIONS

QUESTIONS

Suppose $S=\{f_1,\dots,f_m\}\subseteq F[x_1,\dots,x_n]$. Let $Z(S)=\{(a_1,\dots,a_n)\mid f_i(a_1,\dots,a_n)=0\ \forall i=1,\dots,m\}$ be the zero locus of S. How do we find $Z(S)$? How do we solve $\{f_1=0,\dots,$ and $f_m=0\}$?

FACT

Let $I=\langle S\rangle$. Then, $Z(I)=Z(S)$

Proof

$\because S\subseteq I$ $\therefore$ of course $Z(I)\subseteq Z(S)$ ✓

Conversely, $\forall f\in I$, write $f=\sum_{i=1}^m h_i g_i$, $g_i\in S$, $h_j\in F[x_1,\dots,x_n]$

For any $(a_1,\dots,a_n)\in Z(S)$, $g_i(a_1,\dots,a_n)=0\ \forall i\Rightarrow f(a_1,\dots,a_n)=0$. □

DEFINITION

Let I be an ideal of $F[x_1,\dots,x_n]$.

$I_i:=I\cap F[x_{i+1},\dots,x_n]$ is called the i^{th} elimination ideal of I w.r.t. $x_1>x_2>\dots>x_n$.

$\cap$

$F[x_{i+1},\dots,x_n]$

ELIMINATION THEOREM

Let $G=\{g_1,\dots,g_m\}$ be a Gröbner basis for $I\neq 0$ w.r.t. $x_1>x_2>\dots$

Then, $G_i:=G\cap F[x_{i+1},\dots,x_n]$ is a Gröbner basis of I_i in $F[x_{i+1},\dots,x_n]$

In particular, $I_i=\{0\}\Leftrightarrow G\cap F[x_{i+1},\dots,x_n]=\emptyset$

Proof

By def, $\langle LT(G_i)\rangle\subseteq LT(I_i)$

a_{k_j} is a multiset

Conversely, let $f\in I_i\subseteq I$, write $F[x_{i+1},\dots,x_n]\ni LT(f)=\sum_{i=1}^m h_i LT(g_i)=\sum a_{k_j}\underbrace{X^{\alpha_{k_j}}LT(g_k)}_{LT(f)}$

So, $a_{k_j}\neq 0\Rightarrow LT(g_k)\in F[x_{i+1},\dots,x_n]\Rightarrow g_k\in F[x_{i+1},\dots,x_n]$ since $x_1>x_2>\dots>x_n>x_{n+1}$

$\Rightarrow g_k\in G_i$

Hence, $LT(f)\in\langle LT(G_i)\rangle$

In conclusion, $G=G_0\cup G_1\cup\dots\cup G_{n-1}$

Shun/羊羽海(@shun4midx)

THEOREM 3

Let I, J be ideals of $F[x_1, \dots, x_n]$. Then,

(1) $\underbrace{tI}_{F[t, x_1, \dots, x_n]I} + (1-t)J$ is an ideal of $F = [t, x_1, \dots, x_n]$

(2) $I \cap J = (tI + (1-t)J) \cap F[x_1, \dots, x_n]$ which is the first elimination ideal of $tI + (1-t)J$ w.r.t. $t > x_1 > x_2 > \dots$ (Notice that t is first)

Proof

(1) OK

(2) "$\subseteq$": For $f \in I \cap J$, $f = t\overset{\in I}{f} + (1-t)\overset{\in J}{f} \in RHS$ ✓

"$\supseteq$": For $f \in RHS$, say $f = t\tilde{f}_1 + (1-t)\tilde{f}_2$, $\tilde{f}_1 \in F[t, x_1, \dots, x_n]I$, $\tilde{f}_2 \in F[t, x_1, \dots, x_n]J$, say: $\tilde{f}_1 = \sum (\underbrace{h_i}_{F[t, x_1, \dots, x_n]} t + \underbrace{r_i}_{\in F[x_1, \dots, x_n]}) \underbrace{f_i}_{\in I}$ and $\tilde{f}_2 = \sum (h_j' t + r_j') \underbrace{f_j'}_{\in J}$

Note: f has no variable t

Take $t = 0$, $f = \sum r_j' f_j' \in J$

$t = 1$, $f = \sum (h_i(1, x_1, \dots, x_n) + r_i) f_i \in I$

$\therefore f \in I \cap J$ ✓

EXAMPLE 2

$I = \langle y^2, x - yz \rangle$, $J = \langle x, z \rangle$

$tI + (1-t)J = \langle \underbrace{ty^2}_{f_1}, \underbrace{tx - tyz}_{f_2}, \underbrace{x - tx}_{-f_3}, \underbrace{z - tz}_{-f_4} \rangle$ ∵ we need "monic"

$G_0 = \{f_1, f_2, f_3, f_4\}$

$\overline{S(f_1, f_2)}^{G_0} = 0$

$\overline{S(f_1, f_3)}^{G_0} = xy^2 = f_5$

$\overline{S(f_1, f_4)}^{G_0} = y^2 z = f_7$

$\overline{S(f_2, f_3)}^{G_0} = x - yz = f_6$

$G_1 = \{f_1, \dots, f_7\}$

$\Rightarrow \overline{S(f_i, f_j)}^{G_1} = 0 \quad \forall i, j$

$\therefore I \cap J = \langle xy^2, y^2 z, x - yz \rangle$