3-14-25 (WEEK 4)

Shun/翔海 (@shun4midx)

GRÖBNER BASIS (I) (Sorry for the late upload... Hope the longer length makes up for it. 本当にごめん...)

DEFINITION

Let R be a commutative ring. R is a Noetherian ring if every ideal of R is finitely generated

FACT

Let R be commutative. TFAE

(1) Each ideal of R is finitely generated

(2) ACC on ideals of R, i.e. $I_1 \subseteq I_2 \subseteq \dots \Rightarrow \exists k$, s.t. $I_k = I_{k+1} = \dots$

(3) Maximal condition on ideals: S is a nonempty set of ideals of $R \Rightarrow \exists$ maximum element of S.

Proof

$(1) \Rightarrow (2)$: Let $I = \bigcup_{i=1}^{\infty} I_i$, which is an ideal of R, say $I = \langle a_1, \dots, a_n \rangle$ and $a_i \in I_{k_i}$

If $k := \max\{k_i \mid i = 1, \dots, n\}$, then $a_i \in I_k \ \forall i = 1, \dots, n$, i.e. $I \subseteq I_k \subseteq I_{k+1} \subseteq \dots \subseteq I \Rightarrow I = I_k = I_{k+1} = \dots$

$(2) \Rightarrow (1)$: Let I be an ideal of R. Assume I is not finitely generated. Take $a_1 \in I$

Since $I \neq \langle a_1 \rangle$, $\exists a_2 \in I \setminus \langle a_1 \rangle$. Since $I \neq \langle a_1, a_2 \rangle$, then $\exists a_3 \in I \setminus \langle a_1, a_2 \rangle, \dots$

$\therefore \langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \langle a_1, a_2, a_3 \rangle \subsetneq \dots \to \times$ (b/c not ACC)

$(2) \Rightarrow (3)$: Assume $\nexists$ max element in S.

Take $I_1 \in S$. Since I_1 is not max, $\exists I_2 \in S$, s.t. $I_1 \subsetneq I_2$. Since I_2 is not max, $\exists I_3$, s.t. $I_2 \subsetneq I_3 \dots$

$\therefore \exists I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots \times$

$(3) \Rightarrow (2)$: Let $S = \{I_1, I_2, \dots\}$

By assumption, $\exists$ max I_k in S.

$\therefore I_k \supseteq I_{k+1}, I_k \supseteq I_{k+2}, \dots$. Thus, $I_k = I_{k+1} = I_{k+2} = \dots$ □

HILBERT BASIS THEOREM

If R is Noetherian, then $R[x_1, \dots, x_n]$ is also Noetherian

Proof

Assume that $\exists I \subsetneq R[x_1, \dots, x_n]$ that is not finitely generated

Choose $f_1 \in I$, s.t. f_1 is least degree in I.

$\Rightarrow \exists f_2 \in I$, s.t. f_2 is least degree in $I \setminus \langle f_1 \rangle$

$\vdots$

Let $\deg f_i = n_i$ and the leading term of f_i be a_i.

$\Rightarrow n_1 \leq n_2 \leq n_3 \leq \dots$

Claim: $\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \langle a_1, a_2, a_3 \rangle \subsetneq \dots$ does not satisfy ACC

Proof

If $\exists k$, s.t. $\langle a_1, \dots, a_k \rangle = \langle a_1, \dots, a_k, a_{k+1} \rangle$, then $a_{k+1} = \sum_{i=1}^{k} r_i a_i$

Hence, $f_{k+1} - \sum_{i=1}^{k} r_i x^{n_{k+1} - n_i} f_i < \deg f_{k+1}$

However, $\underbrace{f_{k+1} - \sum_{i=1}^{k} r_i x^{n_{k+1} - n_i} f_i \in I \setminus \langle f_1, \dots, f_k \rangle}_{\text{compare degrees}} \to \times$

QUESTION

Given $f \in F[x_1, \dots, x_n]$, $I \subseteq F[x_1, \dots, x_n]$, how to check if $f \in I$?

- Let $I = \langle f_1, \dots, f_s \rangle$. If $f = \sum_{i=1}^{s} h_i f_i + r$ with remainder r, then $r = 0 \overset{?}{\iff} r = I$

EXAMPLE 1

$f_1 = xy + 1$, $f_2 = y^2 - 1$, $I = \langle f_1, f_2 \rangle$, $f = xy^2 - x = x f_2 \in I$, but $f = y f_1 - (x + y)$

DIVISION ALGORITHM IN $F[x_1, \dots, x_n]$

Shun/羊羽海 (@shun4midx)

EXAMPLE 2

Say $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1$

1. Choose a lexicographical ordering: $x > y$
2. The multidegree: $\partial(f) = (2,1)$, $\partial(f_1) = (1,1)$, $\partial(f_2) = (0,2)$
3. The leading term: $LT(f) = x^2y$, $LT(f_1) = xy$, $LT(f_2) = y^2$
4. $LT(f) = x\,LT(f_1)$: $f = xf_1 + xy^2 + y^2 + x = xf_1 + yf_1 + y^2 + x + y = xf_1 + yf_1 + f_2 + (x+y+1)$

   No term in $x+y+1$ is divisible by $LT(f_1), LT(f_2)$. $\Rightarrow$ Stop

   However, this division is not unique. In fact, $f = xf_1 + (x+1)f_2 + (x+1)$

SUMMARY OF THE ALGORITHM

Fix a monomial ordering and $I = \langle f_1, \dots, f_m \rangle$

Then $\forall f \in F[x_1, \dots, x_n]$, $f = \underbrace{\sum_{i=1}^{m} h_i f_i}_{f_I} + \underbrace{r}_{f^G,\ G = \{f_1, \dots, f_m\}}$, where $h_i, r \in F[x_1, \dots, x_n]$ $\forall i$ and either $r = 0$ or no term of r is divisible by any $LT(f_1), \dots, LT(f_m)$ — Denote by NTOR

GRÖBNER BASIS

DEFINITION

Fix a monomial ordering (Denote by FAMO) and let $I \subseteq F[x_1, \dots, x_n]$. We say $LT(I) = \langle LT(f) \mid f \in I \rangle$

REMARK

Let $I = \langle f_1, \dots, f_m \rangle$. In general, $\langle LT(f_1), \dots, LT(f_m) \rangle \subsetneq LT(I)$

For example, $f_1 = xy^2 + y$, $f_2 = x^2y$. $xf_1 - yf_2 = xy \in \langle f_1, f_2 \rangle$ but $xy \notin \langle xy^2, x^2y \rangle$.

DEFINITION

$\{g_1, \dots, g_m\}$ is called a Gröbner basis for I if $\langle g_1, \dots, g_m \rangle = I$ and $\langle LT(g_1), \dots, LT(g_m) \rangle = LT(I)$

PROPOSITION 1

$LT(I) = \langle LT(g_1), \dots, LT(g_m) \rangle \Rightarrow I = \langle g_1, \dots, g_m \rangle$

Proof

$\forall f \in I$, $f = \sum_{i=1}^{m} h_i f_i + r$, either $r = 0$ or NTOR.

Assume that $r \neq 0$. Since $r = f - f_I \in I$, thus $LT(r) \in LT(I) = \langle LT(g_1), \dots, LT(g_m) \rangle$

Then, $LT(r) = \tilde{h}_1 LT(g_1) + \dots + \tilde{h}_m LT(g_m)$, so not NTOR. $\times$

$\therefore r = 0$, i.e. $f \in \langle g_1, \dots, g_m \rangle$ $\square$

PROPOSITION 2

Each ideal I has a Gröbner basis

Proof

By Hilbert basis theorem, $LT(I)$ is finitely generated, say $LT(I) = \langle f_1, \dots, f_m \rangle$

Write $f_i = \sum_{j=1}^{m_i} h_{ij} LT(g_{ij})$ with $g_{ij} \in I$ and $h_{ij} \in F[x_1, \dots, x_n]$ $\Rightarrow$ $LT(I) = \langle LT(g_{ij}) \mid_{j=1,\dots,m_i}^{i=1,\dots,m} \rangle$

$\therefore \{g_{11}, \dots, g_{mm_m}\}$ is a Gröbner basis of I. $\square$

Shun/翔海(@shun4midx)

PROPOSITION 3

Assume that $\{g_1, \dots, g_m\}$ is a Gröbner basis of I.

- $\forall f \in F[x_1, \dots, x_n]$, $\exists! f_I \in I$, r s.t. $f = f_I + r$, $r = 0$ or NTOR
- $f \in I \Leftrightarrow r = 0$

Proof

- By division algorithm, $f = f_I + r$.
  Now, if $f_I + r = f_I' + r'$, then $r - r' = f_I' - f_I \in I$
  Also, if $r - r' \neq 0$, then $LT(r-r') \in LT(I) = \langle LT(g_1), \dots, LT(g_m) \rangle$ $\rightarrow$ ✗
  $\therefore$ $r - r' = 0 \Rightarrow f_I = f_I'$ ✓
- If $f \in I$, then $f = f_I + r \Rightarrow r = f - f_I \in I \Rightarrow r = 0$ □

HOW DO WE CONSTRUCT A GRÖBNER BASIS?

DEFINITION

Let $f, g \in F[x_1, \dots, x_m]$ and M be the monic least common multiple of $LT(f)$ and $LT(g)$. Then, $S(f,g) = \frac{M}{LT(f)} f - \frac{M}{LT(g)} g$ is called an S-polynomial of f, g.

BUCHBURGER'S ALGORITHM

Let $I = \langle g_1, \dots, g_m \rangle$ and $G = \langle g_1, \dots, g_m \rangle$

A Gröbner basis can be constructed by the algorithm:

↳ $G_0 := G$

↳ $G_{i+1} := G_i \cup (\{ \overline{S(f,g)}^{G_i} \mid f, g \in G_i \} \setminus \{0\})$

If $G_i = G_{i+1}$, then G_i is a Gröbner basis

EXAMPLE 4

Let $x > y$ and $I = \langle f_1 = x^3y - xy^2 + 1, f_2 = x^2y^2 - y^3 - 1 \rangle$, $G_0 = \{f_1, f_2\}$, $S(f_1, f_2) = x + y =: f_3$, $G_1 = \{f_1, f_2, f_3\}$

$\overline{S(f_1, f_3)}^{G_1} = 0$, $\overline{S(f_2, f_3)}^{G_1} = y^4 - y^3 - 1 = f_4 \Rightarrow G_2 = \{f_1, f_2, f_3, f_4\}$

$\overline{S(f_1, f_4)}^{G_2} = \overline{S(f_2, f_4)}^{G_2} = \overline{S(f_3, f_4)}^{G_2} = 0$

$\therefore$ G_2 is a Gröbner basis

KEY LEMMA

Let $f_1, \dots, f_m \in F[x_1, \dots, x_m]$ and $a_1, \dots, a_m \in F$, s.t. $\partial(f_1) = \partial(f_2) = \dots = \partial(f_m) = \alpha$ and $\partial(\underbrace{\sum_{i=1}^m a_i f_i}_{=:h}) < \alpha$. Then, $h = \sum_{i=2}^m b_i S(f_{i-1}, f_i)$

Proof

Write $f_i := c_i f_i'$ with $c_i \in F$ and f_i' be monic with multidegree α. (Note: $S(f_1, f_2) = \frac{1}{c_1} f_1 - \frac{1}{c_2} f_2 = f_1' - f_2'$)

Then, $h = \sum_{i=1}^m a_i c_i f_i' = a_1c_1(f_1' - f_2') + (a_1c_1 + a_2c_2)(f_2' - f_3') + \dots + (a_1c_1 + \dots + a_{m-1}c_{m-1})(f_{m-1}' - f_m') + \underbrace{\cancel{(a_1c_1 + \dots + a_mc_m)f_m'}}_{0\ (\because \text{degree})}$ □

BUCHBURGER'S CRITERION

Assume that $I = \langle g_1, \dots, g_m \rangle$

Then, $G = \{g_1, \dots, g_m\}$ is a Gröbner basis of $I \Leftrightarrow \underbrace{\overline{S(g_i, g_j)}^G = 0}_{S(g_i, g_j) \equiv 0 \pmod G}$ $\forall i, j$

Proof

"$\Rightarrow$": Since $S(g_i, g_j) \in I$, by prop 3, $\overline{S(g_i, g_j)}^G = 0$

"$\Leftarrow$": For $f \in I$, write $f = \sum_{i=1}^m h_i g_i$. Define $\alpha = \max\{\partial(h_1g_1), \dots, \partial(h_mg_m)\}$

We have $\partial(f) \leq \alpha$, so we can select an expression $f = \sum_{i=1}^m h_i g_i$ for f s.t. α is minimal

Claim: $\partial(f) = \alpha$ ($\Rightarrow LT(f) = \sum_{\partial(h_ig_i) = \alpha} LT(h_i) LT(g_i) \Rightarrow LT(f) \in \langle LT(g_1), \dots, LT(g_m) \rangle$)

Proof

Assume that $\partial(f) < \alpha$

Shun/翔海(@shun4midx)

Rewrite $f=\sum_{i=1}^{m} h_i g_i = \underline{\sum_{\partial(h_i g_i)=\alpha} LT(h_i) g_i} + \sum_{\partial(h_i g_i)} (h_i - LT(h_i)) g_i + \sum_{\partial(h_i g_i)<\alpha} h_i g_i$

Let $LT(h_i) = a_i h_i^\circ$ with h_i° being a monic monomial.
Comparing the multidegree on both sides, we get $\partial\left(\sum_{\partial(h_i g_i)=\alpha} a_i h_i^\circ g_i\right) < \alpha$

By key lemma, $\sum_{\partial(h_i g_i)=\alpha} a_i h_i^\circ g_i = c_{12} S(h_{i_1}^\circ g_{i_1}, h_{i_2}^\circ g_{i_2}) + c_{23} S(h_{i_2}^\circ g_{i_2}, h_{i_3}^\circ g_{i_3}) + \underbrace{\cdots}_{\text{finite}}$, where $\partial(h_{i_1} g_{i_1}) = \partial(h_{i_2} g_{i_2}) = \underbrace{\cdots}_{\text{finite}} = \alpha$

By def, if we set $M_{st} = x^{\beta_{st}}$ = the monic lcm of $LT(g_{i_s}), LT(g_{i_t})$ where the multidegree is β_{st}
Then, $S(h_{i_s}^\circ g_{i_s}, h_{i_t}^\circ g_{i_t}) = \frac{x^\alpha}{LT(h_{i_s}^\circ g_{i_s})} h_{i_s}^\circ g_{i_s} - \frac{x^\alpha}{LT(h_{i_t}^\circ g_{i_t})} h_{i_t}^\circ g_{i_t}$

$$= x^{\alpha-\beta_{st}} \left(\frac{x^{\beta_{st}}}{\cancel{h_{i_s}^\circ} LT(g_{i_s})} \cancel{h_{i_s}^\circ} g_{i_s} - \frac{x^{\beta_{st}}}{\cancel{h_{i_t}^\circ} LT(g_{i_t})} \cancel{h_{i_t}^\circ} g_{i_t} \right)$$

$$= x^{\alpha-\beta_{st}} S(g_{i_s}, g_{i_t})$$

Do division on $g_1, \dots, g_m k$, since $\overline{S(g_{i_s}, g_{i_{s+1}})}^G = 0$

By assumption, $\forall$ fixed s, $S(g_{i_s}, g_{i_{s+1}}) = \sum_{j=1}^{m} l_j g_j$ with $\partial(l_j g_j) < \beta_{s(s+1)}$, i.e. $\partial(S(g_{i_s}, g_{i_{s+1}})) < \beta_{s(s+1)}$
$\therefore$ We found $\partial(x^{\alpha-\beta_{s(s+1)}} l_j g_j) < \alpha$ $\forall j$, which contradicts the minimality of α $\times$ $\square$