The Hilbert basis theorem

November 6, 2023 8:58 PM

Assignment #5 due Monday @ 11pm

Course Project posted. Due 11pm Friday Dec 15th.

CLO 2.5 The Hilbert Basis Theorem and Grobner Basis.

Let I be an ideal in $k[x_1,\dots,x_n]$.
If $I = \langle f_1,\dots,f_s\rangle$ we say $\{f_1,\dots,f_s\}$ is a basis for I.

Does every ideal in $k[x_1,\dots,x_n]$ have a finite basis?

Def 1. Suppose $I \neq \{0\}$ and $>$ is a monomial ordering on $\mathbb{Z}^n_{\geq 0}$.
Then $>$ defines $LT(f)$ for $f \in I$.
Define $\langle LT(I)\rangle = \langle LT(f) : f \in I\rangle$.
($\langle LT(I)\rangle$: the leading term ideal; $\langle LT(f) : f\in I\rangle$: monomial ideal).

Let $I = \langle f_1,\dots,f_s\rangle$. Then $LT(f_i) \in \langle LT(I)\rangle$ as $f_i \in I$.

$\Rightarrow \langle LT(f_1),\dots,LT(f_s)\rangle \subset \langle LT(I)\rangle$.

Ex 2. $I = \langle \underbrace{x^2+y^2-3}_{f_1}, \underbrace{x^2-y^2-1}_{f_2}\rangle$. Using $>_{lex}$ with $x>y$;
we have $\langle LT(f_1), LT(f_2)\rangle = \langle x^2, x^2\rangle = \langle x^2\rangle$.

But. $\underset{\in I}{f_3} = \underset{\in I}{f_1} - \underset{\in I}{f_2} = 2y^2-2 \in I \Rightarrow 2y^2 \in \langle LT(I)\rangle$.

Hence $\langle x^2\rangle \subsetneq \langle LT(I)\rangle$ as $2y^2 \notin \langle x^2\rangle$.

Prop 3. Let I be an ideal in $k[x_1,\dots,x_n]$, $I \neq \{0\}$. Then

(i) $\langle LT(I)\rangle$ is a monomial ideal

(ii) $\exists g_1,\dots,g_t \in I$ s.t. $\langle LT(I)\rangle = \langle LT(g_1),\dots,LT(g_t)\rangle$
t is finite.

Proof (i) $\langle LT(I)\rangle = \langle LT(f) : f \in I\rangle$ by def.

$\langle \underset{f_1}{3xy}, \underset{f_2}{5z^2}\rangle$ $= \langle LM(f) : f\in I\rangle$

Vue $\downarrow$ (i) $= \langle LM(f) : f \in I\setminus\{0\}\rangle$.

$\langle xy, z^2\rangle$ a monomial ideal.

(ii) Dickson's Lemma $\Rightarrow \exists g_1, \dots, g_t \in I$ s.t.

$$\langle LT(I) \rangle = \langle LM(g_1), \dots, LM(g_t) \rangle$$

$$\overset{\text{via (i)}}{=} \langle LT(g_1), \dots, LT(g_t) \rangle.$$

Theorem 4 (Hilbert Basis Theorem).

Every ideal $I \subset k[x_1, \dots, x_n]$ has a finite basis, i.e,

$\exists g_1, \dots, g_t \in I$ s.t. $I = \langle g_1, \dots, g_t \rangle$.

Proof. Let $>$ be a monomial ordering on $\mathbb{Z}^n_{\geq 0}$.

Let $LT(f)$ be the leading term of f w.r.t. $>$.

Case $I = \{0\}$. Then $I = \langle 0 \rangle$.

Case $I \neq \{0\}$. By Prop 3 $\exists g_1, \dots, g_s \in I$ s.t.

$$\langle LT(I) \rangle = \langle LT(g_i) : 1 \leq i \leq s \rangle.$$

Claim $I = \langle g_1, \dots, g_s \rangle = G$.

($\supset$) $g_i \in I \Rightarrow \langle g_1, \dots, g_s \rangle \subset I$.

($\subset$) Let $f \in I$. Dividing $f \div \{g_1, \dots, g_s\}$ yields.

$$I \ni f = a_1 \underset{\overset{\Uparrow}{I}}{g_1} + \dots + a_s \underset{\overset{\Uparrow}{I}}{g_s} + r \Rightarrow r \in I.$$

Suppose $r \neq 0$. $LT(r)$ is not divisibly by any $LT(g_i)$.

$r \in I \Rightarrow LT(r) \in \langle LT(I) \rangle \overset{\text{Prop 3.}}{=} \langle LT(g_1), \dots, LT(g_s) \rangle$.

$\Rightarrow LT(r) \in \langle LM(g_1), \dots, LM(g_s) \rangle$

Lemma 2 § 2.4 $\Rightarrow \exists i$ s.t. $LM(g_i) \mid LT(r)$ a contradiction.

Thus $r = 0 \Rightarrow f = a_1 g_1 + \dots + a_s g_s \in I$ $\square$.

Def 5. A finite set $G = \{g_1, \dots, g_t\} \subset I \setminus \{0\}$ in $k[x_1, \dots, x_n]$ is a Gröbner basis for I if $\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$.

Cor 6. Every ideal $I \subset k[x_1, \dots, x_n]$ other than $\{0\}$ has a Gröbner basis and every Gröbner basis for I is a basis for I.

Proof. The set $\{g_1, \dots, g_s\}$ in the proof of the H.B.T. satisfies $\langle LT(g_1), \dots, LT(g_s) \rangle = \langle LT(I) \rangle$ hence I has a Gröbner basis. Moreover the Claim proved $I = \langle g_1, \dots, g_t \rangle$.

Ex 2 $\{f_1 = x^2+y^2-3, f_2 = x^2-y^2-1\}$ is not a GB for $>_{lex}$ with $x > y$.
$I = \langle f_1, f_2 \rangle$ since $f_3 = f_1 - f_2 = 2y^2 - 2 \in I$ but $LT(f_3) = 2y^2 \notin \langle LT(f_1), LT(f_2) \rangle$.

CLO 2.6 Properties of Gröbner bases.

Prop 1. Let $G = \{g_1, \dots, g_t\}$ be a Gröbner basis for the ideal $I \subset k[x_1, \dots, x_n]$ w.r.t. the monomial ordering $>$.
Let $f \in k[x_1, \dots, x_n]$.
The remainder of $f \div G$ using the $\div$ from 2.3 is unique and satisfies

(i) $r = 0$ or no term of r is divisible by $LT(g_i)$ for all $1 \le i \le t$,

(ii) $\exists\, g \in I$ s.t. $\underline{f} = \underline{g} + \underline{r}$ [r is unique $\Rightarrow g$ is unique]

(iii) $f \in I \iff r = 0$. [ideal membership problem].

Proof. Dividing $f \div G$ we have
$$f = \underbrace{a_1 \overset{I}{g_1} + \cdots + a_t \overset{I}{g_t}}_{g} + r \quad \text{where}$$
r satisfies (i) and $g = a_1 \overset{I}{g_1} + \cdots + a_t \overset{I}{g_t}$ satisfies (ii).

(iii). $(\Leftarrow)$ $r = 0 \Rightarrow f = g + r = g \in I \Rightarrow f \in I$.
$(\Rightarrow)$ $f \in I \Rightarrow r = 0$ [see proof of the HBT].

(uniqueness of r). Suppose $f = g_a + r_a$ and $f = g_b + r_b$ satisfy (uniqueness of r). Suppose $f = g_a + r_a$ and $f = g_b + r_b$ satisfy (i) and (ii). $\Rightarrow g_a + r_a = g_b + r_b$

$\Rightarrow \underbrace{g_a - g_b}_{\in I} = r_b - r_a \in I$

G is a G.B.

Suppose $r_b - r_a \neq 0$. Then $LT(r_b - r_a) \in \langle LT(I) \rangle = \langle LT(g_i) \rangle$

$\Rightarrow LT(r_b - r_a) \in \langle LM(g_i) \rangle \Rightarrow LM(g_i) \mid LT(r_b - r_a)$

by Lemma 2 of 2.4 contradicting (i).

Remark. The uniqueness of r does not depend on the order of the g_i in the $\div$ algorithm. But the quotients a_i in $a_1 g_1 + \cdots + a_t g_t$ are not unique in general.

E.g. $I = \langle x, y \rangle$ $\quad G = \{x, y\}$ is a GB for I.

Consider $f = xy + 1$. Let $>$ be any monomial ordering

$xy > 1$.

$$\begin{array}{ll} & a_1 = y \\ & a_2 = 0 \\ g_1 = x & \overline{)\,xy + 1} \\ g_2 = y & -(xy\ \ ) \\ & \overline{\qquad\quad 1} \leftarrow \text{remainder} \end{array} \qquad\qquad \begin{array}{ll} & a_1 = x \\ & a_2 = 0 \\ g_1 = y & \overline{)\,xy + 1} \\ g_2 = x & -xy \\ & \overline{\qquad\quad 1} \leftarrow \text{remainder} \end{array}$$

$$g = a_1 g_1 + a_2 g_2 = y \cdot x + 0 \cdot y = yx \qquad\qquad g = a_1 g_1 + a_2 g_2 = x \cdot y + 0 \cdot x = xy.$$