Lecture 15

4/4/2012

Note Title 4/3/2012

Today: Gröbner Basis

1. Defn.
2. Membership testing
3. Construction
4. Uniqueness

Ideal Membership Problem:

Given: $f_0, f_1, \ldots f_m \in \mathbb{K}[x_1 \ldots x_n]$

Decide: Is $f_0 \in (f_1, \ldots f_m)$

Notation: $\leq$ - admissible ordering on monomials

$LT(f = \sum_d c_d x^d) = c_d x^d$ (Leading Term)

$Lm(f) = x^d$ (Leading monomial)

$LC(f) = c_d$ (Leading Coeff)

Defn: $g_1 \dots g_t \in J = (f_1 \dots f_m)$ form a

Gröbner Basis if

$$(LT(g_1), \dots LT(g_t)) = (LT(J))$$

Motivation:

Want a basis to be "explicitly" representative.

$$\left.\begin{aligned} f_1 &= x^d + p_1 \\ f_2 &= x^d + p_2 \end{aligned}\right\} \Rightarrow p_1 \text{ or } p_2 \text{ or both must be in } G.B.$$

II. Membership Testing

Defn: r is a weak remainder of p divided by $f_1 \dots f_m$ if

1. $\exists q_1 \dots q_m$ s.t. $p = \sum f_i q_i + r$
2. No monomial of r is divisible by $LT(f_1), \dots LT(f_m)$.

We will show eventually that weak remainder when divided by a Gröbner Basis is unique. First a simple claim

---

Claim: $x^a \in (x^{m_1}, x^{m_2}, \dots x^{m_k})$ iff $\exists i$ s.t. $x^{m_i} \mid x^a$

Proof: Obvious

Lemma: Remainder wrt Gröbner basis is unique.

Proof: Suppose $p = \sum a_i g_i + r_1 = \sum b_i g_i + r_2$

& $(LT(g_1), \ldots LT(g_t)) = (LT(J))$

where $J = (g_1 \ldots g_t)$

(1) $r_1 - r_2 \in J$

(2) $LT(r_1 - r_2) \in (LT(J)) = (LT(g_1) \ldots LT(g_t))$

(3) w.l.o.g. $LT(r_1 - r_2) \in r_1$

(4) By Claim $\exists i$ s.t. $LT(g_i) \mid LT(r_1 - r_2)$
$\Rightarrow \exists$ monomial of r_1 which is divisible by $LT(g_i)$ $\Rightarrow$ violation of w.r. defn.

Algorithm for testing membership given G.B.

how?

(1) Compute weak remainder of f_0 with $f_1 \ldots f_m$

(2) Accept iff w.r. $= 0$.

II.V : Aside: G.B. is a Basis

Lemma: if $f \in J$ then

$$w.r.(f; g_1 \dots g_t) = 0$$

Proof: Similar to last proof.

$r \triangleq w.r.(f; g_1 \dots g_t) \in J$

$\Rightarrow LT(r) \in LT(J) \subseteq (LT(g_1) \dots LT(g_t))$

$\Rightarrow$ some monomial of r is divisible by $LT(g_i)$ for some i.

III. Construction of Gröbner Basis

Two new notions

Canonical Remainder $(f; h_1, \ldots h_\ell)$

Repeat { Pick highest monomial $m \in f$ s.t.
$LT(h_i) \mid m$;
$f \leftarrow f - \frac{m}{LT(h_i)} \cdot h_i$ }
until no such m exists ;
Output (f);

Syzygy

"Alignment of three celestial objects in a straight line"

$S(f,g)$ = poly in (f,g) obtained by minimal cancellation of leading terms.

$$= c_e \frac{M}{x^d} f - c_d \frac{M}{x^e} g$$

where $LT(f) = c_d x^d$; $LT(g) = c_e x^e$

$$M = LCM(x^d, x^e)$$

GB algorithm:

Input: $f_1 \dots f_m$

- $B = \{f_1 \dots f_m\}$
- while $\exists\, g, h \in B = \{b_1 \dots b_t\}$

$$r \triangleq \text{Canonical Remainder}\left(S(g,h) ; b_1 \dots b_t\right)$$

$$\neq 0$$

$B \leftarrow B \cup \{r\}$; continue

- report (B) ;

Analysis:

Will prove

At end B is a gröbner basis.

Claim: Canonical remainder comes with strong quotient; $r = C.R.(f; h_1 \dots h_t)$

$$\Rightarrow f = r + \sum_i m_j h_{ij}$$ with m_j being mon—

$$\Delta \quad \deg(m_j h_{ij}) \leq \deg(f).$$

Lemma: if $\forall\, g_i, g_j \in \{g_1 \dots g_t\}$

$$C.R.(S(g_i, g_j); g_1 \dots g_t) = 0$$

then $\forall\, f \in I(g_1 \dots g_t)$

$$LT(f) \in I(LT(g_1), \dots LT(g_t))$$

Proof:

Let $f = \sum_{j=1}^{K} m_j g_{i_j}$ where m_j's are monomials

① $\deg(m_j g_{i_j}) \geq \deg(m_{j+1} g_{i_{j+1}})$

& equality $\Rightarrow$ $i_j < i_{j+1}$

② $\deg(m_j g_{i_j})$ minimal, i_j smallest possible;

given $m_1 g_1, \ldots m_{j-1} g_{i_{j-1}}$.

- Now, if $\deg(m_1 g_{i_1}) > \deg(m_2 g_{i_2})$

then we are done;

- So assume $\deg(m_1 g_{i_1}) = \deg(m_2 g_{i_2})$;

Also wlog $i_1 = 1$, $i_2 = 2$.

$\Rightarrow \quad LT(m_1 g_1) = LT(m_2 g_2)$

Now consider $S(g_1, g_2) = a_1 g_1 - a_2 g_2$

(a_1, a_2 are monomials)

Since $LT(m_1 g_1) = LT(m_2 g_2)$

$\Rightarrow \quad m_1 = w \cdot a_1 \quad \& \quad m_2 = w \cdot a_2$

$\Rightarrow \quad m_1 g_1 - m_2 g_2 = w \cdot S(g_1, g_2)$

By termination condition

$S(g_1, g_2) = \sum g_i q_i$

with $\deg(g_i q_i) < \deg(a_1 g_1)$

So $m_1 g_1 - m_2 g_2 = \sum w g_i q_i$

with $\deg(w g_i q_i) < \deg(m_1 g_1)$

So $m_2 g_2 = m_1 g_1 +$ lesser order terms.

Contradicts (2)

$\boxtimes$