MAG Lecture 7 : Buchberger's Algorithm

mag7
1
27/7/22

Suppose we are given affine varieties $V = \mathbb{V}(I)$, $W = \mathbb{V}(J)$ and we want to know if they meet, i.e. whether $V \cap W = \phi$. Suppose $I = \langle f_1, \dots, f_n \rangle$, $J = \langle g_1, \dots, g_m \rangle$, then

$$V \cap W = \mathbb{V}(I + J) = \mathbb{V}(f_1, \dots, f_n, g_1, \dots, g_m)$$

while $\phi = \mathbb{V}(k[x_1, \dots, x_n])$. Suppose for the moment $\mathbb{I}(V \cap W) = I + J$ then

$$\begin{aligned} V \cap W = \phi &\iff \mathbb{I}(V \cap W) = \mathbb{I}(\phi) \\ &\iff I + J = k[x_1, \dots, x_n] \\ &\iff 1 \in I + J. \end{aligned}$$

How do we tell if $1 \in I + J$? We can run the division algorithm on 1 and $G = (f_1, \dots, f_n, g_1, \dots, g_m)$ and if it returns remainder 0 then $1 \in I + J$. But if the remainder is <u>nonzero</u> it doesn't necessarily mean $1 \notin I + J$. So the division algorithm isn't so useful for <u>generic</u> generating sets. However, the situation is better for Gröbner bases. Recall:

<u>Def^n</u> Let $k[x_1, \dots, x_n]$ have monomial order $<$, and let $G = \{g_1, \dots, g_n\}$ be a set of nonzero polynomials. Then G is a Gröbner basis for an ideal I if

$$\langle LT(g_1), \dots, LT(g_n) \rangle = \langle LT(I) \rangle.$$

the leading term of any $f \in I$ is divisible by some $LT(g_i)$.

Recall from last lecture (CLO Corollary 2.5.6) that every ideal has a Gröbner basis.

<u>Proposition CLO 2.6.1</u> Let $I \subseteq R = k[x_1, \dots, x_n]$ be an ideal with Gröbner basis $G = \{g_1, \dots, g_t\}$. Then given $f \in R$ there is a unique $r \in R$ with

(i) No term of r is divisible by any of $LT(g_1), \dots, LT(g_t)$

(ii) There is $g \in I$ such that $f = g + r$

Note r only depends on G as a <u>set</u>.

<u>Proof</u> The <u>existence</u> of r satisfying (i), (ii) follows from the division algorithm

$$f = \underbrace{q_1 g_1 + \cdots + q_t g_t}_{g} + r$$

To prove uniqueness suppose $f = g + r = g' + r'$ with r, r' both satisfying (i), (ii).
Then $r = f - g = (g' + r') - g \quad \therefore r - r' = g' - g \in I$. But then if $r - r' \neq 0$,

$$LT(r - r') \in \langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$$

so some $LT(g_i)$ divides $LT(r - r')$. But this is (proportional to) a term of r or r', which contradicts (i). Hence $r = r'$. $\square$

<u>Corollary CLO 2.6.2</u> Let $G = \{g_1, \dots, g_t\}$ be a Gröbner basis for an ideal $I \subseteq k[x_1, \dots, x_n]$ and let $f \in k[x_1, \dots, x_n]$. Then $f \in I$ iff. the remainder of f upon division by G is zero.

<u>Proof</u> If $r = 0$ clearly $f \in I$. If $f \in I$ then we have

$$f = q_1 g_1 + \cdots + q_t g_t + r \qquad \text{(by division)}$$
$$f = f + 0$$

and the uniqueness of the proposition gives $r = 0$. $\square$

Def^n Given a sequence $F = (f_1, \dots, f_s)$ we write $\overline{f}^F$ for the remainder of f upon division by F.

Clearly then we want to get our hands on Gröbner bases. We will now build towards an algorithm that computes Gröbner bases; the key idea (which is deep, and interesting for other reasons) is to examine the reasons behind polynomial equations (the poetic name for a reason is syzygy).

Def^n Given $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ we define $LCM(x^\alpha, x^\beta) = x^\gamma$ where $\gamma_i = \max\{\alpha_i, \beta_i\}$ for $1 \leq i \leq n$.

Def^n Let $f, g \in k[x_1, \dots, x_n]$ be nonzero, $x^\gamma = LCM(LM(f), LM(g))$. Then the S-polynomial of f, g is

$$S(f,g) = \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g$$

Lemma CLO 2.6.5 Suppose we have a sum $\sum_{i=1}^s p_i$ where $\text{multideg}(p_i) = \delta$ for all i. If $\text{multideg}(\sum_{i=1}^s p_i) < \delta$ (i.e. cancellations occur) then $\sum_{i=1}^s p_i$ is a linear combination, with coefficients in k, of $\{S(p_i, p_j)\}_{1 \leq i, j \leq s}$. Furthermore each $S(p_i, p_j)$ has multidegree $< \delta$.

Proof Let $d_i = LC(p_i)$ so $d_i x^\delta = LT(p_i)$. Then $\sum_{i=1}^s d_i = 0$ since $\text{multideg}(\sum_i p_i) < \delta$. Note

$$S(p_i, p_j) = \frac{1}{d_i} p_i - \frac{1}{d_j} p_j \qquad (\text{has multideg} < \delta)$$

Hence

$$\begin{aligned} \sum_{i=1}^{s-1} d_i S(p_i, p_s) &= d_1\left(\frac{1}{d_1} p_1 - \frac{1}{d_s} p_s\right) + d_2\left(\frac{1}{d_2} p_2 - \frac{1}{d_s} p_s\right) + \cdots \\ &= p_1 + \cdots + p_{s-1} - \frac{1}{d_s}(d_1 + \cdots + d_{s-1}) p_s \\ &= p_1 + \cdots + p_{s-1} - \frac{1}{d_s}(-d_s) p_s \\ &= \sum_{i=1}^s p_i. \quad \square \end{aligned}$$

In the situation of the lemma

$$\sum_{i=1}^{s} p_i = \sum_{i=1}^{s-1} d_i \, S(p_i, p_s)$$

cancellation is only present after addition

cancellations explicit before addition

Thus "all cancellation comes from S-polynomials".

<u>Theorem CLO 2.6.6</u> (Buchberger's criterion) Let I be a polynomial ideal. Then a basis $G = \{g_1, \dots, g_t\}$ of I is a Gröbner basis if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (in some order) is zero.

<u>Proof</u> ($\Rightarrow$) since $S(g_i, g_j) \in I$ this follows from the earlier result.

($\Leftarrow$) Let $f \in I$ be nonzero. We will show that $LT(f) \in \langle LT(g_1), \dots, LT(g_t) \rangle$, as follows. A <u>representation</u> of f is $\underline{h} = (h_1, \dots, h_t)$ with $h_i \in k[x_1, \dots, x_n]$ such that

$$f = \sum_{i=1}^{s} h_i g_i \qquad (*)$$

It is easy to see $\text{multideg}(f) \leq \delta_{\underline{h}} := \max\{\text{multideg}(h_i g_i) \mid 1 \leq i \leq n\}$.
Consider the set $\{\delta_{\underline{h}} \mid \underline{h} \text{ is a representation of } f\} \subseteq \mathbb{Z}^n_{\geq 0}$. By well-ordering this set has a minimal element δ. We have $\text{multideg}(f) \leq \delta$.

If $\text{multideg}(f) = \delta$ we are done, since then $\text{multideg}(f) = \text{multideg}(h_i g_i)$ for some i and so $LT(g_i) \mid LT(f)$.

Now suppose $\text{multideg}(f) < \delta$ and let $f = \sum_{i=1}^{s} h_i g_i$ with $\delta = \delta_{\underline{h}}$.
We will show this leads to a contradiction.

$$f = \sum_{\mathrm{multideg}(h_ig_i)=\delta} h_i g_i + \sum_{\mathrm{multideg}(h_ig_i)<\delta} h_i g_i$$

$$= \underbrace{\sum_{\mathrm{multideg}(h_ig_i)=\delta} LT(h_i) g_i}_{\text{call this } F} + \underbrace{\sum_{\mathrm{multideg}(h_ig_i)=\delta} (h_i - LT(h_i)) g_i + \sum_{\mathrm{multideg}(h_ig_i)<\delta} h_i g_i}_{\text{all terms of multidegree } < \delta} \qquad (*)$$

Since $\mathrm{multideg}(f) < \delta$ we have that $\mathrm{multideg}(F) < \delta$. Note $p_i = LT(h_i) g_i$ (for those i appearing in F) satisfy the hypotheses of the Lemma, hence F is a k-linear combination of S-polynomials $S(p_i, p_j)$. But $\mathrm{multideg}(p_i) = \delta$ so

$$S(p_i, p_j) = \frac{x^\delta}{LT(p_i)} p_i - \frac{x^\delta}{LT(p_j)} p_j$$

$$= \frac{x^\delta}{\cancel{LT(h_i)}LT(g_i)} \cancel{LT(h_i)} g_i - \frac{x^\delta}{\cancel{LT(h_j)}LT(g_j)} \cancel{LT(h_j)} g_j$$

$$= \frac{x^\delta}{LT(g_i)} g_i - \frac{x^\delta}{LT(g_j)} g_j \qquad \gamma_i = \max\{\alpha_i + \alpha'_i, \beta_i + \beta'_i\}$$

$$= x^{\delta - \gamma_{ij}} S(g_i, g_j) \qquad \gamma_{ij} = LCM(LM(g_i), LM(g_j))$$

Hence F is a k-linear combination of $x^{\delta - \gamma_{ij}} S(g_i, g_j)$'s. Since $\overline{S(g_i, g_j)}^{G} = 0$, the division algorithm gives $S(g_i, g_j) = \sum_{l=1}^{t} A_l g_l$, $\mathrm{multideg}(A_l g_l) \leq \mathrm{multideg}(S(g_i, g_j))$, whenever $A_l g_l \neq 0$. Hence

$$x^{\delta - \gamma_{ij}} S(g_i, g_j) = \sum_{l=1}^{t} B_l g_l \qquad B_l = x^{\delta - \gamma_{ij}} A_l$$

whenever $B_l g_l \neq 0$ $\mathrm{multideg}(B_l g_l) \leq \mathrm{multideg}(x^{\delta - \gamma_{ij}} S(g_i, g_j)) < \delta$ since $LT(S(g_i, g_j)) < x^{\gamma_{ij}}$.

Hence for some $\tilde{B}_l$

$$F = \sum_{l=1}^{t} \tilde{B}_l g_l$$

where if $\tilde{B}_l g_l \neq 0$ then multideg$(\tilde{B}_l g_l) < \delta$. But then $(*)$ is a representation of f with <u>all</u> terms of multidegree $< \delta$, which contradicts minimality of δ. $\square$