Lecture LVIII: Towards Gröbner bases III

Recall: Notions discussed in Lecture 57.

- **Monomial Order:** a total ordering on the set of monomials $\{\underline{x}^{\underline{\alpha}} : \underline{\alpha} \in \mathbb{Z}^n_{\geq 0}\}$ (or $\mathbb{Z}^n_{\geq 0}$) such that (1) $\underline{x}^{\underline{\alpha}} \leq \underline{x}^{\underline{\beta}} \Rightarrow \underline{x}^{\underline{\alpha}+\underline{\gamma}} \leq \underline{x}^{\underline{\beta}+\underline{\gamma}}$ $\forall\, \underline{\gamma} \in \mathbb{Z}^n_{\geq 0}$

  (2) $\leq$ is a well-ordering (so $1 < \underline{x}^{\underline{\alpha}}$ $\forall\, \underline{\alpha} \in \mathbb{Z}^n_{\geq 0} \setminus \{\underline{0}\}$)

Remark: Given (1), we have (2) $\Leftrightarrow$ $1 < x^{\underline{\alpha}}$ $\forall\, \underline{\alpha} \in \mathbb{Z}^n_{\geq 0} \setminus \{\underline{0}\}$.

Definition: Given $I \subseteq K[x_1, \ldots, x_n]$ an ideal, we define the leading ideal of I as

$$LT(I) = \text{ideal in } K[x_1, \ldots, x_n] \text{ generated by } \{LT(f) : f \in I\}$$

$LT(f) = x^{\underline{\alpha}_0}$ for $f = \sum c_{(\underline{\alpha})} x^{\underline{\alpha}}$ if $\cdot\ c_{(\underline{\alpha}_0)} \neq 0$

$\cdot\ x^{\underline{\alpha}} \leq x^{\underline{\alpha}_0}$ $\forall\, \underline{\alpha}$ with $c_{(\underline{\alpha})} \neq 0$

Definition: A finite set of generators of I say $\{g_1, \ldots, g_m\}$ is called a Gröbner basis of I with respect to a monomial order $<$ on $K[x_1, \ldots, x_n]$ if

$$LT(I) = (LT(g_1), \ldots, LT(g_m))$$

Key: We will only need $\{g_1, \ldots, g_m\} \subseteq I$ & $(LT(g_1), \ldots, LT(g_m)) = LT(I)$.

Notation: If $LT(\sum_{\underline{\alpha}} c_{\underline{\alpha}} x^{\underline{\alpha}}) = x^{\underline{\alpha}_0}$ we write $L(\sum_{\underline{\alpha}} c_{\underline{\alpha}} x^{\underline{\alpha}}) = c_{\underline{\alpha}_0} x^{\underline{\alpha}_0}$ (ie include coefficient of the leading monomial)

§58.1 Multivariate Division Algorithm:

- FIXED DATA: $g_1, \ldots, g_m \in K[x_1, \ldots, x_n]$, $<$ = a monomial order
- INPUT: $f \in K[x_1, \ldots, x_n]$
- OUTPUT: $q_1, \ldots, q_m \in K[x_1, \ldots, x_n]$, $r \in K[x_1, \ldots, x_n]$ such that $f = q_1 g_1 + \cdots + q_m g_m + r$

  where (1) No Term in r is divisible by $LT(g_1), LT(g_2), \ldots, LT(g_m)$

  (2) $LT(q_i g_i) \leq LT(f)$ $\forall\, i = 1, \ldots, m$.

- PROCEDURE:

  Start by setting $q_1, \ldots, q_m, r = 0$, $p = f$

  While $p \neq 0$:

- if $LT(p)$ is divisible by $LT(g_i)$ for some i (eg test in order $i=1,\dots,m$)

say $L(p) = a_i L(g_i)$ for $a_i \in K[x_1,\dots x_n]$ (it will be a monomial!), then

$$q_i \longmapsto q_i + a_i$$

$$p \longmapsto p - a_i g_i$$

- else:

$$r \longmapsto r + LT(p)$$

$$p \longmapsto p - LT(p)$$

Remarks: (1) Each step of the algorithm does not produce monomials in p that are larger that $LT(f)$.

(2) At each step, we only add terms to r that are not divisible by any $LT(g_1),\dots,LT(g_m)$

These 2 observations ensure the output has the desired properties. Furthermore, we obtain an extra condition on each $g_i g_i$:

Lemma: The polynomials at each step of the procedure satisfy:

$$LT(f) \geq LT(p) \quad \text{and} \quad LT(f) \geq LT(q_i g_i) \quad \text{whenever } g_i g_i \neq 0.$$

Example 1: $m=1$, $n=2$, $<$ = lexicographic with $x<y$

$f = x^3y^3 + 3x^2y^4$ $\quad g = g_1 = xy^4$ $\quad LT(f) = x^2y^4$ $\quad LT(g) = xy^4$

- $L(g) \mid 3x^2y^4 \rightsquigarrow a = 3x$ so $q_1 \longmapsto 3x$, $r = 0$

$$p \longmapsto p - 3x \cdot xy^4 = x^3y^3 \rightsquigarrow LT(p) = x^3y^3$$

$LT(g) \nmid x^3y^3$ so $f \longmapsto f - LT(f) = 0$, $r \longmapsto r + x^3y^3$

$$f = 3x\, g + r = 3x\,(xy^4) + x^3y^3$$

Example 2: $m=2$ $n=2$ $<$ = lex order with $x>y$

$f = xy^2+1$ $\quad g_1 = xy+1$ $\quad g_2 = y+1$ $\quad LT(f) = xy^2$ $\quad LT(g_1)=xy$, $LT(g_2)=y$

q_1 $\quad y$

q_2 $\quad -1$

$g_1 = xy+1$ | xy^2+1

$g_2 = y+1$ | $-\ xy^2+y$ $\quad y(xy+1)$

$1-y$

$-\ -1-y$ $\quad -1(y+1)$

2 $\quad$ ($LT(g_1) \nmid 2$ & $LT(g_2) \nmid 2$)

$$\Rightarrow f = y\, g_1 + (-1)\, g_2 + 2 \qquad g_1 = y,\ g_2 = -1,\ r = 2$$

Proof of Correctness and Lemma: By construction, no monomial of r is divisible by any $LT(g_i)$

The variable p represents the intermediate dividend at each step. With this notation, we show that:

$$f = q_1 g_1 + \cdots + q_m g_m + p + r \qquad (*)$$

and

$$LT(f) \geq LT(p) \;\&\; \forall i \; LT(f) \geq LT(q_i g_i) \quad \text{if} \quad q_i g_i \neq 0 \qquad (**)$$

after each iteration.

This is clearly true at the first step ($q_1 = \cdots = q_m = r = 0$, $p = f$)

(1) If some $LT(g_i)$ divides $LT(p) \Rightarrow$ Write $LT(p) = a_i LT(g_i)$

$$f \overset{?}{=} q_1 g_1 + \cdots + (q_i + a_i) g_i + \cdots + q_m g_m + (p - a_i g_i) + r. \quad \checkmark$$

because we had (*) valid from the previous step.

Now: $LT(p) = a_i LT(g_i) \Rightarrow LT(p - a_i g_i) < LT(p) \leq LT(f)$ because

- for each monomial x^α in g_i we have $a_i x^\alpha \leq a_i LT(g_i) = LT(p)$ and the inequality is strict if $x^\alpha \neq LT(g_i)$.
- $LT(p - a_i g_i)$ does not contain the monomial $LT(p)$.

$$LT((q_i + a_i) g_i) \leq \max\{ LT(q_i g_i), LT(a_i g_i) \} \leq LT(f)$$

$\leq LT(f)$; $LT(p) \leq LT(f)$

- For $j \neq i$ $LT(q_j g_j) \leq LT(f)$ is known from the previous step

This confirms (**)

(2) If no $LT(g_i)$ divides $LT(p)$, then:

$$f = q_1 g_1 + \cdots + q_m g_m + (p - LT(p)) + (r + LT(p)) \quad \checkmark$$

Now $LT(p - LT(p)) < LT(p) \leq LT(f)$

$LT(q_i g_i) \leq LT(f)$ $\forall i$ with $q_i g_i \neq 0$ by the previous step.

Q: Why does the procedure terminate?

Indeed, $f - a_i g_i$ will typically have more terms than f, so we need to give a reason to ensure our while loop is not infinite.

Proof of Termination: As we showed in the proof of correctness, at each step of the algorithm we get $LT(p_{new}) < LT(p)$ where $p_{new} = \begin{cases} p - a_i g_i \\ p - LT(p) \end{cases}$ depending

on whether some $LT(g_i) \mid LT(p)$ or not.

Then, if the algorithm didn't terminate (ie, we never get $p=0$), then we would produce a strictly decreasing sequence of monomials, contradicting the well-ordering property of $<$. This cannot happen.

§58.2 Existence of Gröbner basis:

Our first result weakens the requirement for a GB to being a generating set (it will be a consequence).

Proposition 1: Assume $I \subseteq R = K[x_1, \dots, x_n]$ is a non-zero ideal and $\{g_1, \dots, g_m\} \subseteq I$ satisfy $LT(I) = (LT(g_1), \dots, LT(g_m))$. Then, $\{g_1, \dots, g_m\}$ is a Gröbner basis of I.

Proof: We need to prove $(g_1, \dots, g_m) = I$.

Pick $f \in I$ & use multivariate division algorithm to write

$$f = \sum_{i=1}^{m} q_i g_i + r$$

where $r = 0$ or $r \neq 0$ & no monomial in r is divisible by any $LT(g_i)$ for i.

As $f, g_1, \dots, g_m \in I$, we have $r \in I$. Then, $LT(r) \in LT(I)$.

Claim: $LT(r) \in (LT(g_1), \dots, LT(g_m)) \Rightarrow \exists i$ st $LT(g_i) \mid LT(r)$

Pf/ By definition, we have $LT(r) = \sum_{i=1}^{m} h_i LT(g_i)$ for some $h_1, \dots, h_m \in R$.

Now, $LT(r)$ and each $LT(g_i)$ are all monomials.

So, $LT(r)$ must be a monomial on the (RHS) $\Rightarrow \exists$ i and x^α in some h_i with $LT(r) = x^\alpha LT(g_i)$

This shows $LT(g_i) \mid LT(r)$ for some i. □

As a consequence, we must have $r = 0$ (otherwise, we get $LT(g_i) \nmid LT(r)$ $\forall i$ and $\exists i$ with $LT(g_i) \mid LT(r)$, which is impossible).

Hence $f \in (g_1, \dots, g_m)$, as we wanted to show.

Theorem 1: Gröbner bases exist.

Proof: Since $LT(I)$ is an ideal of R, which is Noetherian, we know it is finitely generated. Furthermore, by Lemma §51.3 we can find a finite generating set for $LT(I)$ among $\{LT(f) : f \in I\}$. That is $\exists\ g_1, \dots, g_m \in I$ with

$LT(I) = (LT(g_1), \dots, LT(g_m))$. By Proposition, we conclude $\{g_1, \dots, g_m\}$ is a GB of I.

Remark: If we can show directly that $LT(I)$ is always finitely generated (without invoking Hilbert's Basis Theorem), the existence of Gröbner basis would reprove $K[x_1, \dots, x_n]$ is Noetherian. The later statement is true and it is known as Dickson's Lemma. It can be proved by using induction on n,

- The main application of GB is to provide a concrete certificate for when a polynomial lies in a given ideal

Theorem 2 (Membership Test) Let $I \subset R = K[x_1, \dots, x_n]$ be an ideal and let $\{g_1, \dots, g_m\}$ be a Gröbner basis of I. Then, for every $f \in R$, there exist unique elements $f_I \in I$ and $r \in R$ such that:

(1) $f = f_I + r$

(2) No monomial appearing in r is divisible by any $LT(g_i)$ for $i = 1, \dots, m$.

Proof: We write $f = \underbrace{\sum_{i=1}^{m} q_i g_i}_{= f_I \in I} + r$ using the multivariate division algorithm.

This confirms conditions (1) and (2) are true. Thus, we only need to prove uniqueness.

Assume $f = f_I + r = \tilde{f}_I + \tilde{r} \Rightarrow r - \tilde{r} = \tilde{f}_I - f_I \subset I$

$\Rightarrow LT(r - \tilde{r}) \in LT(I) = (LT(g_1), \dots, LT(g_m))$ by definition of GB.

The proof of the Claim in Proposition 1 ensures $\exists i$ with $LT(g_i) \mid LT(r - \tilde{r})$

Since $LT(r - \tilde{r})$ is a monomial in either r or $\tilde{r}$ (if it is non-zero), we get a contradiction unless $r - \tilde{r} = 0$. Thus, $r = \tilde{r}$ and so $f_I = \tilde{f}_I$

Corollary: $f \in I \iff r = 0$.

Meaning: if we are given an ideal I, as being generated by $f_1, \dots, f_\ell$ and asked to check whether $f \in I$ or not

(1) Replace $\{f_1, \dots, f_\ell\}$ by a Gröbner basis of I, say $\{g_1, \dots, g_m\}$

(2) Use the division algorithm to compute the remainder r

- $r = 0 \Rightarrow f \in I$
- $r \neq 0 \Rightarrow f \notin I$ (This part will be false if $\{g_1, \ldots, g_m\}$ is NOT a GB)