Computer Algebra for Computer Engineers

Polynomial Manipulation in $k[x_1, \ldots, x_n]$

Priyank Kalla

Department of Electrical and Computer Engineering

University of Utah, Salt Lake City

Monomial Orderings

A Power product is an expression of the form $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$, where x_i is a variable and $\alpha_i \in Z_{\geq 0}$. For simplicity we will write a power product as $x^\alpha,\ \alpha \in Z_{\geq 0}^n$. Power product is also a monomial.

- Term = $a \cdot x^\alpha$ = coeff. times a power product
- $\mathbb{T}^n = \{x^\alpha : \alpha \in \mathbb{Z}_{\geq 0}\}$ is the set of all power products
- A multivariate polynomial is then a sum of terms

To operate on polynomials, we need an ordering of monomials: Lex, DegLex and DegRevLex orders.

Monomial Ordering

The order should be a total order $<$ on $\mathbb{T}^n$, and it should be a well-ordering.

- Total order: One and only one of the following should be true: $x^\alpha > x^\beta$ or $x^\alpha = x^\beta$ or $x^\alpha < x^\beta$.
- $1 < x^\alpha, \quad \forall x^\alpha \quad (x^\alpha \neq 1)$
- $x^\alpha < x^\beta \implies x^\alpha \cdot x^\gamma < x^\beta \cdot x^\gamma$.

Definition 1 **Lexicographic order:** *Let* $x_1 > x_2 > \cdots > x_n$ *lexicographically. Also let* $\alpha = (\alpha_1, \ldots, \alpha_n)$; $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. *Then we have:*

$$x^\alpha < x^\beta \iff \begin{cases} \textit{Starting from the left, the first co-ordinates of } \alpha_i, \beta_i \\ \textit{that are different satisfy } \alpha_i < \beta_i \end{cases} \tag{1}$$

DegLex and DegRevLex Orderings

Definition 2 **Degree Lexicographic order:** *Let* $x_1 > x_2 > \cdots > x_n$ *lexicographically. Also let* $\alpha = (\alpha_1, \ldots, \alpha_n);\ \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. *Then we have:*

$$x^\alpha < x^\beta \iff \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i & \text{or} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ AND } x^\alpha < x^\beta & \text{w.r.t. LEX order} \end{cases} \tag{2}$$

Definition 3 **Degree Reverse Lexicographic order:** *Let* $x_1 > x_2 > \cdots > x_n$ *lexicographically. Also let* $\alpha = (\alpha_1, \ldots, \alpha_n);\ \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. *Then we have:*

$$x^\alpha < x^\beta \iff \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \text{ or} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ AND the first co-ordinates} \\ \alpha_i, \beta_i \text{ from the RIGHT, which are different, satisfy } \alpha_i > \beta_i \end{cases} \tag{3}$$

Ordering Examples

[Textbook Example from p22] Let $f = 2x^2yz + 3xy^3 - 2x^3$

- LEX $x > y > z$: $f = -2x^3 + 2x^2yz + 3xy^3$
- DEGLEX $x > y > z$: $f = 2x^2yz + 3xy^3 - 2x^3$
- DEGREVLEX $x > y > z$: $f = 3xy^3 + 2x^2yz - 2x^3$

In singular: we declare ordering as:

```
ring r = 0, (x, y, z), lp; //LEX x > y > z
ring r = 0, (x, z, y), Dp; //DEGLEX x > z > y
ring r = 0, (y, z, x), dp; //DEGREVLEX y > z > x
```

Multivariate Division

Explained in the textbook, Sec 1.5.

- To divide f by g, we denote it as $f \xrightarrow{g} h$, where $h = f - \frac{X}{\mathsf{lt}(g)} g$. Here, X may not be the leading term.
- From Ex. 1.5.2, step 2 in the division process: $f = \frac{1}{4}x^3 + \frac{7}{2}yx - \frac{11}{4}x^2, \;\; g = 2y + x + 1$; Ordering: deglex $y > x$. Note that LT(f) is not divisible by LT(g), but $\frac{7}{2}yx$ is divisible by LT(g). So, we move the term LT(f) = $\frac{1}{4}x^3$ into the remainder, and continue to divide (reduce) the next term $\frac{7}{2}yx$ by LT(g) = $2y$.

Multivariate Division

Definition 4 *Let* $f, f_1, \ldots, f_s, h \in k[x_1, \ldots, x_n], f_i \neq 0; \; F = \{f_1, \ldots, f_s\}$. *Then* f *reduces to* h *modulo* F*:*

$$f \xrightarrow{F}_+ h$$

if and only if there exists a sequence of indices $i_1, i_2, \ldots, i_t \in \{1, \ldots, s\}$ *and a sequence of polynomials* $h_1, \ldots, h_{t-1} \in k[x_1, \ldots, x_n]$ *such that*

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h$$

Definition 5 *If* $f \xrightarrow{F}_+ r$, *then no term in* r *is divisible by LT*$(f_i), \; \forall f_i \in F$. *Then* r *is reduced w.r.t.* F *as is called the remainder.*

Division Algorithm

Study the Division algorithm 1.5.1 from the textbook.

Definition 6 *Let* $f, f_1, \ldots, f_s, r \in k[x_1, \ldots, x_n], f_i \neq 0; \quad F = \{f_1, \ldots, f_s\}$. *Then* f *reduces to* r *modulo* F*:*

$$f \xrightarrow{F}_{+} r$$

then

$$f = u_1 f_1 + \cdots + u_s f_s + r$$

then we have

- r *is reduced w.r.t.* F
- $u_1, \ldots u_s \in k[x_1, \ldots, x_n]$
- $LP(f) = MAX(LP(f_1)LP(u_1), \ldots LP(f_s)LP(u_s), r)$

Subtleties of the Division Process

Suppose we have: $f \xrightarrow{F}_{+} r$. If $r = 0$ then $f \in I =< F >$. But, if $r \neq 0$ then we cannot decided ideal membership unequivocally. Thats why we need Groebner Bases.

Let $f = xy^2 - x;\ f_1 = xy + 1;\ f_2 = y^2 - 1$. Note that $f \in I = \langle f_1, f_2 \rangle$ as $f = xf_2$.

$$f \xrightarrow{f_1, f_2}: f = y \cdot f_1 + 0 \cdot f_2 + (-x - y)$$

$$f \xrightarrow{f_2, f_1}: f = x \cdot f_2 + 0 \cdot f_1 + 0$$

Moral of the Story If we change the order in which we divide by $f_1, \ldots, f_s$, we obtain different quotients and different remainders.

Motivating Gröbner Bases

Let $F = \{f_1, \ldots, f_s\}$; $I = \langle f_1, \ldots, f_s \rangle$ and let $f \in I$. Then we should be able to represent $f = u_1 f_1 + \cdots + u_s f_s + r$ where $r = 0$. If we were to divide f by $F = \{f_1, \ldots, f_s\}$, then we will obtain an intermediate remainder (say, h) after every one-step reduction. The leading term of every such remainder (LT(h)) should be divisible by the leading term of atleast one of the polynomials in F. Only then we will have $r = 0$.

Definition 7 *Let* $F = \{f_1, \ldots, f_s\}$; $G = \{g_1, \ldots, g_t\}$; $I = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$. *Then* G *is a* **Gröbner Basis** *of* I

$$\Longleftrightarrow$$

$$\forall f \in I \ \ (f \neq 0), \quad \exists i : LP(g_i) \mid LP(f)$$