Lesson 7 – Monomial Orderings and the Division Algorithm

Last lesson we talked about the implicit ordering ($x > y > z$) used in row reduction when eliminating variables in a system of linear equations. We also discussed the ordering of monomials in the univariate case: $1 < x < x^2 < \cdots < x^n$. The first of these orderings was really arbitrary, but the second was necessary in ensuring the termination of the Division Algorithm. Now we wish to generalize the Division Algorithm for polynomials in one variable to multivariable polynomials $f \in k[x_1, x_2, \ldots, x_n]$. In order to do this, we will need a way of ordering the monomials appearing in a polynomial. (Recall that a **monomial** in the variables $x_1, x_2, \ldots, x_n$ is a product of the form ${x_1}^{\alpha_1}{x_2}^{\alpha_2}\cdots{x_n}^{\alpha_n}$.)

Motivating Question: How might you order the terms in the following polynomial in $\mathbb{R}[x, y, z]$? Which term would say is the biggest?

$$f(x, y, z) = x^6 + y^5 - 2x^5z^3 + 4x^4y^3z^4 + 3x^3y^4z^4 - 6z^4 + xyz - 4y^3$$

Observe that every term in $f(x, y, z)$ has the form $Cx^{\alpha_1}y^{\alpha_2}z^{\alpha_3}$, where $\alpha_i \in \mathbb{Z}_{\geq 0}$. Hence ordering the monomials amounts to ordering triples $(\alpha_1, \alpha_2, \alpha_3)$ in $\mathbb{Z}^3_{\geq 0}$.

Definition. A **monomial ordering** on $k[x_1, x_2, \ldots, x_n]$ is any relation > on $\mathbb{Z}^n_{\geq 0}$, or equivalently, any relation > on the set of monomials $x^\alpha = {x_1}^{\alpha_1}{x_2}^{\alpha_2}\cdots{x_n}^{\alpha_n}$, $\alpha \in \mathbb{Z}^n_{\geq 0}$ satisfying:

(1) > is a total (or linear) order on $\mathbb{Z}^n_{\geq 0}$.
(2) If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$.
(3) > is a well-ordering on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under >.

Question: Why is *this* the definition?

Exercise 1 Prove that (0, 0, 0, ..., 0) must be the smallest element in $\mathbb{Z}^n_{\geq 0}$ under any monomial ordering.

We will consider three different monomial orderings: the Lexicographic Order, the Graded Lexicographic Order, and the Graded Reverse Lexicographic Order.

I. Three Monomial Orderings

The Lexicographic ("Dictionary") Order

Definition (lex) Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}_{\geq 0}^n$, the leftmost nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

The Graded Lexicographic Order

Definition (grlex) Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. We say $\alpha >_{grlex} \beta$ if,

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i \quad \text{or} \quad |\alpha| = |\beta| \text{ and } \alpha >_{lex} \beta.$$

Hence, in the graded lexicographic order, monomials with the highest total agree are considered the largest, and then the lexicographic order is used to "break ties".

The Graded Reverse Lexicographic Order

Definition (grevlex) Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. We say $\alpha >_{grevlex} \beta$ if,

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i \quad \text{or} \quad |\alpha| = |\beta| \text{ and the rightmost nonzero entry of } \alpha - \beta \in \mathbb{Z}_{\geq 0}^n \text{ is negative.}$$

Hence, in the graded reverse lexicographic order, monomials with the highest total agree are considered the largest, and ties are broken by looking at the rightmost (or smallest) variable; smaller powers win.

Exercise 2. Order the monomials in $f(x, y, z) = x^6 + y^5 - 2x^5z^3 + 4x^4y^3z^4 + 3x^3y^4z^4 - 6z^4 + xyz - 4y^3$ using each of the three monomial orderings defined above.

Before stating the multivariate Division Algorithm we need a few more definitions.

Definition Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, x_2, \dots, x_n]$ and let > be a monomial order.

(i) The **multidegree** of f is multideg(f) = max$\{\alpha \in \mathbb{Z}_{\geq 0}^n : a_\alpha \neq 0\}$ where the maximum is taken with respect to the order >.
(ii) The **leading coefficient** of f is LC(f) = $a_{\text{multideg}(f)} \in k$.
(iii) The **leading monomial** of f is LM(f) = $x^{\text{multideg}(f)}$.
(iv) The **leading term** of f is LT(f) = LC(f) · LM(f)

Observe that the multidegree of a polynomial is an n-tuple and not an integer.

Exercise 3. What is the multidegree of the polynomial

$$f(x, y, z) = x^6 + y^5 - 2x^5z^3 + 4x^4y^3z^4 + 3x^3y^4z^4 - 6z^4 + xyz - 4y^3$$

with respect to each of the three orders? What are the leading terms under each of the three monomial orderings?

II. Examples of Multivariate Polynomial Division

Let's start with a simple example...

Exercise 4 Let $f(x, y) = 6x^2y - x + 4y^3 - 1$ and $g(x, y) = 2xy + y^3$. Try to emulate the univariate division algorithm to write $f = gq + r$ using the lex ordering with $x > y$.

Exercise 5 Once again, let $f(x,y) = 6x^2y - x + 4y^3 - 1$ and $g(x,y) = 2xy + y^3$. Now try to emulate the univariate division algorithm to write $f = gq + r$ using the **grlex ordering** with $x > y$.

Next we want to generalize the above process to reduction modulo a *set* of non-zero polynomials.

Exercise 6 Find the quotients and remainder in $\mathbb{Q}[x]$ when reducing $f(x,y) = x^2y + xy^2 + y^2$ by $g_1(x,y) = xy - 1$ and $g_2(x,y) = y^2 - 1$ with respect to the lex order with $x > y$. (That is, divide $x^2y + xy^2 + y^2$ by the set *F* = $(xy - 1,\ y^2 - 1)$, *in that order*.)

We need holders for the quotients and this time we encounter terms in the divisor that are not divisible by either leading term of the $g_i's$. These must be transferred to the remainder before proceeding:

III. The Multivariate Division Algorithm

Definition. Let $G = \{g_1, g_2, \dots, g_s\} \subseteq k[x_1, x_2, \dots, x_n]$. A polynomial $f \in k[x_1, x_2, \dots, x_n]$ **reduces to** h **modulo** G, $f \xrightarrow{G}_+ h$, if there is a sequence $i_1, i_2, \dots, i_t$ such that

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

A polynomial h is said to be **reduced** with respect to G if either $h = 0$ or every term of h is indivisible by any $\mathrm{LT}(g_i)$, $g_i \in G$. Such an h is called a **remainder** of f with respect to G.

Theorem (The Division Algorithm in $k[x_1, x_2, \dots, x_n]$) Fix a monomial order > on $\mathbb{Z}^n_{\geq 0}$ and let $F = (g_1, g_2, \cdots, g_s)$ be an ordered s-tuple of polynomials in $k[x_1, x_2, \dots, x_n]$. Then for any $f \in k[x_1, x_2, \dots, x_n]$ there exist $a_1, a_2, \dots, a_s, r \in k[x_1, x_2, \dots, x_n]$ such that

1. $f = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s + r$ and r is reduced with respect to G.
2. $\max\{\mathrm{LT}(a_1)\mathrm{LT}(g_1), \dots, \mathrm{LT}(a_s)\mathrm{LT}(g_s), \mathrm{LT}(r)\} = \mathrm{LT}(f)$

(Condition 2 stated above is stronger than and implies the textbook's second condition "if $a_i g_i \neq 0$, then $\mathrm{multideg}(f) \geq \mathrm{multideg}(a_i g_i)$".)

Remarks:

1. The criterion that r is reduced is analogous to the condition in the univariate case that $\deg r < \deg g$ so that no further reduction is possible.
2. The second condition means that there is no cancellation among higher order terms in the quotient/remainder form. Note that it is a simple exercise to prove that $\mathrm{LT}(a_i g_i) = \mathrm{LT}(a_i)\mathrm{LT}(g_i)$.

The Idea of the Proof:

INITIAL VALUES: $a_1 := 0, a_2 := 0, \dots, a_s := 0, r := 0, h := f$

ALGORITHM: While $h \neq 0$ do

-if $\exists i$ such that $\mathrm{LT}(g_i) | \mathrm{LT}(h)$ then choose the least such i and

$$a_i := a_i + \frac{\mathrm{LT}(h)}{\mathrm{LT}(g_i)}$$

$$h := h - \frac{\mathrm{LT}(h)}{\mathrm{LT}(g_i)} g_i$$

-else $r := r + \mathrm{LT}(h)$

$h := h - \mathrm{LT}(h)$

The well-ordering of the term order ensures this algorithm terminates, as the order of the leading power of h reduces at each pass through the loop. Moreover at each stage we have

$$f = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s + r + h$$

$$\mathrm{LT}(f) = \max\{\mathrm{LT}(a_1)\mathrm{LT}(g_1), \dots, \mathrm{LT}(a_s)\mathrm{LT}(g_s), \mathrm{LT}(r), \mathrm{LT}(h)\}$$

which can be proved by induction.

Exercise 7 Divide the polynomial $f(x,y) = x^2y - y$ by the set $\langle g_1, g_2 \rangle$ where $g_1(x,y) = xy + x$ and $g_2(x,y) = x^2 - 1$, assuming the lex order with $x > y$.

Exercise 8 Now divide the polynomial $f(x,y) = x^2y - y$ by the set $\langle g_2, g_1 \rangle$ where $g_1(x,y) = xy + x$ and $g_2(x,y) = x^2 - 1$. That is, switch the order of the polynomials in the set. (Again, order the monomials lexicographically, with $x > y$.)

Example 9 - True or False (for parts a-d, assume that the monomial order is fixed)

a) Suppose we apply the division algorithm twice on a given $f \in k[x_1, x_2, \dots, x_n]$. First we divide f by an s-tuple $(\boldsymbol{g_1}, \boldsymbol{g_2}, \dots, g_s)$ and obtain $f = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s + r_1$; then we divide f by the s-tuple $(\boldsymbol{g_2}, \boldsymbol{g_1}, \dots, g_s)$ and obtain $f = b_1 g_1 + b_2 g_2 + \cdots + b_s g_s + r_2$. Then $a_i = b_i$, for all $1 \leq i \leq s$, and $r_1 = r_2$.

b) If we apply the division algorithm to divide $f \in k[x_1, x_2, \dots, x_n]$ by the set $F = (g_1, g_2, \dots, g_s)$ and get $f = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s + 0$ (so the remainder is zero), then $f \in \langle g_1, g_2, \dots, g_s \rangle$.

c) If $f \in I = \langle g_1, g_2, \dots, g_s \rangle$ and we apply the division algorithm to divide $f \in k[x_1, x_2, \dots, x_n]$ by the set $F = (g_1, g_2, \dots, g_s)$, then the remainder will be zero.

d) If we divide $f \in k[x_1, x_2, \dots, x_n]$ by an s-tuple $(g_1, g_2, \dots, g_s)$ *in that order* and obtain $f = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s + r$, then the $a_1, a_2, \dots, a_s$ and r are unique *for division in that order*.

e) If we want to determine if a given polynomial $f \in k[x_1, x_2, \dots, x_n]$ is in an ideal $I = \langle g_1, g_2, \dots, g_s \rangle$, then we can simply apply the division algorithm to express $f = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s + r$, and check to see if $r = 0$.

f) Suppose we apply the division algorithm twice on a given $f \in k[x_1, x_2, \dots, x_n]$. First we divide f by an s-tuple $(g_1, g_2, \dots, g_s)$ using the **lex order**, and we obtain $f = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s + r_1$; then we divide f by the s-tuple $(g_1, g_2, \dots, g_s)$ using the **grlex order** and obtain $f = b_1 g_1 + b_2 g_2 + \cdots + b_s g_s + r_2$. Then $a_i = b_i$, for all $1 \leq i \leq s$, and $r_1 = r_2$.