Multivariate Polynomials

October 19, 2023 8:29 AM

Assignment #3 due Monday @ 11pm.

Let R be a ring and $R[x_1, x_2, \ldots, x_n] = \{ \sum_{i=1}^{t} a_i x_1^{e_{1i}} \cdot x_2^{e_{2i}} \cdot \cdots \cdot x_n^{e_{ni}} : a_i \in R \}$

Def. The vectors $[e_{1i}, e_{2i}, \ldots, e_{ni}] \in \mathbb{Z}^n_{\geq 0}$ are called <u>exponent vectors</u>.

If $n=3$ we will use x, y, z instead of x_1, x_2, x_3.

E.g. $a = 7y^4 + 3x^2y^2 + 2xy^4 - 7xy^2 - 2x^3 \in \mathbb{Z}[x,y]$.

$[0,4]$ $[2,2]$ $[1,4]$ $[1,2]$ $[3,0]$ $\deg(a) = 5$.

Def. The total degree $\deg(a) = \max_{i=1}^{t} \sum_{j=1}^{n} e_{ji}$.

If R is an integral domain and $a, b \in R[X]$

$$\deg(a \cdot b) = \deg(a) + \deg(b).$$

The terms $a_i \cdot x_1^{e_{1i}} \cdot x_2^{e_{2i}} \cdot \cdots \cdot x_n^{e_{ni}}$ for $1 \leq i \leq t$ are usually ordered in a term ordering (or a monomial ordering).

Def (Monomial Ordering). A monomial ordering on $R[X]$ is a order relation $>$ on $\mathbb{Z}^n_{\geq 0}$, or, equivalently on the set of monomials $\{ X^\alpha : \alpha \in \mathbb{Z}^n_{\geq 0} \}$ such that $\forall\ \alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$ satisfies.

(i) $>$ is a total order on $\mathbb{Z}^n_{\geq 0}$ i.e., either

$\alpha > \beta$ or $\alpha < \beta$ or $\alpha = \beta$. and

$\alpha > \beta$ and $\beta > \gamma \Rightarrow \alpha > \gamma$.

(ii) $\alpha > \beta \Rightarrow \alpha + \underline{\gamma} > \beta + \underline{\gamma}$

$(X^\alpha > X^\beta \Rightarrow X^\alpha \cdot X^\gamma > X^\beta \cdot X^\gamma).$

(iii) $>$ is a well ordering on $\mathbb{Z}^n_{\geq 0}$, i.e., every non-empty subset $S \subset \mathbb{Z}^n_{\geq 0}$ must have a least element, equivalently $1 = X^{[0,0,\ldots,0]} \leq X^\alpha$.

There are an infinite number of monomial orderings if $n \geq 2$.
If $n=1$ there is only one, namely, $\underline{1 < x < x^2 < x^3 < \cdots}$

(Pure) lexicographical order

If $u, v \in \mathbb{Z}_{\geq 0}^n$ then

$u > v$ if $\underline{u_k > v_k}$ for some $1 \leq k \leq n$ and $u_j = v_j$ for $1 \leq j < k$.

E.g. $a = 2x^3 + 7x^2y + 3x^2y^2 + 5y^5$

$[3,0] > [2,1] < [2,2] > [0,5]$

deg: 3 3 4 5.

Graded lexicographical order. Terms are ordered in decreasing total degree with ties broken using lex. order.

$$5y^5 + 3x^2y^2 + 2x^3 + 7x^2y.$$

Def. Let $LT(a)$ be the largest term in $>$ and let $LC(a)$ and $LM(a)$ be the coefficient of $LT(a)$ and the monomial of $LM(a)$.

Eg. In lex $LT(a) = 2x^3$, $LC(a) = 2$, $LM(a) = x^3$.

In grlex $LT(a) = 5y^5$, $LC(a) = 5$, $LM(a) = y^5$.

Properties. If R is an integral domain and $a, b \in R[X]$ then

$$LT(a \cdot b) = LT(a) \cdot LT(b)$$
$$LC(a \cdot b) = LC(a) \cdot LC(b)$$
$$LM(a \cdot b) = LM(a) \cdot LM(b).$$

Division in $F[X]$ where F is a field.

Input $a, b \in F[X]$, $b \neq 0$.

Output $q, r \in F[X]$ s.t. $a = bq + r$ and no term in r is divisible by $LT(b)$.

$r \leftarrow 0$

$q \leftarrow 0$

$$a = b \cdot q$$
$$LT(a) = LT(b) \cdot LT(q)$$

$r \leftarrow 0$
$q \leftarrow 0$
while $a \neq 0$ do
  if $LT(b) \mid LT(a)$ then
    $t \leftarrow LT(a)/LT(b)$
    $q \leftarrow q + t$
    $\boxed{a \leftarrow a - tb}$
  else
    $r \leftarrow r + LT(a)$
    $a \leftarrow a - LT(a)$.
Output q, r.

$a = b \cdot q$
$LT(a) = LT(b) \cdot LT(q)$
$\Rightarrow LT(b) \mid LT(a)$.

Why does this algorithm terminate.
Because either $a = 0$ or $LM(a - tb) < LM(a)$. (Proof?).
and $>$ is a well ordering.

Example   Using grlex with $x > y > z$.

$q = 3xyz + 2x^2$

$b = xy^2 + 3z$) $3x^2y^3z + 4xyz^4 + 2x^3y^2 + 9xyz^2 + 6x^2z = a$

$-t \cdot b$ $-(3x^2y^3z + 9xyz^2)$

$0 + \boxed{4xyz^4} + 2x^3y^2 + 0 + 6x^2z = a$

$r = 4xyz^4$ $(-4xyz^4)$

$2x^3y^2 + 6x^2z = a$.

$-(2x^3y^2 + 6x^2z)$

0.

In lex order $q = 2x^2 + 3xyz$

$b = xy^2 + 3z$) $2x^3y^2 + 3x^2y^3z + 6x^2z + 4xyz^4 + 9xyz^2 = a$

$-(2x^3y^2 + 6x^2z)$

$0 + 3x^2y^3z + 0 + 4xyz^4 + 9xyz^2 = a$

$r = 4xyz^4$ $-(3x^2y^3z + 9xyz^2)$

$4xyz^4$

$-4xyz^4$

0.