Advanced Robotics

Lecture 6

pajdla@cmp.felk.cvut.cz

"Division theorem"

Let k be a field and g be a non-zero polynomial in $k[x]$.

(i) Then every $f \in k[x]$ can be written as

$$f = q\,g + r$$

where $q, r \in k[x]$, and either

$$r = 0 \quad \text{or} \quad \deg(r) < \deg(g)$$

(ii) Furthermore, q and r are unique.

pajdla@cmp.felk.cvut.cz

Proof: "Division algorithm"

Input: g, f

Output: q, r

$q := 0$

$r := f$

WHILE $r \neq 0$ AND $LT(g)$ divides $LT(r)$ DO

{

$$q := q + \frac{LT(r)}{LT(g)}$$

$$r := r - \frac{LT(r)}{LT(g)} \cdot g$$

}

pajdla@cmp.felk.cvut.cz

Observe that $f = q g + r$ holds true

(a) $q = 0$ & $r = f \Rightarrow 0 \cdot g + f = f$

(b) Let q_i, r_i be such that $f = q_i g + r_i$, then

$$q_{i+1} g + r_{i+1} = \underbrace{\left(q_i + \frac{LT(r_i)}{LT(g)} \right)}_{q_{i+1}} g + \underbrace{\left(r_i - \frac{LT(r_i)}{LT(g)} \cdot g \right)}_{r_{i+1}} =$$

$$= q_i g + r_i = f$$

If the algorithm terminates, then either

$r = 0$ or

$LT(g)$ does not divide $LT(r) \Leftrightarrow \deg(r) < \deg(g)$

Let us show that the algorithm terminates

Assume that the algorithm does not terminate. Then, $LT(g)$ divides $LT(r)$ and $r \neq 0$.

Observe that for $r_{i+1} = r_i - \frac{LT(r_i)}{LT(g)} \cdot g$ holds

$$r_{i+1} \begin{cases} \text{either} & = 0 \\ \text{or} & \deg(r_{i+1}) < \deg(r_i) \end{cases}$$

write $r_i = a_0 x^m + a_1 x^{m-1} + \cdots + a_m$ with $m \geq \ell$

$g = b_0 x^\ell + b_2 x^{\ell-1} + \cdots + b_\ell$ ($LT(g)$ divides $LT(r_i)$)

$$r_{i+1} = r_i - \frac{LT(r_i)}{LT(g)} \cdot g = \underbrace{(a_0 x^m + a_1 x^{m-1} + \cdots) - \frac{a_0}{b_0} x^{m-\ell} (b_0 x^\ell + b_1 x^{\ell-1} + \cdots)}_{\text{cancel}}$$

$$= (a_1 x^{m-1} + \cdots) - (\frac{a_0}{b_0} b_1 x^{m-1} + \cdots)$$

$$= (a_1 - \frac{a_0}{b_0} b_1) x^{m-1} + (a_2 - \frac{a_0}{b_0} b_2) x^{m-2} + \cdots$$

and therefore we see that

either $r_{i+1} = 0$ if all coefficients vanish

or $\deg(r_i+1) \leq m-1 < m = deg(r_i)$

pajdla@cmp.felk.cvut.cz

Monomial ordering

Monomials in one variable are easy to order by their degree, i.e.

$$x^0 <_{deg} x^1 <_{deg} x^2 <_{deg} \dots$$

also notice that $x^m <_{deg} x^n \iff x^m$ divides x^n

Not so simple with more variables

consider xy^2, x^2y ... neither one divides the the other but

$$\deg(xy^2) = 1+2 = 3 = 2+1 = \deg(x^2y)$$

pajdla@cmp.felk.cvut.cz

A monomial ordering on $k[x_1, \dots, x_n]$ is any ordering relation $<$ on $\mathbb{Z}^n_{\geq 0}$ satisfying :

(i) $\forall\, \alpha, \beta :\quad \alpha > \beta$ or $\alpha < \beta$

(ii) $\alpha > \beta$ & $\gamma \in \mathbb{Z}^n_{\geq 0} \Rightarrow \alpha + \gamma > \beta + \gamma$

(iii) $\forall\, \alpha :\quad \alpha > 0$

we write $\quad x^\alpha > x^\beta \stackrel{def}{\equiv} \alpha > \beta$

pajdla@cmp.felk.cvut.cz

Lexicographic order

$$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n), \quad \beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$$

$\alpha >_{lex} \beta$ if the left-most non-zero element of $\alpha - \beta$ is positive or $\alpha - \beta = 0$.

Examples

$$(1,2,0) >_{lex} (0,3,4) \Leftarrow (1,-1,-4)$$

$$(3,2,4) >_{lex} (3,2,1) \Leftarrow (0,0,3)$$

Behold!

$$x,y,z \xrightarrow{\text{rename}} x_1, x_2, x_3 \Rightarrow \begin{array}{ccccc} x & & y & & z \\ | & & | & & | \\ (1,0,0) & >_{lex} & (0,1,0) & >_{lex} & (0,0,1) \\ | & & | & & | \\ z & & y & & x \end{array}$$

$$x,y,z \xrightarrow{\text{rename}} x_3, x_2, x_1$$

There is $n!$ lex orders

pajdla@cmp.felk.cvut.cz

The lex ordering on $\mathbb{Z}^n_{\geq}$ is a monomial ordering

$<_{lex}$ is an ordering $(\alpha > \alpha\,;\ \alpha > \beta \,\&\, \beta > \gamma \Rightarrow \alpha > \gamma\,,\ \alpha > \beta \,\&\, \beta > \alpha \Rightarrow \alpha = \beta)$

(a) $\alpha - \alpha = 0 \Rightarrow \alpha >_{lex} \beta$

$\exists\, i, j \in \mathbb{Z}^n_{\geq 0}$ such that $(\alpha-\beta)_k = 0$ and $(\beta-\gamma)_m = 0$ for $k < i$, $m < j$ &

(b) $\alpha >_{lex} \beta\,,\ \beta >_{lex} \gamma \quad (\alpha-\beta)_i > 0 \;\&\; (\beta-\gamma)_j > 0$

$(\alpha-\gamma)_k = 0 \quad k = 1, \ldots, \min(i,j) - 1 \qquad \alpha_k = \beta_k = \gamma_k$

$(\alpha-\gamma)_{\min(i,j)} > 0 \quad \begin{cases} \min(i,j) = i & \alpha_i \geq \beta_i = \gamma_i \\ \min(i,j) = j & \alpha_j = \beta_j \geq \gamma_j \end{cases}$

$\Rightarrow \alpha >_{lex} \gamma$

(c) $\alpha >_{lex} \beta \;\&\; \beta >_{lex} \alpha \Rightarrow$ $\left.\begin{array}{l}\text{either } \alpha - \beta = 0 \text{ or} \\ \exists\, i \in \mathbb{Z}_{\geq 0}\ ((\alpha-\beta)_i > 0 \,\&\, (\beta-\alpha)_i > 0)\end{array}\right\} \Rightarrow \alpha - \beta = 0$

The lex ordering is a monomial ordering

(i) $\forall\, \alpha, \beta : \quad \alpha \underset{lex}{>} \beta$ or $\beta \underset{lex}{>} \alpha$:

$c = \alpha - \beta = 0 \Rightarrow \alpha = \beta$ or there is the first non-zero element c_i. If $c_i > 0$, then $\alpha \underset{lex}{>} \beta$, $\beta \underset{lex}{>} \alpha$ otherwise.

(ii) $\alpha \underset{lex}{>} \beta$ & $\gamma \in \mathbb{Z}^n_{\geq 0} \Rightarrow \alpha + \gamma \underset{lex}{>} \beta + \gamma$

$\alpha + \gamma - (\beta + \gamma) = \alpha - \beta$

(iii) $\forall\, \alpha : \quad \alpha \underset{lex}{>} 0$

$(\alpha - 0)_i \geq 0$

pajdla@cmp.felk.cvut.cz

a non-zero $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \dots, x_n]$ & a monomial ordering $>$

multidegree of f $\qquad \mathrm{multideg}(f) = \max_{>} (\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0)$

leading term $\longrightarrow$ $LT(f) = LC(f) \cdot LM(f)$

leading coefficient $\qquad$ leading monomial

$LC(f) = a_{\mathrm{multideg}(f)} \qquad LM(f) = x^{\mathrm{multideg}(f)}$

Example: $\quad f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \quad , \quad >_{lex}$

$$= 4x^{(1,2,1)} + 4x^{(0,0,2)} - 5x^{(3,0,0)} + 7x^{(2,0,2)}$$

$\mathrm{multideg}(f) = (3,0,0)$

$LC(f) = -5$

$LM(f) = x^3$

$LT(f) = -5x^3$