PKR Lab-09 Solution

Algorithms

Algorithm 1: Multivariate Polynomial Division Algorithm

Input: $f, F = (f_1, \dots, f_s), \geq$ (monomial ordering)
Output: $(q_1, \dots, q_s), r$ such that $f = \sum_{i=1}^{s} q_i f_i + r$, $\mathrm{LT}_{\geq}(r)$ is not divisible by any of $\mathrm{LT}_{\geq}(f_i)$ or $r = 0$

$q_1 \leftarrow \cdots \leftarrow q_s \leftarrow r \leftarrow 0$
$p \leftarrow f$
while $p \neq 0$ **do**
  $i \leftarrow 1$
  divisionoccured $\leftarrow$ **False**
  while $i \leq s$ **and not** divisionoccured **do**
    if $\mathrm{LT}_{\geq}(f_i)$ divides $\mathrm{LT}_{\geq}(p)$ **then**
      $q_i \leftarrow q_i + \frac{\mathrm{LT}_{\geq}(p)}{\mathrm{LT}_{\geq}(f_i)}$
      $p \leftarrow p - \frac{\mathrm{LT}_{\geq}(p)}{\mathrm{LT}_{\geq}(f_i)} f_i$
      divisionoccured $\leftarrow$ **True**
    else
      $i \leftarrow i + 1$
  if not divisionoccured **then**
    $r \leftarrow r + \mathrm{LT}_{\geq}(p)$
    $p \leftarrow p - \mathrm{LT}_{\geq}(p)$
return $(q_1, \dots, q_s), r$

Tasks

Task 1. *Consider a polynomial $f = y^5 + 2xy^2 + x$. Order the terms of f (from largest to smallest) according to the lexicographic monomial ordering for the ordering of variables $x > y$.*

Solution: For $f = \sum_{\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geq 0}} a_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}$ we define

$$\mathrm{terms}(f) \stackrel{\text{def}}{=} \{a_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}} \mid a_{\boldsymbol{\alpha}} \neq 0\}.$$

For f given in the task we have

$$\mathrm{terms}(f) = \{y^5, 2xy^2, x\}.$$

We first compare y^5 with $2xy^2$. We have $y^5 = \mathbf{x}^{\boldsymbol{\alpha}} = (x, y)^{(0,5)}$ and $xy^2 = \mathbf{x}^{\boldsymbol{\beta}} = (x, y)^{(1,2)}$. Since the left most nonzero element of $\boldsymbol{\alpha} - \boldsymbol{\beta} = (-1, 3)$ is not positive and $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$, then $\mathbf{x}^{\boldsymbol{\beta}} \geq_{\text{lex}} \mathbf{x}^{\boldsymbol{\alpha}}$, or

$$2xy^2 \geq_{\text{lex}} y^5.$$

Remark. *In other words, in order to compare two monomials $\mathbf{x}^{\boldsymbol{\alpha}}$ and $\mathbf{x}^{\boldsymbol{\beta}}$ w.r.t. $\geq_{\text{lex}}$ we compare the exponents in individual variables starting from the largest variable towards the lowest variable: if $\alpha_j > \beta_j$, then $\mathbf{x}^{\boldsymbol{\alpha}} \geq_{\text{lex}} \mathbf{x}^{\boldsymbol{\beta}}$; if $\alpha_j < \beta_j$, then $\mathbf{x}^{\boldsymbol{\beta}} \geq_{\text{lex}} \mathbf{x}^{\boldsymbol{\alpha}}$; if $\alpha_j = \beta_j$, then we move to comparing the exponents α_{j+1} and β_{j+1} for the next variable.*

Next we compare x with y^5 and x with $2xy^2$:

$$x \geq_{\text{lex}} y^5, 2xy^2 \geq_{\text{lex}} x.$$

Then

$$f = 2xy^2 + x + y^5$$

with the terms written in the decreasing order. $\square$

Task 2. *Consider a monomial ordering $x \geq_{\text{lex}} y$. Divide a polynomial $f = x^2 + xy + x + y^3 + 1$ by an ordered tuple of polynomials*

$$F = (f_1, f_2, f_3) = (xy + x + 1, y^2 + 1, xy + 1)$$

using $\geq_{\text{lex}}$. Consider a permuted tuple $F' = (f_3, f_2, f_1)$ of F and divide f by F' using $\geq_{\text{lex}}$. Compare the two remainders.

Solution: We apply Algorithm 1. We represent f as a sum $p + \sum_i q_i \cdot f_i + r$ during every iteration of the **while** $p \neq 0$ **do** loop:

$$\begin{aligned}
\underbrace{x^2+xy+x+y^3+1}_{f} &= \underbrace{x^2+xy+x+y^3+1}_{p} + \underbrace{0}_{q_1} \cdot \underbrace{(xy+x+1)}_{f_1} + \underbrace{0}_{q_2} \cdot \underbrace{(y^2+1)}_{f_2} + \underbrace{0}_{q_3} \cdot \underbrace{(xy+1)}_{f_3} + \underbrace{0}_{r} \\
&= \underbrace{xy+x+y^3+1}_{p} + \underbrace{0}_{q_1} \cdot \underbrace{(xy+x+1)}_{f_1} + \underbrace{0}_{q_2} \cdot \underbrace{(y^2+1)}_{f_2} + \underbrace{0}_{q_3} \cdot \underbrace{(xy+1)}_{f_3} + \underbrace{x^2}_{r} \\
&= \underbrace{y^3}_{p} + \underbrace{1}_{q_1} \cdot \underbrace{(xy+x+1)}_{f_1} + \underbrace{0}_{q_2} \cdot \underbrace{(y^2+1)}_{f_2} + \underbrace{0}_{q_3} \cdot \underbrace{(xy+1)}_{f_3} + \underbrace{x^2}_{r} \\
&= \underbrace{-y}_{p} + \underbrace{1}_{q_1} \cdot \underbrace{(xy+x+1)}_{f_1} + \underbrace{y}_{q_2} \cdot \underbrace{(y^2+1)}_{f_2} + \underbrace{0}_{q_3} \cdot \underbrace{(xy+1)}_{f_3} + \underbrace{x^2}_{r} \\
&= \underbrace{0}_{p} + \underbrace{1}_{q_1} \cdot \underbrace{(xy+x+1)}_{f_1} + \underbrace{y}_{q_2} \cdot \underbrace{(y^2+1)}_{f_2} + \underbrace{0}_{q_3} \cdot \underbrace{(xy+1)}_{f_3} + \underbrace{x^2-y}_{r}
\end{aligned}$$

We now divide f by F':

$$\begin{aligned}
\underbrace{x^2+xy+x+y^3+1}_{f} &= \underbrace{x^2+xy+x+y^3+1}_{p} + \underbrace{0}_{q_1} \cdot \underbrace{(xy+1)}_{f_1} + \underbrace{0}_{q_2} \cdot \underbrace{(y^2+1)}_{f_2} + \underbrace{0}_{q_3} \cdot \underbrace{(xy+x+1)}_{f_3} + \underbrace{0}_{r} \\
&= \underbrace{xy+x+y^3+1}_{p} + \underbrace{0}_{q_1} \cdot \underbrace{(xy+1)}_{f_1} + \underbrace{0}_{q_2} \cdot \underbrace{(y^2+1)}_{f_2} + \underbrace{0}_{q_3} \cdot \underbrace{(xy+x+1)}_{f_3} + \underbrace{x^2}_{r} \\
&= \underbrace{x+y^3}_{p} + \underbrace{1}_{q_1} \cdot \underbrace{(xy+1)}_{f_1} + \underbrace{0}_{q_2} \cdot \underbrace{(y^2+1)}_{f_2} + \underbrace{0}_{q_3} \cdot \underbrace{(xy+x+1)}_{f_3} + \underbrace{x^2}_{r} \\
&= \underbrace{y^3}_{p} + \underbrace{1}_{q_1} \cdot \underbrace{(xy+1)}_{f_1} + \underbrace{0}_{q_2} \cdot \underbrace{(y^2+1)}_{f_2} + \underbrace{0}_{q_3} \cdot \underbrace{(xy+x+1)}_{f_3} + \underbrace{x^2+x}_{r} \\
&= \underbrace{-y}_{p} + \underbrace{1}_{q_1} \cdot \underbrace{(xy+1)}_{f_1} + \underbrace{y}_{q_2} \cdot \underbrace{(y^2+1)}_{f_2} + \underbrace{0}_{q_3} \cdot \underbrace{(xy+x+1)}_{f_3} + \underbrace{x^2+x}_{r} \\
&= \underbrace{0}_{p} + \underbrace{1}_{q_1} \cdot \underbrace{(xy+1)}_{f_1} + \underbrace{y}_{q_2} \cdot \underbrace{(y^2+1)}_{f_2} + \underbrace{0}_{q_3} \cdot \underbrace{(xy+x+1)}_{f_3} + \underbrace{x^2+x-y}_{r}
\end{aligned}$$

We notice that the remainder r of the division (as well as the quotient polynomials q_j and the number of iterations) depend on the order of the divisors f_j. □