Polynomials

We will consider polynomials in n unknowns $x_1, x_2, \dots, x_n$ with rational coefficients $a_1, a_2, \dots, a_n$

Polynomials are linear combinations of a finite number of monomials

Monomials : $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$, where α_i are non-negative integers

$\alpha_i \in \mathbb{Z}_{\geq 0}$ - exponents

To simplify the notation we will write

$$x^{\alpha} = x^{\alpha_1} \dots x_n^{\alpha_n}$$

for n-touple of exponents $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$

N-touple α is called multidegree of monomial x^{α}

e.g. for $\alpha = (2,0,1)$ we get $x^{\alpha} = x_1^2 x_2^0 x_3 = x_1^2 x_3$

We define the total degree of a non-zero monomial with exponent $\alpha = (\alpha_1, \dots, \alpha_n)$ as $d = \alpha_1 + \alpha_2 + \dots + \alpha_n$

The total degree <u>deg(f)</u> of a polynomial f is the maximum of the total degrees of its monomials (zero polynomial has no degree)

With this notation <u>polynomials</u> with rational coefficients can be written in the form:

$$f = \sum_{\alpha} a_\alpha x^\alpha \qquad a_\alpha \in \mathbb{Q}$$

where the sum is over a finite set of n-toupees $\alpha \in \mathbb{Z}_{\geq 0}^n$

The <u>set of all polynomials</u> in unknowns $x_1, x_2, \dots, x_n$ with rational coefficients will be denoted $\mathbb{Q}[x_1, \dots, x_n]$

There is an infinite (countable) number of monomials

They can be ordered using a total ordering (linear ordering)
(ordering where every two elements are comparable)

Polynomials with rational coefficients can be also understood as complex functions
We can evaluate polynomial f on point $\vec{p} \in \mathbb{C}^n$

$$f(\vec{p}) = \left(\sum_\alpha a_\alpha x^\alpha\right)(\vec{p}) = \sum_\alpha a_\alpha x^\alpha(\vec{p}) = \sum_\alpha a_\alpha \vec{p}^{\,\alpha} = \sum_\alpha a_\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

Evaluated polynomial is a linear combination of the evaluated monomials

Division of terms

$\alpha, \beta \in \mathbb{Z}_{\geq}^n$ $\qquad a_\alpha, b_\alpha \in \mathbb{Q}[\mathfrak{u}]$

$x^\alpha, x^\beta \in \mathbb{Q}[x_1, \dots, x_n]$ - monomials

$$a_\alpha x^\alpha \ \underline{\text{divides}}\ b_\beta x^\beta \stackrel{\text{def}}{\equiv} \beta_i - \alpha_i \geq 0 \quad , \quad i = 1, \dots, n$$

If $a_\alpha x^\alpha$ divides $b_\beta x^\beta$ then there is exactly one monomial

$$c_\gamma x^\gamma = \frac{b_\beta}{a_\alpha} x^{\beta - \alpha}$$

For monomials in one variable $\alpha, \beta \in \mathbb{Z}_{\geq 0}$

Univariate polynomials

Polynomials in a single unknown are often called <u>univariate polynomials</u>

$\Rightarrow$ - α is a single number

- The total degree $\deg(f)$ of f is then called <u>degree</u>

- The set of all polynomials in a single unknown x over rational numbers $\mathbb{Q}[x]$ forms a ring
- Polynomials are almost as real numbers except for the division
- Polynomials <u>can't in general be divided</u>

- In fact polynomials behave in many aspects as whole numbers $\mathbb{Z}$

It is easy to introduce <u>long polynomial division</u> in the same way as it is used in whole numbers

<u>Leading term</u> : of a non-zero polynomial

$$f(x) = \underset{\neq 0}{a_m} x^m + a_{m-1} x^{m-1} + \dots + a_0 \quad \in \mathbb{Q}[x]$$

$$LT(f) = a_m x^m \equiv \underline{\text{leading term}}$$

Example: $f(x) = 2x^3 - 4x + 3 \Rightarrow LT(f) = 2x^3$

" <u>Division theorem</u> "

Consider polynomials $f, g \in \mathbb{Q}[x]$ $\quad g \neq 0$

Then there are <u>unique</u> polynomials $q, r \in \mathbb{Q}[x]$ such that

$$f = q \cdot g + r \quad \text{with} \quad \deg(r) < \deg(g)$$

$$\text{or} \quad r = 0$$

q - is the quotient

r - is the reminder (of f on division by g)

One often writes $f \equiv r \pmod g$ $\quad (r = f \bmod g)$

Example: $f = 2x^3 - 4x + 3$ $\quad g(x) = x - 1$

$$f : g = (2x^2 + 2x - 2)(x - 1) + 1$$

Notice $\deg(f) = \deg(LT(f))$

$LT(g)$ divides $LT(f) \iff \deg(LT(g)) \leq \deg(LT(f)) \iff \deg(g) \leq \deg(f)$

<u>Proof</u>: of Division theorem $\Rightarrow$ <u>Division algorithm</u>

<u>Input</u>: g, f

<u>Output</u>: q, r

$q := 0$

$r := f$

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

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

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

}

$f = 2x^3 - 4x + 3$	$q = 0$	$q = 2x^2$	$q = 2x^2 + 2x$	$q = 2x^2 + 2x - 2$
$g = x - 1$	$r = 2x^3 - 4x + 3$	$r = 2x^2 - 4x + 3$	$r = -2x + 3$	$r = 1$

$$f = (2x^2 + 2x - 2)(x - 1) + 1$$

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 $r_i = a_0 x^m + a_1 x^{m-1} + \dots + a_m$
$g = b_0 x^\ell + b_1 x^{\ell-1} + \dots + b_\ell$
with $m \geq \ell$ $(LT(g)$ divides $LT(r_i))$

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

$$= (a_1 x^{m-1} + \dots \quad) - \left(\frac{a_0}{b_0} b_1 x^{m-1} + \dots \quad\right)$$

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

and therefore
- either $r_{i+1} = 0$ (if all coeficients vanish)
- or $\deg(r_{i+1}) \leq m-1 < m = \deg(r_i)$

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

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

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

Not so simple with more variables

Consider xy^2, x^2y - neither one divides the other

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

$\Downarrow$

total degrees does not define an ordering of monomials

by degrees $\to$ partial ordering

to have a total ordering we have to extend this

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

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

(ii) $\alpha > \beta$ & $\gamma \in \mathbb{Z}^n_{\geq 0} \Rightarrow \alpha + \gamma > \beta + \gamma$ $\quad$ ($\deg(m_1) < \deg(m_2) \Rightarrow \deg(m_1 . m) < \deg(m_2 m)$)

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

We write $x^\alpha > x^\beta \overset{\text{def.}}{\equiv} \alpha > \beta$

<u>Lexicographic ordering</u>

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

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

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

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

Lex orders monomials as words in dictionary

An important parameter of $<_{lex}$ ordering is the order of unknowns (order of letters)

e.g $\quad xy^2z = x.y.y.z <_{lex} x.y.z.z = xyz^2 \quad$ if $\quad x < y < z$

$xyz^2 = xyzz <_{lex} xyyz = xy^2z \quad$ if $\quad z < y < x$

There are $n!$ possible $<_{lex}$ orderings when dealing with n unknowns

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

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

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

b) $\alpha >_{lex} \beta$, $\beta >_{lex} \gamma$

$\Rightarrow$ $\exists$ $i, j \in \mathbb{Z}^n_{\geq 0}$ such that

$(\alpha-\beta)_h = 0$ and $(\beta-\gamma)_m = 0$ for $h < i$, $m < j$ & $(\alpha-\beta)_i > 0$ & $(\beta-\gamma)_j > 0$

$(\alpha-\gamma)_h = 0$ $\quad h = 1, \dots, \min(i,j)-1$ $\quad \alpha_h = \beta_h = \gamma_h$

$(\alpha-\gamma)_{\min(i,j)} > 0$ $\left\langle \begin{array}{ll} \min(i,j) = i & \alpha_i \geq \beta_i = \gamma_i \\ \min(i,j) = j & \alpha_j = \beta_j \geq \gamma_j \end{array} \right.$

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

c) $\alpha >_{lex} \beta$ & $\beta >_{lex} \alpha$ $\Rightarrow$ either $\alpha - \beta = 0$

or $\exists$ $i \in \mathbb{Z}_{\geq 0}$ $(\alpha-\beta)_i > 0$ $\Rightarrow$ $\alpha - \beta = 0$

& $(\beta - \alpha)_i > 0$

The lex ordering is a monomial ordering

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

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

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

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

iii) $\forall \alpha : \alpha >_{lex} 0$

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

<u>Graded reverse Lex monomial ordering</u> (Grevlex) $<_{grevlex}$

is an extension of the partial ordering by the total degree to a total monomial ordering

Monomial <u>$x^\alpha <_{grevlex} x^\beta$</u> (as well as $\alpha <_{grevlex} \beta$ for exponents) when either <u>$\deg(\alpha) < \deg(\beta)$</u> or <u>$\deg(\alpha) = \deg(\beta)$</u> and the <u>last</u> non-zero element of $\beta - \alpha$ is <u>negative</u>

e.g $y^3z \sim (0,3,1) <_{grevlex} (1,1,2) \sim xyz^2$ since $0+3+1=4<5=1+2+2$

$xy^2z^2 \sim (1,2,2) <_{grevlex} (1,3,1) \sim xy^3z$ since $1+2+2=1+3+1$ and $(1,3,1)-(1,2,2)=(0,1,\underline{-1})$

A non-zero polynomial $f=\sum_{\alpha} a_\alpha x^\alpha \in \mathbb{Q}[x_1,\dots,x_n]$ & a monomial ordering $>$

<u>Multidegree of f</u> : $\text{multideg}(f) = \max_{>} (\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0)$

<u>Leading term</u> $\rightarrow$ $LT(f) = LC(f) . LM(f)$

leading coefficient $LC(f) = a_{\text{multideg}(f)}$

leading monomial $LM(f) = x^{\text{multideg}(f)}$

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

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

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

$LC(f) = 5$ $\quad LM(f) = x^3$ $\quad LT(f) = -5x^3$

Polynomial division with more divisors in more variables

Division by more then one polynomial

$$f = 3x^4 - x^2 + 2x \quad , \quad f_1 = x-1 \quad , \quad f_2 = x^2+1$$

$$\begin{aligned}
f &= 0.(x-1) + 0(x^2+1) + 3x^4 - x^2 + 2x &+ 0 \\
&= 3x^3(x-1) + 0(x^2+1) + 3x^3 - x^2 + 2x &+ 0 \\
&= (3x^3+3x^2)(x-1) + 0(x^2+1) + 2x^2 + 2x &+ 0 \\
&= (3x^3+3x^2+2x)(x-1) + 0.(x^2+1) + 4x &+ 0 \\
&= (3x^3+3x^2+2x+4)(x-1) + 0.(x^2+1) &+ 4
\end{aligned}$$

$$\begin{aligned}
&= 3x(x^2+1) + 0.(x-1) - x^2 - x &+ 0 \\
&= (3x-1)(x^2+1) + 0.(x-1) - x + 1 &+ 0 \\
&= (3x-1)(x^2+1) - 1.(x-1) &+ 0
\end{aligned}$$

We see that $f:(f_1, f_2) \neq f:(f_2, f_1) \Rightarrow f:\{f_1, f_2\}$ is not well defined

"Divison theorem" for more than one divisor in $k[x_1, \dots, x_n]$

Let $>$ be a monomial order on $\mathbb{Z}^n_{\geq 0}$ and $F = (f_1, \dots, f_s)$ an ordered s-touple of $f_i \in k[x_1, \dots, x_n]$. Then every $f \in k[x_1, \dots, x_n]$ can be written as:

$$f = a_1 f_1 + \dots + a_s f_s + r$$

$a_i, r \in k[x_1, \dots, x_n]$ and

either $r = 0$

or none of the monomials of r is divisible by any of $LT(f_1), \dots, LT(f_s)$

Furthermore $a_i f_i \neq 0 \Rightarrow \text{multidegree}(f) \geq \text{multidegree}(a_i f_i)$

$r \equiv$ reminder of f on division by F $\qquad r = \overline{f}^F$

"<u>Division algorithm</u>" for more than one divisor in $k[x_1, \dots, x_n]$

<u>Input</u> : $F = (f_1, \dots, f_s)$, f

<u>Output</u> : $a_1, \dots, a_s, r = \overline{f}^F$

$a_1 := a_2 := \dots := a_s := r := 0$, $p := f$

WHILE $p \neq 0$ DO

{ $i := 1$

divisionoccured := FALSE

WHILE $i \leq s$ AND divisionoccured = FALSE DO

{ IF $LT(f_i)$ divides $LT(p)$ THEN

{ $a_i := a_i + \frac{LT(p)}{LT(f_i)}$

$p := p - \frac{LT(p)}{LT(f_i)} \cdot f_i$

divisionoccured := TRUE }

ELSE { $i := i+1$ } }

IF divisionoccured = FALSE THEN

{ $r := r + LT(p)$

$p := p - LT(p)$ }

}

[Proof as for 1 variable

degree $\to$ multidegree

$r \to p$]

Example

$x >_{lex} y$ $\qquad f = \underset{(1,2)}{xy^2} + \underset{(1,0)}{x} + \underset{(0,0)}{1}$, $\quad f_1 = \underset{(1,1)}{xy} + \underset{(0,0)}{1}$, $\quad f_2 = \underset{(0,1)}{y} + \underset{(0,0)}{1}$

multidegrees

$$f = y.(xy+1) + \underset{(1,0)}{x} - \underset{(0,1)}{y} + \underset{(0,0)}{1} = \underset{a_1}{y}(xy+1) - \underset{a_2}{1}(y+1) + \underbrace{x+2}_{r}$$

$$f = \overbrace{0}^{a_1}.f_1 + \overbrace{0}^{a_2}.f_2 + \overbrace{xy^2 + x + 1}^{p} + \overbrace{0}^{r}$$

$$= y.f_1 + 0.f_2 + x - y + 1 + 0$$

$$= y.f_1 + 0.f_2 + -y + 1 + x$$

$$= y.f_1 - 1.f_2 + 2 + x$$

$$= y.f_1 - 1.f_2 + x + 2$$

The order of monomials in F matters!

$f = xy^2 - x$, $f_1 = xy + 1$, $f_2 = y^2 - 1$ $\quad >_{lex}$, $x >_{lex} y$

a) $f : (f_1, f_2)$

$$xy^2 - x = \underbrace{y}_{a_1}(xy+1) + \underbrace{0}_{a_2} \cdot (y^2 - 1) + \underbrace{(-x-y)}_{r}$$

b) $f : (f_2, f_1)$

$$xy^2 - x = \underbrace{x}_{a_1}(y^2-1) + \underbrace{0}_{a_2} \cdot (xy+1) + \underbrace{0}_{r}$$