Advanced Robotics

Lecture 5

pajdla@cmp.felk.cvut.cz

ALGEBRAIC EQUATIONS

pajdla@cmp.felk.cvut.cz

2000-1600 BC:

Old Babylonian Mathematics was able to solve quadratic equations

$$x^2 + b\, x = c$$

with positive c using the formula

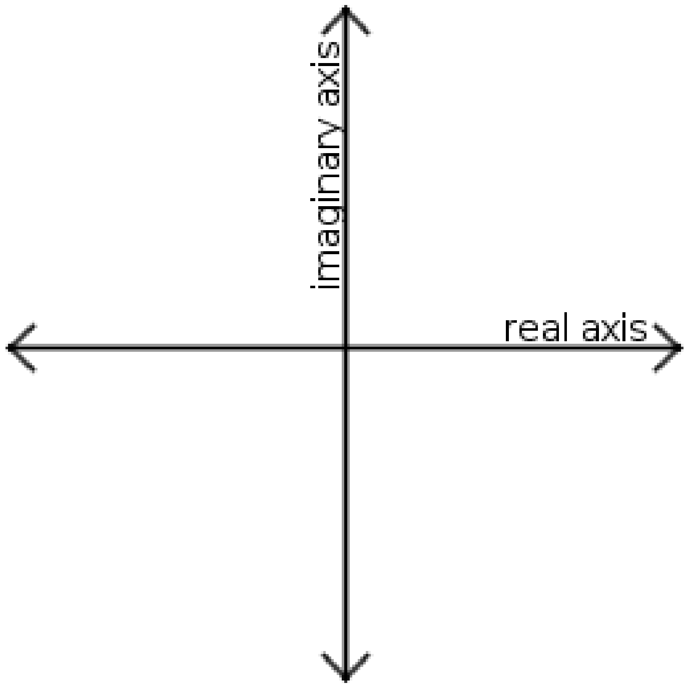
$$x = -\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + c}$$

and some simpler qubic equations, e.g.

$$x^3 + x^2 = c$$

820:

The word algebra is derived from operations described in the treatise written by the Persian mathematician Muhammad ibn Musa al-Kwarizmi titled Al-Kitab al-Jabr wa-l-Muqabala (meaning "The Compendious Book on Calculation by Completion and Balancing") on the systematic solution of linear and quadratic equations.



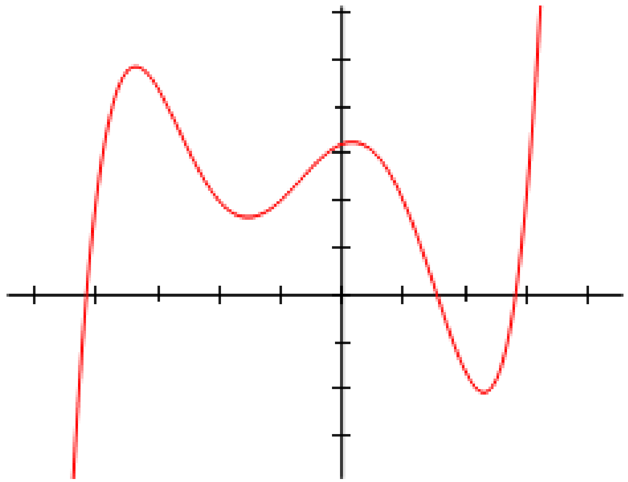
1608, Petrus Roth:

"A polynomial equation of degree n (with real coefficients) may have n solutions"

1806, Jean-Robert Argand:

A rigorous proof of the Fundamental Theorem of Algebra:

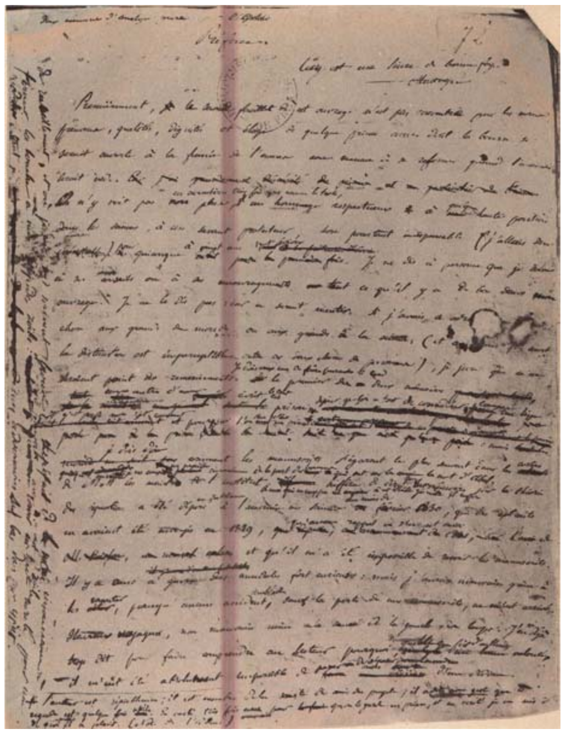
Every complex polynomial $p(z)$ *in one variable and of degree* $n \geq 1$ *has some complex root.*



1799 Paolo Ruffini,
1824 Niels Henrik Abel,
1832 Évariste Galois:

"Abel–Rufini Impossibility Theorem"

The solution of fifth degree algebraic equations cannot in all cases be expressed by starting with the coefficients and using only finitely many of the operations of addition, subtraction, multiplication, division and root extraction.



An example: $x^5 - x + 1 = 0$

1888, David Hilbert: "Finitness theorem"

Every ideal has a finite generating set

1964, Heisuke Hironaka: "Standard basis"

1965, Bruno Buchberger: "Gröbner basis"

→ an algorithm for solving systems polynomial equations

Algorithm:

$\{f_1, \dots, f_s\}$ polynomials in $k[x_1, \dots, x_n]$

Input: $F = (f_1, \dots, f_s)$ Output: a Groebner basis $G = (g_1, \dots, g_t)$

```
G := F
REPEAT
  { G' := G
    FOR each pair (p,q) ∈ {1,...,s}^2, p ≠ q DO
      { S = \overline{S(p,q)}^{G'}
        IF S ≠ 0 THEN { G := G ∪ {S} }
      }
  }
UNTIL G = G'
```


pajdla@cmp.felk.cvut.cz

One algebraic equation in one variable

pajdla@cmp.felk.cvut.cz

SOLVING 1 ALGEBRAIC EQUATION

1 equation, 1 variable $\rightarrow$ companion matrix $\rightarrow$ eigenvalues

$$f(x) = x^3 + 4\,x^2 + x - 6 \;=\; -6 + 1\,x + 4\,x^2 + 1\,x^3$$

$$\mathtt{M}_x = \begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & -1 \\ 0 & 1 & -4 \end{bmatrix}$$

... a simple rule

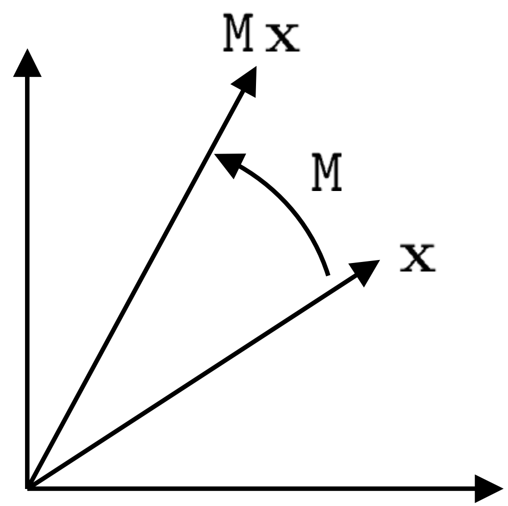
```
>> e=eig(Mx)
```

$$\mathtt{e} \;=\; \begin{bmatrix} 1 \\ -2 \\ -3 \end{bmatrix} \qquad x_1 = 1,\; x_2 = -2,\; x_3 = -3$$

It works when eig works, i.e. order 100 in Matlab is often OK.

SOLVING 1 ALGEBRAIC EQUATION

Linear maping $\quad \mathtt{M} \in \mathbb{R}^{n \times n}$



Eigenvalues $\quad \mathtt{M}\,\mathbf{x} = \lambda\,\mathbf{x}$

$$\Updownarrow$$

$$\mathtt{M}\,\mathbf{x} - \lambda\,\mathbf{x} = 0$$

$$\Updownarrow$$

$$\mathtt{M}\,\mathbf{x} - \lambda\,\mathtt{I}\,\mathbf{x} = 0$$

$$\Updownarrow$$

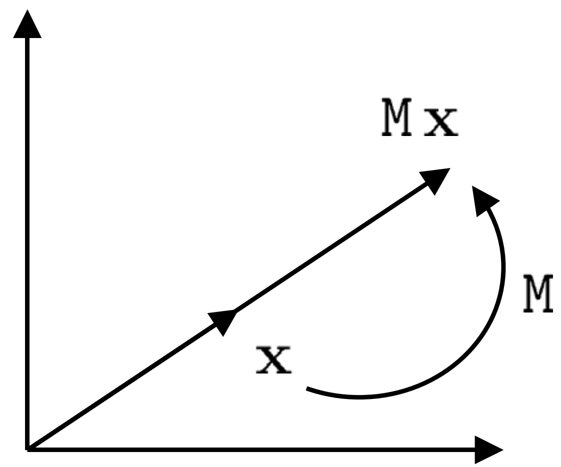
$$(\mathtt{M} - \lambda\,\mathtt{I})\,\mathbf{x} = 0$$

$$\mathbf{x} \neq 0 \;\Rightarrow\; \Updownarrow$$

$$\operatorname{rank}(\mathtt{M} - \lambda\,\mathtt{I}) < n$$

$$\Updownarrow$$

$$\det(\mathtt{M} - \lambda\,\mathtt{I}) = 0$$



SOLVING 1 ALGEBRAIC EQUATION

algebraic equation

$$f(x) = x^4 + a_3\,x^3 + a_2\,x^2 + a_1\,x + a_0 = \det(-\mathtt{M} + x\,\mathtt{I})$$

$$-\mathtt{M} + x\,\mathtt{I} = \begin{bmatrix} x & & & a_0 \\ -1 & x & & a_1 \\ & -1 & x & a_2 \\ & & -1 & x + a_3 \end{bmatrix}$$

$$f(x) = x^4 + a_3\,x^3 + a_2 x^2 + a_1 x + a_0$$

Polynomials in one variable

Leading term: a non-zero polynomial

$$f(x) = \underbrace{a_m x^m}_{} + a_{m-1} x^{m-1} + \cdots + a_0 \quad \in k[x]$$

$a_m \neq 0$ $\quad\quad$ $LT(f) = a_m x^m$ $\equiv$ the leading term

Example:

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

pajdla@cmp.felk.cvut.cz

Division of terms

$\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, $a_\alpha, b_\beta \in k$, $x^\alpha, x^\beta \in k[x_1, \dots, x_n]$ monomials

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

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

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

such that $b_\beta x^\beta = a_\alpha x^\alpha \cdot c_\gamma \cdot x^\gamma$

pajdla@cmp.felk.cvut.cz

"Division" of polynomials in one variable

polynomials cannot be divided but can be "divided"

$$f : g \overset{\text{def}}{\equiv} f = q\,g + r \,,\quad r = 0 \vee \deg(r) < \deg(g)$$

Example $f = 2x^3 - 4x + 3$, $g(x) = x - 1$

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

$$= (2x^2 + 2x)(x-1) - 2x + 3 = \underbrace{(2x^2+2x-2)}_{q}(x-1) + \underbrace{1}_{r}$$

notice that: $\deg(f) = \deg(LT(f))$

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

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

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

{

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

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

}

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 $m \geq l$

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

pajdla@cmp.felk.cvut.cz

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

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

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

and therefore we see that

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

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

Monomial ordering

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

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

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

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

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

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

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

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

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

pajdla@cmp.felk.cvut.cz

Lexicographic order

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

$\alpha >_{lex} \beta$ 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! $x,y,z \xrightarrow{\text{rename}} x_1, x_2, x_3 \Rightarrow$

$$\begin{array}{ccccc} x & & y & & z \\ | & & | & & | \\ (1,0,0) & >_{lex} & (0,1,0) & >_{lex} & (0,0,1) \\ | & & | & & | \\ z & & y & & x \end{array}$$

There is $n!$ lex orders

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

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

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

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

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

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

(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) $\forall\, \alpha, \beta: \quad \alpha >_{lex} \beta$ 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 $\alpha >_{lex} \beta$, $\beta >_{lex} \alpha$ otherwise.

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

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

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

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

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 $\quad$ $\text{multideg}(f) = \max_{>} (\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0)$

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

leading coefficient $\quad$ leading monomial

$LC(f) = a_{\text{multideg}(f)}$ $\quad$ $LM(f) = x^{\text{multideg}(f)}$

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

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

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

$LC(f) = -5$

$LM(f) = x^3$

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

pajdla@cmp.felk.cvut.cz

Polynomial division with more divisors in more variables

"Division" by more than one polynomial

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

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

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

pajdla@cmp.felk.cvut.cz

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

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

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

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

$r = 0$ or none of the monomials of r is divisible by any of $LT(f_1), \dots, LT(f_s)$.

Furthermore

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

$r \equiv$ remainder of f on division by F ... $r = \overline{f}^F$

with the notation $F = (f_1, \dots, f_s)$

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

Input: $F=(f_1,\dots,f_s)$, f Output: $a_1,\dots,a_s,r \equiv \overline{f}^F$

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

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 → multidegree

$r \to p$

pajdla@cmp.felk.cvut.cz

Example

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

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

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

$$= y \cdot f_1 + 0 \cdot f_2 + x - y + 1 + 0$$

$$= y \cdot f_1 + 0 \cdot f_2 \qquad - y + 1 + x$$

$$= y \cdot f_1 - 1 \cdot f_2 \qquad + 2 + x$$

$$= y \cdot f_1 - 1 \cdot f_2 \qquad + x + 2$$

Example:

$$f = xy^2 - x \qquad f_1 = xy + 1 \qquad f_2 = y^2 - 1$$

$>_{lex}$, $x >_{lex} y$

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) $f : (f_2, f_1)$

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

The order of polynomials in F matters

Affine varieties

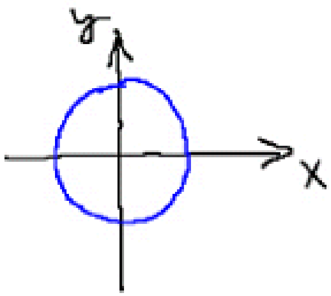
$f_k(x_1, x_2, \dots, x_n)$ ... algebraic equations

Algebraic variety $\equiv$ the set of points for which all equations f_k are satisfied

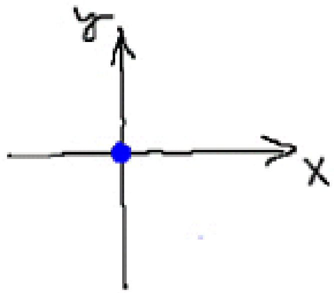
$$V = \{(x_1, x_2, \dots, x_n) \mid \underline{f_k(x_1, x_2, \dots, x_n) = 0}, \; k = 1, 2, \dots, s\}$$

Examples:

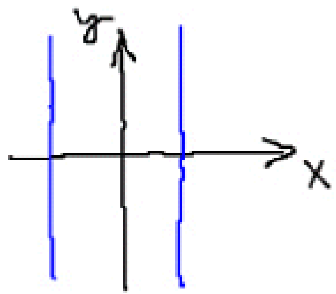
$\{x^2 + y^2 = 2\}$



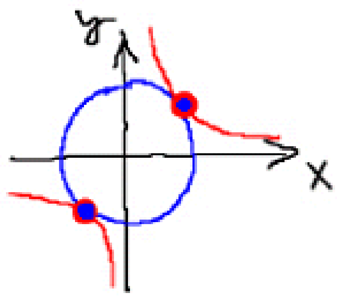
$\{x^2 + y^2 = 0\}$



$\{x^2 = 1\}$



$\{x^2 + y^2 = 1, \; xy = 1\}$



For solving IKU, we are interested in situations when there is a finite number of solutions $\equiv$ finite affine varieties

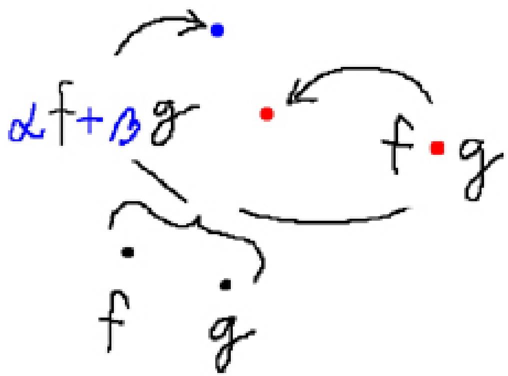
Notice that:

1) $f(a_1,a_2,\dots,a_n)=0$ & $g\in k[x_1,x_2,\dots,x_n] \Rightarrow (f\cdot g)(a_1,a_2,\dots,a_n)=0$

2) $f(a_1,a_2,\dots,a_n)=0$ & $g(a_1,a_2,\dots,a_n)=0 \Rightarrow (f+g)(a_1,a_2,\dots,a_n)=0$

$\Rightarrow$ there is an infinite number of different sets of algebraic equations defining the same variety

new "true" equations can be generated by algebraic operations with polynomials



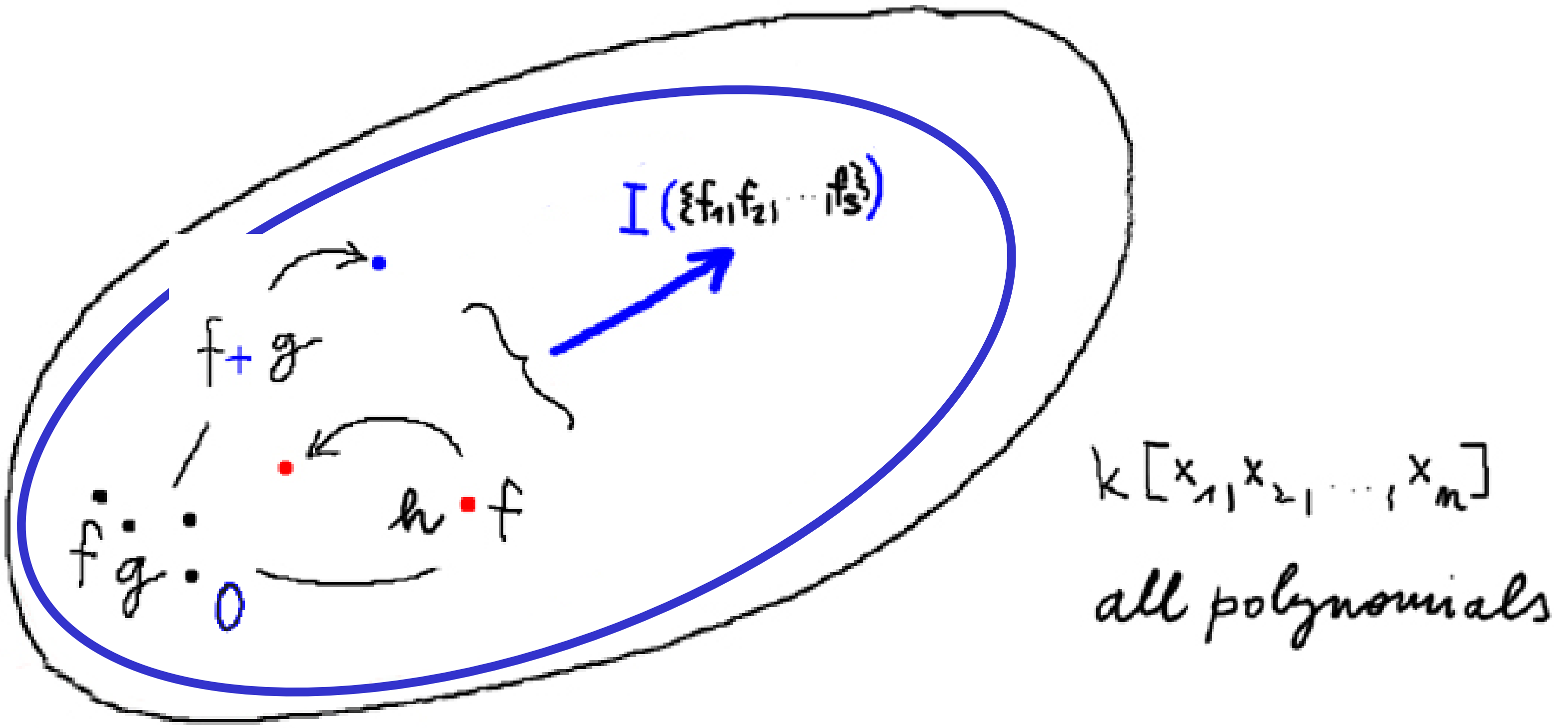
Ideal generated by polynomials

Ideal: A subset $I \subseteq k[x_1, x_2, \dots, x_n]$ is an ideal if it satisfies:

(i) $0 \in I$

(ii) $f, g \in I \Rightarrow f + g \in I$

(iii) $f \in I$ & $h \in k[x_1, x_2, \dots, x_n] \Rightarrow h \cdot f \in I$



Ideal generated by a variety

Theorem: Let V be an affine variety. Then

$$I(V) = \{f \in k[x_1, \ldots, x_n] \,|\, f(x) = 0, \forall x \in V\}$$

is an ideal.

Proof:

(i) $0 \in I$
(ii) $f, g \in I \Rightarrow f + g \in I$
(iii) $f \in I$ & $h \in k[x_1, x_2, \ldots, x_n] \Rightarrow h \cdot f \in I$

(i) $0(x) = 0$

(ii) $f(x) = 0$ & $g(x) = 0$
$\Rightarrow (f + g)(x) = f(x) + g(x) = 0 + 0 = 0$

(iii) $f(x) = 0$
$\Rightarrow (f \cdot h)(x) = f(x) \cdot h(x) = 0 \cdot h(x) = 0$

pajdla@cmp.felk.cvut.cz

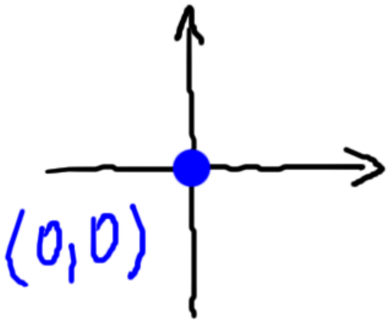
Ideal generated by polynomials and by the corresponding variety

polynomials		Variety generated by $\{f_1, f_2, \dots, f_s\}$
$\{f_1, f_2, \dots, f_s\}$	$\longrightarrow$	$V(\{f_1, f_2, \dots, f_s\})$
$\downarrow$		$\downarrow$
$I(\{f_1, f_2, \dots, f_s\})$	$\subseteq$	$I(V)$
The ideal generated by polynomials $\{f_1, f_2, \dots, f_s\}$	$\uparrow$	The ideal generated by variety V
	?	

pajdla@cmp.felk.cvut.cz

Example

$$\begin{array}{ccc} \{x^2, y^2\} & \longrightarrow & V(\{x^2, y^2\}) \\ \downarrow & & \downarrow \\ I(\{x^2, y^2\}) & \subseteq & I(V(\{x^2, y^2\})) \end{array}$$



$$\{x^2, y^2\}$$

$$V(\{x^2, y^2\}) = \{(0,0)\}$$

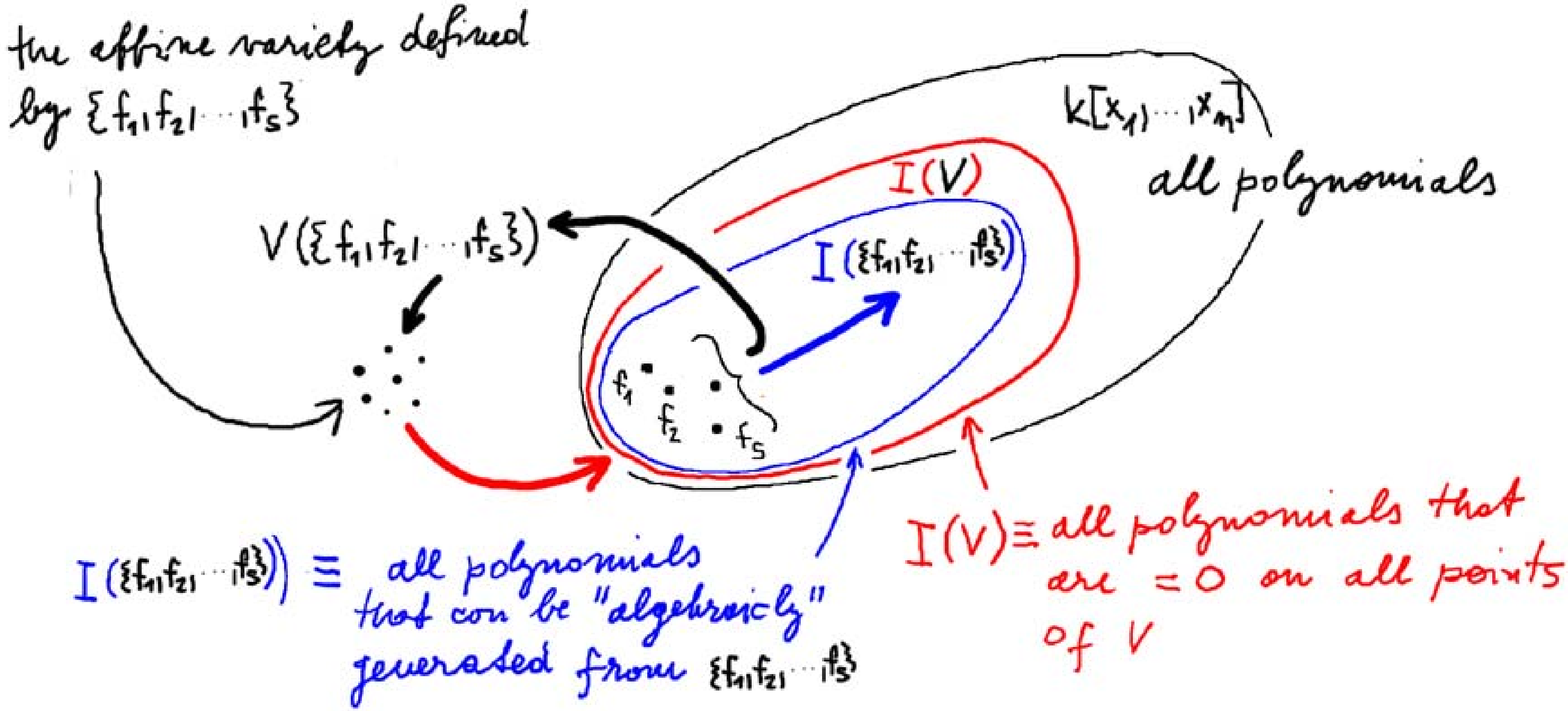
$$I(V(\{x^2, y^2\})) = I(\{x, y\})$$

$$I(\{x^2, y^2\}) \subset I(\{x, y\})$$

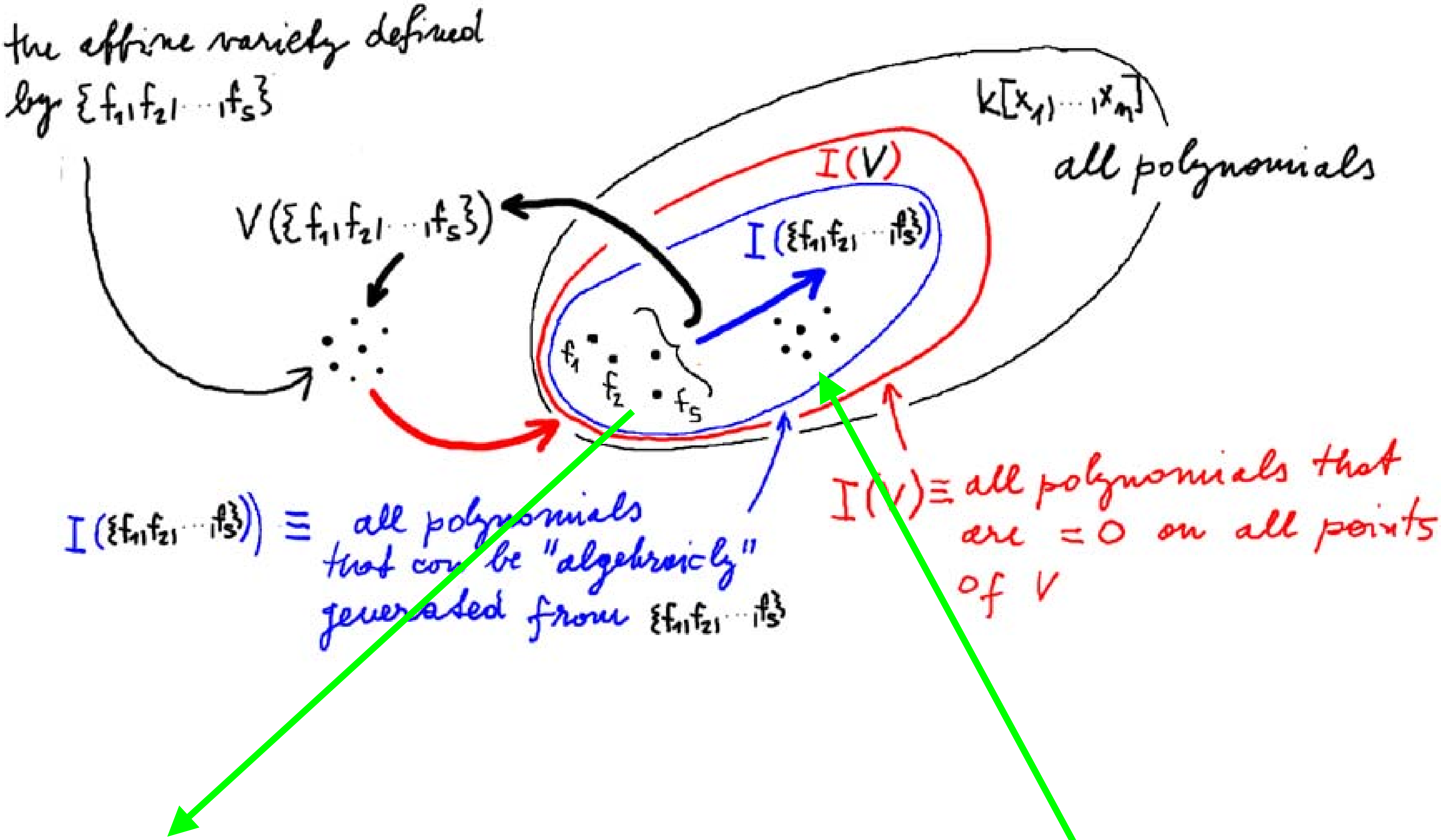
because $x, y \in I(\{x, y\})$ but $x, y \notin I(\{x^2, y^2\})$

as every ~~0~~ $h_1(x,y)\,x^2 + h_2(x,y)\,y^2$ has total degree at least two

The complete picture



Groebner basis is a special basis of the Ideal



Basis: $B = \{f_1, f_2, \ldots, f_s\}$	$\xrightarrow{\text{Algebraic manipulation}}$	Groebner basis w.r.t. $<_{lex}$: $G = \{g_1, g_2, \ldots, g_n\}$

pajdla@cmp.felk.cvut.cz

Reading the solution out from a Groebner basis

Theorem 3: Let G be a Groebner basis constructed by the Buchberger algorithm w.r.t. $x_1 >_{lex} \cdots >_{lex} x_n$ from polynomials $\{f_1, \ldots, f_s\} \in \mathbb{C}[x_1, \ldots, x_n]$ for which equations $\{f_i = 0\}_{i=1,\ldots,s}$ have a finite number of solutions. Then G contains a polynomial $g \in \mathbb{C}[x_n]$.

There is often even more:

G often consists of a set of polynomials

$g_n(x_n)$

$g_{n-1}(x_n, x_{n-1})$

$g_{n-2}(x_n, x_{n-1}, x_{n-2})$

$\vdots$

$g_1(x_n, x_{n-1}, x_{n-2}, \ldots, x_1)$

pajdla@cmp.felk.cvut.cz

A working definition of a

Groebner basis (of an ideal)

(A basis) $G = (g_1, \dots, g_t)$ (of an ideal I) is a Groebner basis if the remainder on division of $f \in k[x_1, \dots, x_n]$ by G does not depend on the ordering of g_i in G.

Beware! only r is unique – a_i's need not be unique

Least common multiple of monomials

Let $x^\alpha, x^\beta \in k[x_1, \ldots, x_n]$ be monomials, then x^γ with

$\gamma_i = \max(\alpha_i, \beta_i)$, $i = 1, \ldots, n$ is

the **least common multiple** – $LCM(x^\alpha, x^\beta)$ – of x^α, x^β

Example: $x^\alpha = x y^3 z^2$, $x^\beta = y z^6$

$$\alpha = (1, 3, 2) \qquad \beta = (0, 1, 6)$$

$$\gamma = \max((1,3,2), (0,1,6)) = (1, 3, 6)$$

$$x^\gamma = x y^3 z^6$$

pajdla@cmp.felk.cvut.cz

The S-polynomial (designed to cancel the leading terms)

The S-polynomial of $f, g \in k[x_1, \ldots, x_n]$ is the (algebraic) combination

$$S(f,g) = \frac{\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} \cdot f - \frac{\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(g)} \cdot g$$

Example: $f = x^3y^2 - x^2y^3 + x, \quad g = 3x^4y + y^2 \in \mathbb{R}[x,y]$

with $x >_{lex} y$

$$S(f,g) = \frac{\mathrm{LCM}(x^3y^2, x^4y)}{x^3y^2} \cdot f - \frac{\mathrm{LCM}(x^3y^2, x^4y)}{3x^4y} \cdot g = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} g$$

$$= x \cdot f - \frac{1}{3} y g = x^4y^2 - x^3y^3 + x^2 - x^4y^2 - \frac{1}{3}y^3 = -x^3y^3 + x^2 - \frac{1}{3}y^3$$

cancel

Characterization of Groebner bases in terms of S-polynomials

A set $G = \{g_1, \dots, g_t\}$ of polynomials in $k[x_1, \dots, x_n]$ is a Groebner basis if for all $i, j \in 1, \dots, t$, $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (with arbitrary but fixed order of g_k) is zero

Algorithm:

$\{f_1, \dots, f_s\}$ polynomials in $k[x_1, \dots, x_n]$

Input: $F = (f_1, \dots, f_s)$ Output: a Groebner basis $G = (g_1, \dots, g_t)$

```
G := F
REPEAT
  { G' := G
    FOR each pair (p,q) ∈ G', p ≠ q DO
      { S = \overline{S(p,q)}^{G'}
        IF S ≠ 0 THEN { G := G ∪ {S} }
      }
  }
UNTIL G = G'
```

Example: $k[x,y]$, $x >_{lex} y$ $F = (f_1, f_2) = (x^3 - 2xy, x^2y - 2y^2 + x)$

F is not GB: $S(f_1, f_2) = \frac{x^3y}{x^3} f_1 - \frac{x^3y}{x^2y} f_2 = y f_1 - x f_2 = -2xy^2 + 2xy^2 - x^2 = -x^2$

and $\overline{S(f_1, f_2)}^F = -x^2 \neq 0$

$G_1 = F \cup \{-x^2\} = (f_1, f_2, -x^2)$

$S(f_1, x^2) = \frac{x^3}{x^3} f_1 - \frac{x^3}{x^2} x^2 = -2xy$; $\overline{S(f_1, x^2)}^{G_1} = -2xy$

$S(f_2, x^2) = \frac{x^2y}{x^2y} f_2 - \frac{x^2y}{x^2} x^2 = -2y^2 + x$; $\overline{S(f_2, x^2)}^{G_1} = -2y^2 + x$

$G_2 = (f_1, f_2, -x^2, -2xy, x - 2y^2) = (f_1, f_2, f_3, f_4, f_5)$

$S(f_1, f_4) = \frac{x^3y}{x^3} f_1 - \frac{x^3y}{-2xy} f_4 = -2xy^2$; $\overline{S(f_1, f_4)}^{G_2} = 0$

$S(f_2, f_4) = \frac{x^2y}{x^2y} f_2 - \frac{x^2y}{-2xy} f_4 = x - 2y^2$; $\overline{S(f_2, f_4)}^{G_2} = 0$

$\vdots$

$S(f_4, f_5) = \frac{xy}{-2xy} f_4 - \frac{xy}{x} f_5 = 3y^3$; $\overline{3y^3}^{G_2} = 3y^3$

$$G_3 = (\underbrace{x^3 - 2xy}_{f_1},\ \underbrace{x^2y - 2y^2 + x}_{f_2},\ \underbrace{-x^2}_{f_3},\ \underbrace{-2xy}_{f_4},\ \underbrace{x - 2y^2}_{f_5},\ \underbrace{3y^3}_{f_6})$$

$$\left.\begin{aligned} f_1 &= -x f_3 + f_4 \\ f_2 &= -y f_3 + f_5 \\ f_3 &= -x f_5 + y f_4 \\ f_4 &= -2y f_5 - \tfrac{4}{3} f_6 \end{aligned}\right\} \Rightarrow G_4 = (\underbrace{x - 2y^2}_{f_5},\ \underbrace{3y^3}_{f_6})$$

$$S(f_5, f_6) = \frac{xy^3}{x} f_5 - \frac{xy^3}{3y^3} f_6 = -2y^5$$

$$\overline{-2y^5}^{G_4} = 0$$

Therefore G_3 is a Groebner basis. It containes f_1, f_2

G_4 is also a Groebner basis. It generates the same ideal as G_3.

Solving Algebraic Equations by Groebner Bases in Maple

IRO-2007-Solving-by-GB.mws

Click to start