Advanced Robotics

Lecture 8

pajdla@cmp.felk.cvut.cz

Algebraic equations & affine varieties

alg. equations $\underbrace{f_k(x_1, x_2, \dots x_n)}_{\text{polynomial}} = 0 \qquad k = 1, \dots, s$

monomial

$$f_k(x_1, x_2, \dots x_n) = \sum_{\alpha} a_\alpha x^\alpha$$

$x^\alpha \equiv x_1^{\alpha_1} \cdot x_2^{\alpha_2} \dots x_n^{\alpha_n} \qquad \alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \qquad \alpha_i \in \underbrace{\mathbb{Z}_{\geq 0}}_{\text{nonnegative whole numbers}}$

$a_\alpha \in k \dots$ a field $(\mathbb{R}, \mathbb{C}, \dots)$

$k[x_1, x_2, \dots, x_n] \equiv$ the set of all polynomials in $x_1, x_2, \dots, x_n$

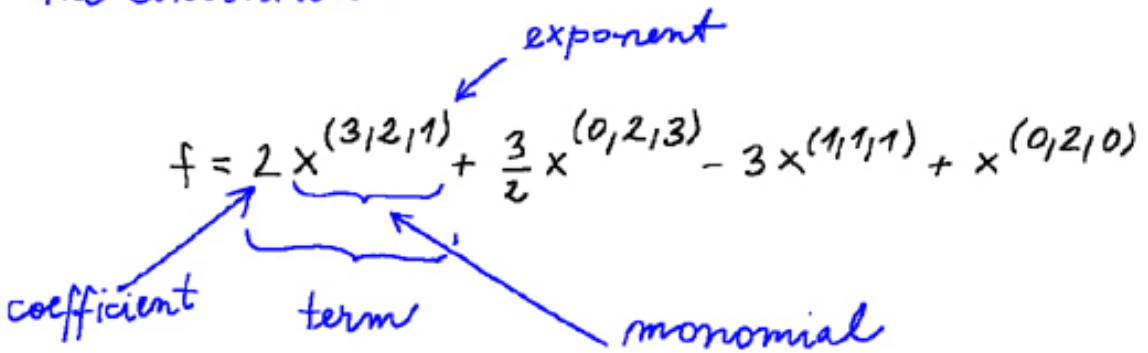
$(x_1, x_2, \dots, x_n) \in k^n \equiv n$-dimensional linear space

pajdla@cmp.felk.cvut.cz

Example: variables x_1, x_2, x_3

$$f = 2x_1^3 x_2^2 x_3 + \frac{3}{2} x_2^3 x_3^3 - 3x_1 x_2 x_3 + x_2^2$$

The convention:



Total degree of f: $\deg(f) = \max_{\alpha \text{ of } f} |\alpha|$, where $f = \sum_{\alpha} a_\alpha x^\alpha$, $\alpha \in \mathbb{Z}^n_{\geq 0}$

$$|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$$

Example:

$deg(0) = -\infty$, or undefined

$$\deg(f) = \max_{\alpha \in \{(3,2,1),(0,2,3),(0,2,0)\}} |\alpha| = |(3,2,1)| = 3+2+1 = 6$$

pajdla@cmp.felk.cvut.cz

Polynomials in one variable

Leading term: a non-zero polynomial

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

$a_m \neq 0$

$LT(f) = a_m x^m \equiv$ 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

$a_\alpha x^\alpha$ 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 $LT(f) \Leftrightarrow \deg(LT(g)) \leq \deg(LT(f)) \Leftrightarrow \deg(g) \leq \deg(f)$

$$LT(g) \text{ divides } LT(f) \Leftrightarrow \deg(g) \leq \deg(f)$$

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

{

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

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

}

pajdla@cmp.felk.cvut.cz

Observe that $f = qg + r$ 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 $LT(r) \Leftrightarrow \deg(r) < \deg(g)$

pajdla@cmp.felk.cvut.cz

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} either $= 0$

r_{i+1} or $\deg(r_{i+1}) < \deg(r_i)$

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

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

pajdla@cmp.felk.cvut.cz

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

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.

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

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 ... neider 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 $k[x_1, \ldots, x_n]$ is any ordering relation $<$ on $\mathbb{Z}_{\geq 0}^n$ satisfying :

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

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

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

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

pajdla@cmp.felk.cvut.cz

Lexicographic order

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

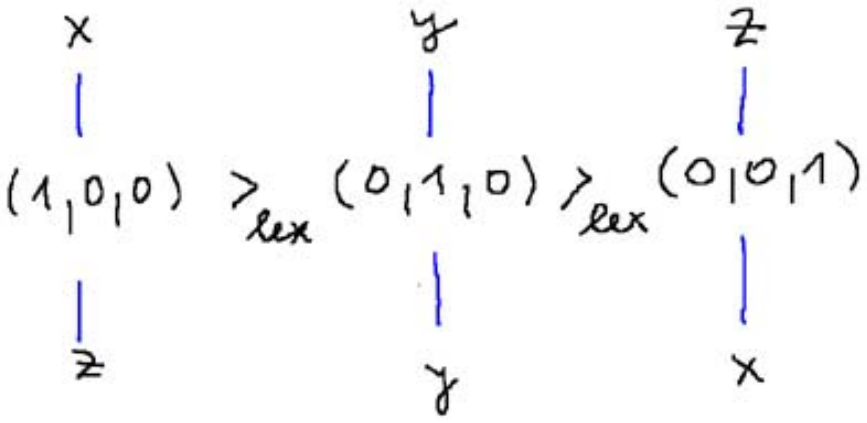
$\alpha >_{lex} \beta$ if the left-most non-zero element of

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



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 $\mathbb{Z}_{\geq}^{n}$ is a monomial ordering

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

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

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

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

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

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

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

pajdla@cmp.felk.cvut.cz

The lex ordering is a monomial ordering

(i) $\forall \alpha, \beta : \alpha \geq_{lex} \beta$ or $\beta \geq_{lex} \alpha$:

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

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

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

(iii) $\forall \alpha : \alpha \geq_{lex} 0$

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

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

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

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

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

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

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

$multideg(f) = (3,0,0)$

$LC(f) = -5$

$LM(f) = x^3$

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

pajdla@cmp.felk.cvut.cz

Polynomial division with more divisors in more variables

pajdla@cmp.felk.cvut.cz

"Division" by more than one polynomial

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

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

We see that $f:(f_1, f_2) \neq f:(f_2, f_1) \Rightarrow f:\{f_1, f_2\}$

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 $\mathbb{Z}_{\geq}^n$ and $F = (f_1, \dots, f_s)$ an ordered s-tuple, $f_i \in k[x_1, \dots, x_n]$. Then every $f \in k[x_1 \cdots x_n]$ 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 $F = (f_1, \dots, f_s)$

pajdla@cmp.felk.cvut.cz

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

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

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

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

$r \rightarrow p$

pajdla@cmp.felk.cvut.cz

Example

$x >_{lex} y$

$f = xy^2 + x + 1$, $f_1 = xy + 1$, $f_2 = y + 1$

$xy^2 + x + 1$: $(1,2)$ $(1,0)$ $(0,0)$ — $xy + 1$: $(1,1)$ $(0,0)$ — $y + 1$: $(0,1)$ $(0,0)$

$$f = y(xy+1) + x - y + 1 = y(xy+1) - 1(y+1) + \underbrace{x+2}_{r}$$

$x - y + 1$: $(1,0)$ $(0,1)$ $(0,0)$ — a_1 — a_2

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

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

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

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

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

pajdla@cmp.felk.cvut.cz

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

pajdla@cmp.felk.cvut.cz

Affine varieties

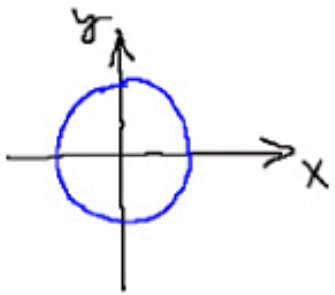
$f_k(x_1, x_2, \dots, x_n)$ ... algebraic equations

Algebraic variety ≡ the set of points for which all equations f_k are satisfied

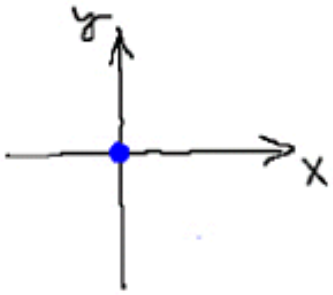
$$V = \{ (x_1, x_2, \dots, x_n) \mid f_k(x_1, x_2, \dots, x_n) = 0,\ k = 1, 2, \dots, s \}$$

Examples:

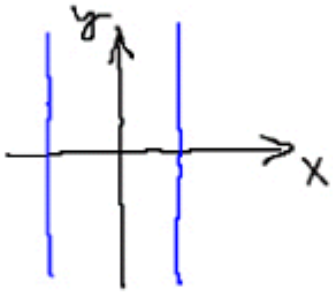
$\{x^2 + y^2 = 2\}$



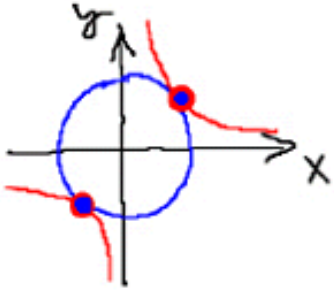
$\{x^2 + y^2 = 0\}$



$\{x^2 = 1\}$



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



pajdla@cmp.felk.cvut.cz

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

pajdla@cmp.felk.cvut.cz

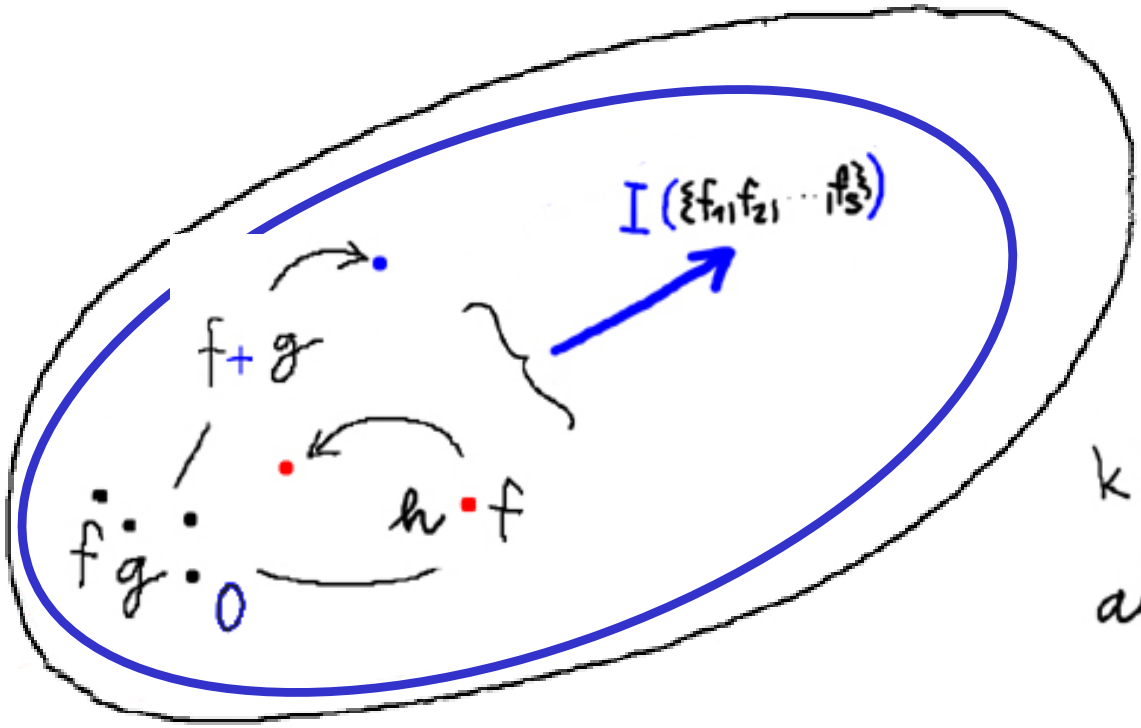
Ideal generated by polynomials

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



$k[x_1, x_2, \dots, x_n]$

all polynomials

pajdla@cmp.felk.cvut.cz

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

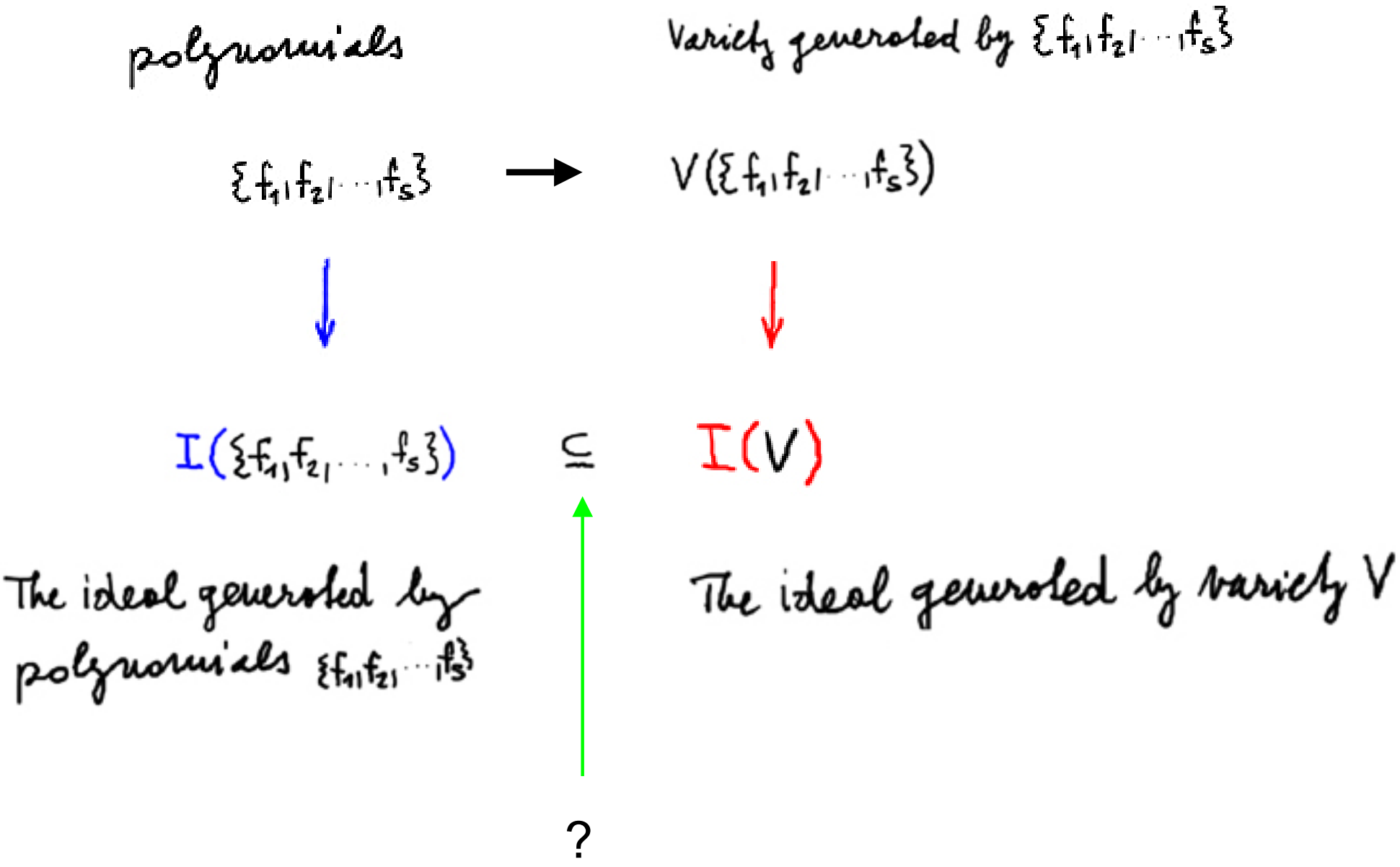
(i) $0(x) = 0$

(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

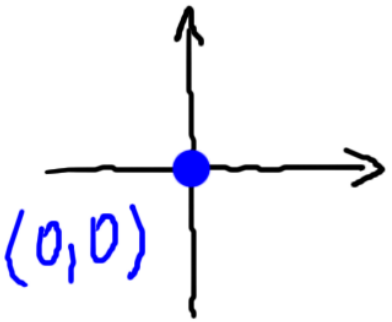


pajdla@cmp.felk.cvut.cz

Example $\{x^2, y^2\} \rightarrow V(\{x^2, y^2\})$

$\downarrow \qquad \downarrow$

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



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

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

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

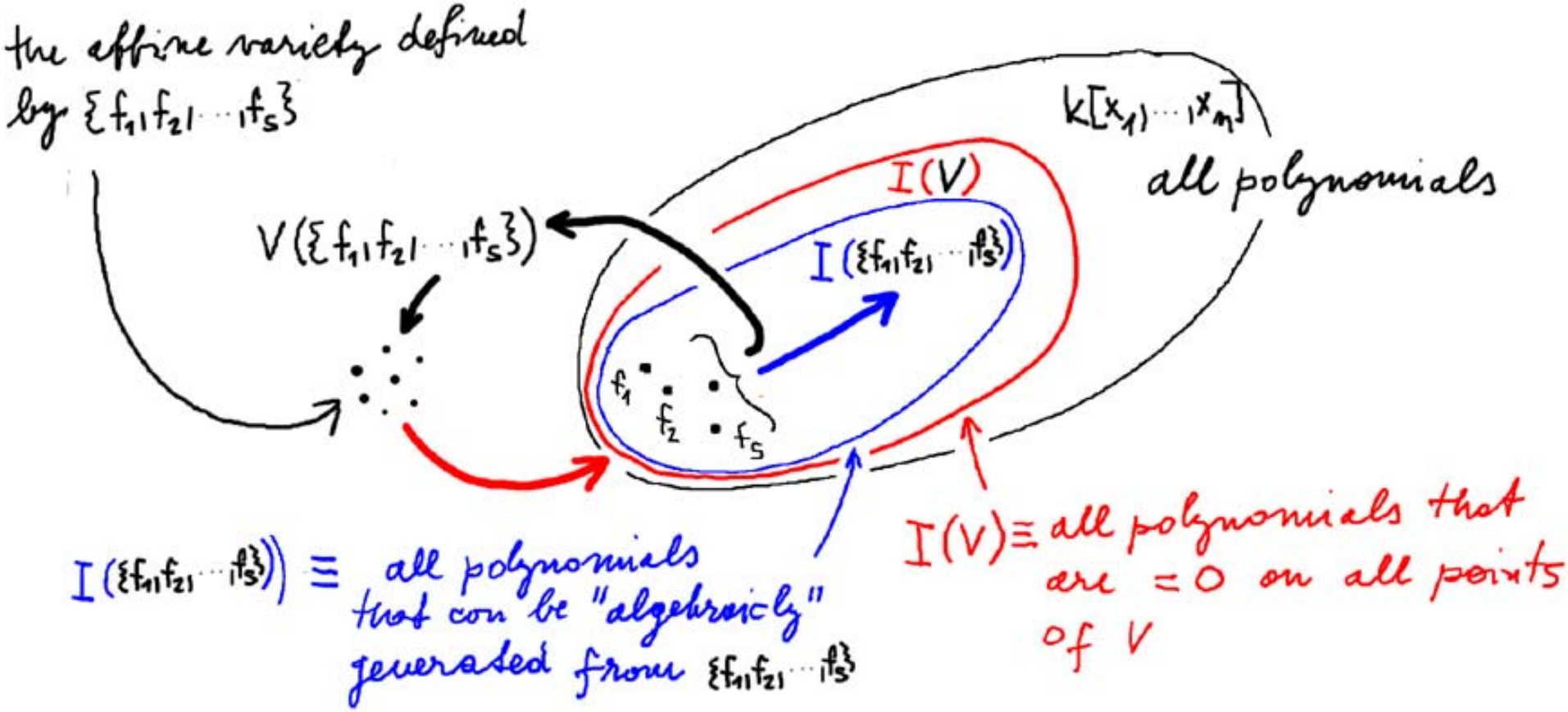
$I(\{x^2, y^2\}) \subset I(\{x, y\})$

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

as every $\not{0}$ $h_1(x,y)\,x^2 + h_2(x,y)\,y^2$ has total degree at least two

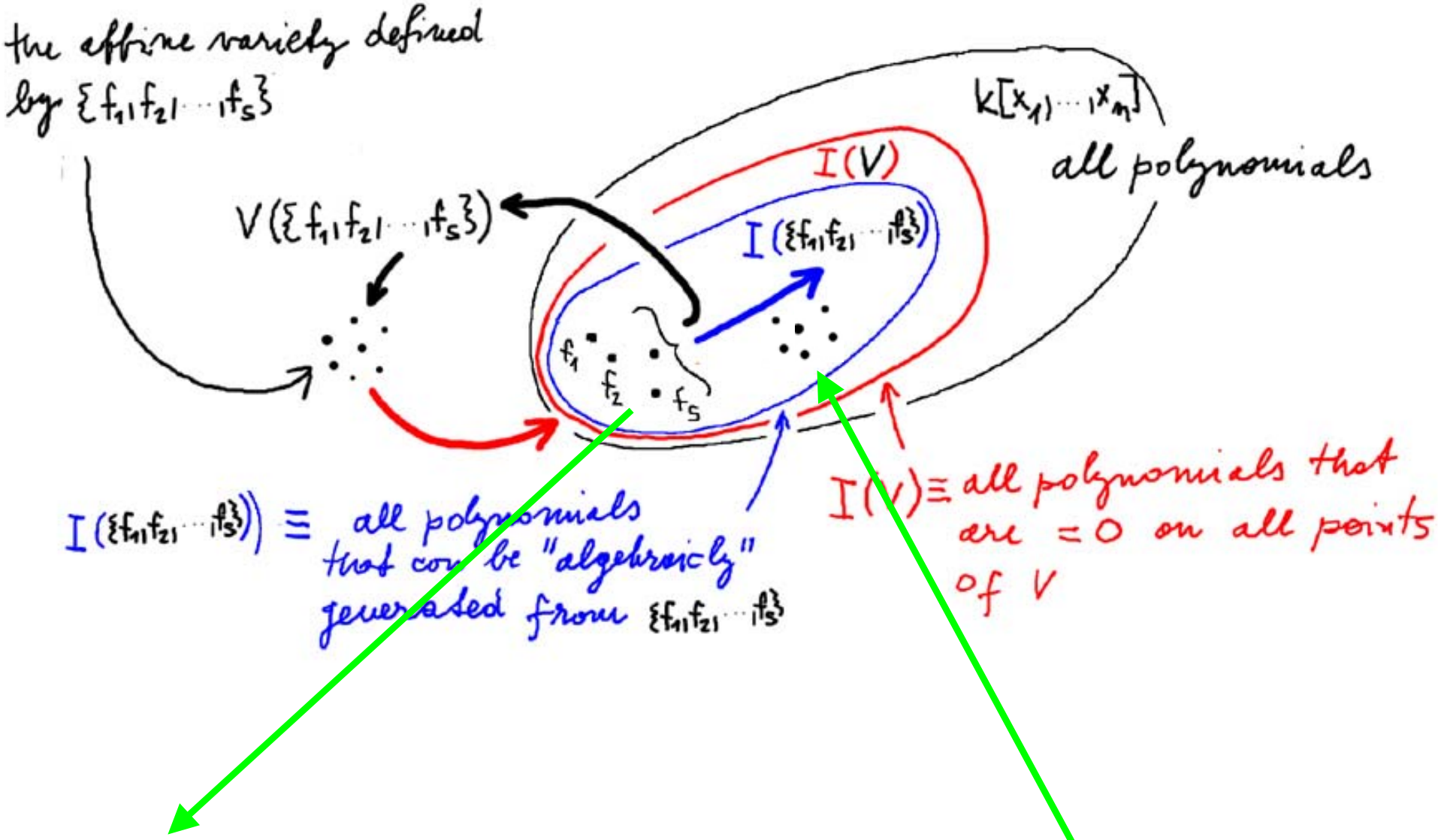
pajdla@cmp.felk.cvut.cz

The complete picture



pajdla@cmp.felk.cvut.cz

Groebner basis is a special basis of the Ideal



Basis:
$B = \{f_1, f_2, \dots, f_s\}$

Algebraic manipulation

Groebner basis w.r.t. $<_{lex}$:
$G = \{g_1, g_2, \dots, g_n\}$

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. $x_1 \geq_{lex} \cdots \geq_{lex} x_n$ 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

pajdla@cmp.felk.cvut.cz

Least common multiple of monomials

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

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

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

Example:

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

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

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

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

pajdla@cmp.felk.cvut.cz

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

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

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

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

with $x >_{lex} y$

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

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

cancel

pajdla@cmp.felk.cvut.cz

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'
```


pajdla@cmp.felk.cvut.cz

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

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

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

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

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

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

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

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

$\vdots$

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

pajdla@cmp.felk.cvut.cz

$$G_3 = (x^3 - 2xy,\ x^2y - 2y^2 + x,\ -x^2,\ -2xy,\ x - 2y^2,\ 3y^3)$$

f_1 f_2 f_3 f_4 f_5 f_6

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

f_5 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 contains f_1, f_2

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

pajdla@cmp.felk.cvut.cz