Advanced Robotics

Lecture 5

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

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

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

$a_\alpha \in k \; \dots$ 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

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

The convention:

$$f = \underbrace{\underbrace{2}_{\text{coefficient}}\,\underbrace{x^{\overbrace{(3,2,1)}^{\text{exponent}}}}_{\text{monomial}}}_{\text{term}} + \frac{3}{2} x^{(0,2,3)} - 3 x^{(1,1,1)} + x^{(0,2,0)}$$

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

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

Example:

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

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

Ring of polynomials

like $\mathbb{R}$ without the division

plus $\oplus$, times $\odot$:

$$k[x_1, x_2, \ldots, x_n] \times k[x_1, x_2, \ldots, x_n] \longrightarrow k[x_1, x_2, \ldots, x_n]$$

cartesian product

i.e. $f \oplus g = h$ or $f \odot g = m$

Be $f = \sum_{\alpha \in A} a_\alpha x^\alpha = \sum_{\alpha \in A \cup B} a'_\alpha x^\alpha$ where $a'_\alpha = \begin{cases} a_\alpha, & \alpha \in A \\ 0, & \alpha \notin A \end{cases}$

$g = \sum_{\beta \in B} b_\beta x^\beta = \sum_{\beta \in A \cup B} b'_\beta x^\beta$ where $b'_\beta = \begin{cases} b_\beta, & \beta \in B \\ 0, & \beta \notin B \end{cases}$

Define:

plus $f \oplus g = \sum_{\gamma \in A \cup B} (a'_\gamma + b'_\gamma)\, x^\gamma$ ($\sum_\alpha 0 \cdot x^\alpha$ is the ... zero polynomial

times $f \odot g = \sum_{\alpha \in A \cup B} \sum_{\beta \in A \cup B} (a'_\alpha \cdot a'_\beta)\, x^{(\alpha+\beta)}$ ($1 \cdot x^{(0,0,\ldots,0)} + 0 \cdot x^\alpha + \ldots$ unit polynomial

Excercises:

1. Show that $(k[x_1, \ldots, k_n], \oplus, \odot)$ is a ring, i.e. that holds true
   (a) $f \oplus g = g \oplus f$
   (b) $(f \oplus g) \oplus h = f \oplus (g \oplus h)$
   (c) $\exists 0 \in k[x_1, \ldots, k_n]$: $f \oplus 0 = f$
   (d) $\forall f \, \exists e \in k[x_1, \ldots, k_n]$: $e \oplus f = 0$
   (e) $f \odot g = g \odot f$
   (f) $(f \odot g) \odot h = f \odot (g \odot h)$
   (g) $\exists 1 \in k[x_1, \ldots, k_n]$: $f \odot 1 = f$
   (h) $f \odot (g \oplus h) = (f \odot g) \oplus (f \odot h)$

   for arbitrary $f, g, h \in k[x_1, \ldots, k_n]$.

Dual nature of polynomials – "∞ tables" & functions

Observations

1) there is no limit on the total degree of a polynomial
2) a polynomial has always a finite number of non-zero a_α's

$\Rightarrow$ polynomials $\equiv$ infinite tables (sequences) with a finite number of non-zero entries

$$f = \sum_{\alpha \in A} a_\alpha x^\alpha = \underbrace{a_{(0,0,\dots,0)}} x^{(0,0,\dots,0)} + \dots + \underbrace{a_{(\alpha_1,\alpha_2,\dots,\alpha_n)}} x^{(\alpha_1,\alpha_2,\dots,\alpha_n)} + \dots$$

non-zero "coordinates" of $s(k_1,k_2,\dots,k_n)$, $k_i \in \mathbb{Z}_{\geq 0}$

$$f \equiv s(\underbrace{k_1,k_2,\dots,k_n}) \qquad s(k_1,k_2,\dots,k_n) = \begin{cases} a_\alpha & \text{if } \exists\, \alpha \in A : (k_1,k_2,\dots,k_n) = \alpha \\ 0 & \text{otherwise} \end{cases}$$

n-times infinite sequence

$k_i \in (1,2,\dots,\infty) \equiv$ infinite sequence

pajdla@cmp.felk.cvut.cz

Example:

$$f(x) = 2x^3 + x + 3 = 3x^0 + 1\cdot x^1 + 0\cdot x^2 + 2x^3 + 0\cdot x^4 + 0\cdot x^5 + \dots$$

$$\equiv (3, 1, 0, 2, 0, 0, \dots\dots \infty) \quad \dots \text{an infinite sequence}$$

$$\quad x^0 \;\; x^1 \;\; x^2 \;\; x^3 \;\; x^4 \;\; x^5 \;\; \dots$$

with non-zero values on a finite number of coordinates

but we often write $(2, 0, 1, 3)$ instead

plus $\oplus$

on polynomials $\rightsquigarrow$ operations on tables

times $\odot$

plus $\oplus$ $\equiv$ coordinatewise addition

$$(s \oplus t)_{(k_1, k_2, \dots, k_n)} = s_{(k_1, k_2, \dots, k_n)} + t_{(k_1, k_2, \dots, k_n)}$$

addition in k

element-wise multiplication by a scalar $\in k$

$$\underbrace{\left(s_{(k_1, k_2, \dots, k_n)}, \oplus, \cdot\right)}_{\infty\text{-dimensional linear space}}$$

$$s_{(k_1, k_2, \dots, k_n)} \in k^{(1,2,\dots,\infty)^n}$$

n-times infinite sequence

Example:

$$f(x) = 2x^3 + x + 3 \equiv (3, 1, 0, 2, 0, 0, \dots\dots \infty)$$

$$g(x) = 4x^4 + x^3 + x^2 \equiv (0, 0, 1, 1, 4, 0, \dots\dots \infty)$$

$$(f \oplus g)(x) \equiv (3, 1, 1, 3, 4, 0, \dots\dots \infty)$$

times $\odot$ $\equiv$ "shifting" of elements (algebraic ~ non-linear operation)

$$(s \odot t)_{(k_1, k_2, \dots, k_n)} = \sum_{\{(\alpha, \beta) \mid \alpha, \beta \in \mathbb{Z}^n_{\geq 0},\ \alpha + \beta = (k_1, k_2, \dots, k_n)\}} s_\alpha \cdot t_\beta$$

Example: $f(x) = 2x^3 + x + 3 \equiv (3, 1, 0, 2, 0, 0, \dots\dots \infty)$

$g(x) = 4x^4 + x^3 + x^2 \equiv (0, 0, 1, 1, 4, 0, \dots\dots \infty)$

$$(f \odot g)(x) \equiv \underbrace{\sum_{\{(0,0)\}} f_\alpha \cdot g_\beta}_{(f \odot g)_{(0)}} + \underbrace{\sum_{\{(1,0),(0,1)\}} f_\alpha \cdot g_\beta}_{(f \odot g)_{(1)}} + \underbrace{\sum_{\{(2,0),(1,1),(0,2)\}} f_\alpha \cdot g_\beta}_{(f \odot g)_{(2)}} + \cdots\cdots + \underbrace{\sum_{\{(7,0),(6,1),\dots,(0,7)\}} f_\alpha \cdot g_\beta}_{(f \odot g)_{(7)}}$$

$$= (3 \cdot 0,\ 1 \cdot 0 + 3 \cdot 0,\ 0 \cdot 0 + 1 \cdot 0 + 3 \cdot 1,\ \dots\dots,\ 0 \cdot 0 + 0 \cdot 0 + \dots + 3 \cdot 0, \dots$$

$$= (0, 0, 3, 3+1, 12+1, 2+4, 2, 8, 0, 0, \dots, \infty)$$

pajdla@cmp.felk.cvut.cz

Dual nature of polynomials – "∞ tables" & functions

Observation

(i) $f(x_1, x_2, \dots, x_n) : k^n \longrightarrow k$ is a function

(ii) Assume the field $\mathbb{Z}_2 = (\{0,1\}, x+y \bmod 2, x \cdot y)$

$0+0 = 0 \bmod 2 = 0$ ≡ neutral element of the addition

$0+1 = 1 \bmod 2 = 1$

$1+1 = 2 \bmod 2 = 0$

$0+0=0$ … inverse of 0 is 0

$1+1=0$ …. inverse of 1 is 1

$0 \cdot 0 = 0$

$0 \cdot 1 = 0$

$1 \cdot 1 = 1$ ≡ identity of the multiplication, inverse of 1 is 1

And now the punch line!

$x(x+1) = x^2 - x$ is NOT a zero polynomial, but

$0 \cdot (0+1) = 0 \cdot 1 = 0$ & $1 \cdot (1+1) = 1 \cdot 0 = 0$ is the zero function

pajdla@cmp.felk.cvut.cz

Excercises:

1. Is $\mathbb{Z}_3$, i.e. $(\{0,1,2\}, x+y \text{ mod } 3, x \cdot y)$, a field?

2. Is there a non-zero polynomial in $\mathbb{Z}_3$, which is the zero function?

pajdla@cmp.felk.cvut.cz

Polynomials in one variable

Leading term: a non-zero polynomial

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

$a_m \neq 0$

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

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

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

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

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

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"

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

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