MMA 数学特論 I

Algorithms for polynomial systems: elimination & Gröbner bases

多項式系のアルゴリズム: グレブナー基底 & 消去法

Lecture III: The division algorithm

May, 6th 2010. Part I: Generalities on multivariate polynomials

Part II: Monomial orders

Part III: The algorithm

Part I: Generalities

The polynomial ring $R[X_1, \ldots, X_n]$ (1/3)

Notation: A multi-integer α is an element of $\mathbb{N}^n$, for a given n: hence, $\alpha = (\alpha_1, \ldots, \alpha_n)$, with $\alpha_i \in \mathbb{N}$.

Addition: Given $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ two multi-integers, we denote by $\alpha + \beta$ the multi-integer $(\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$.

For $n > 1$, $P \in R[X_1, \ldots, X_n]$ is a multivariate or n-variate polynomial, or a polynomial in n variables, with coefficients in (a commutative) ring R.

We write: $P = \sum_{\alpha \in \mathbb{N}^n} p_\alpha X^\alpha$, where $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, and $p_\alpha \neq 0$ only for a finite number of multi-integers α.

Monomial: It is a polynomial P with all $p_\alpha = 0$ except for a multi-integer β, for which $p_\beta = 1$. This means $P = X_1^{\beta_1} \cdots X_n^{\beta_n}$.

The polynomial ring $R[X_1, \ldots, X_n]$ (2/3)

Coefficient: the ring R is called the coefficient ring of $R[X_1, \ldots, X_n]$.

For a polynomial $P = \sum_\alpha p_\alpha X^\alpha$, the elements (p_α) are the coefficients of P.

Given a multi-integer α, the coefficient p_α is the coefficient of (the monomial) X^α of P.

If $p_\alpha \neq 0$, we say that the monomial X^α occurs in P.

The coefficient $p_{(0,\ldots,0)}$ is called the constant term of P.

Multiplication: $$PQ = \sum_{\alpha \in \mathbb{N}^n} \left(\sum_{\substack{\beta,\gamma \in \mathbb{N}^n \\ \beta+\gamma=\alpha}} p_\beta q_\gamma \right) X^\alpha$$ (notice that $PQ = QP$).

Ring structure: With the addition and multiplication above, $R[X_1, \ldots, X_n]$ is a commutative ring.

The polynomial ring $R[X_1, \dots, X_n]$ (3/3)

Proposition 1 *If R is an integral domain, then $R[X_1, \dots . X_n]$ is also integral.*

PROOF:By induction on n. When $n = 1$, it is proven in Lect. II. If this is true for polynomials in $n - 1$ variables over R, then let $R' = R[X_1, \dots, X_{n-1}]$ in integral.

The case in 1 variable done in Lect. II shows that $R'[X_n]$ is integral. But $R'[X_n] = R[X_1, \dots, X_n]$. □

Remark 1: Assume $R = \Bbbk$ is a field. Then $\Bbbk[X_1, \dots, X_n]$ is a $\Bbbk$-vector space. As a ring, it is also a $\Bbbk$-algebra.

The degree

Given a multi-integer $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, the sum of α is $|\alpha| := \alpha_1 + \cdots + \alpha_n$

The degree of a monomial X^α is $|\alpha|$.

The degree of a polynomial $P \in R[X_1, \ldots, X_n]$ is the maximal degree of one of the monomials occuring in P.

For any polynomials P and Q in $R[X_1, \ldots, X_n]$, we have:

(i) $\deg(P + Q) \leq \max\{\deg(P)\,, \deg(Q)\}$, with equality if $\deg(P) \neq \deg(Q)$.

(ii) $\deg(PQ) = \deg(P) + \deg(Q)$ (not true over any ring, but true over any *integral domain*)

Remark: Assume $R = \Bbbk$ is a field, and let $L \in \mathbb{N}^*$. Let $\Bbbk[X_1, \ldots, X_n]_{<L}$ be the set of polynomials of degree $< L$.

This is a sub-vector space of finite dimension (Exercise: what is the dimension ?)

The degree

By the 2 previous sildes, the following map is $\mathbb{k}$-bilinear:

$$\begin{array}{rcl} Mult : \quad \mathbb{k}[X_1,\ldots,X_n]_{<L_1} \times \mathbb{k}[X_1,\ldots,X_n]_{<L_2} & \longrightarrow & \mathbb{k}[X_1,\ldots,X_n]_{<L_1+L_2} \\ (A,B) & \longmapsto & AB \end{array}$$

It follows that $\mathbb{k}[X_1,\ldots,X_n]$ is a graded commutative algebra.

Remark 1: There are several monomials of same degree.

Remark 2: There is no Euclidean division **!**

Comment: The degree is sometimes called the total degree of a polynomial P.

The partial degree in X_i of P, denoted $\deg_{X_i}(P)$ is the maximal exponent α_i of X_i among all the monomials occuring in P.

The partial degree is the degree of the univariate polynomial P seen in $R_i[X_i]$, whith $R_i = \mathbb{k}[X_1,\ldots,X_{i-1},X_{i+1},\ldots,X_n]$.

Polynomial function

Here we assume $R = \Bbbk$ is a field. Let $P \in \Bbbk[X_1, \ldots, X_n]$ be a polynomial.

Function: The map $\Bbbk^n \to \Bbbk$, $(x_1, \ldots, x_n) \mapsto P(x_1, \ldots, x_n)$ is the function defined by P.

A zero of P is a point $(x_1, \ldots, x_n)$ such that $P(x_1, \ldots, x_n) = 0$.

!!: There are some non-zero polynomials P, that defined the zero function.

Example, even with $n = 1$: the non-zero polynomial $X^p - X \in \mathbb{F}_p[X]$ define the null function of $\mathbb{F}_p \to \mathbb{F}_p$.

Lemma 1 *Assume that $\Bbbk$ is infinite, and that there are some infinite subsets $S_1, \ldots, S_n$ of $\Bbbk$ such that:*

$$\forall a_i \in S_i, \quad f(a_1, \ldots, a_n) = 0.$$

Then $f = 0$ (the null polynomial).

PROOF:When $n = 1$ it is (Lect. I, Corollary 1). Then by induction on n. $\square$

Ideals of $\Bbbk[X_1, \dots, X_n]$

Definition of an ideal $\rightarrow$ Lect. II, Definiton 3.

Example: Finitely generated ideals. The subset $\langle f_1, \dots, f_s \rangle$ of $\Bbbk[X_1, \dots, X_n]$ defined by:

$$\langle f_1, \dots, f_s \rangle := \left\{ \sum_{i=1}^{s} f_i g_i, \quad g_i \in \Bbbk[X_1, \dots, X_n] \right\},$$

is an ideal of $\Bbbk[X_1, \dots, X_n]$. Its basis $f_1, \dots, f_s$ is *finite* (it s a *finitely generated* ideal)

All the ideals of $\Bbbk[X_1, \dots, X_n]$ are finitely generated ! (Hilbert. Proof, next class).

A geometric interpretation

Suppose $\mathbb{k}$ is infintite (polynomials $\iff$ polynomial functions).

Let $F := \{f_1(X_1, \ldots, X_n)\,,\, f_2(X_1, \ldots, X_n)\,, \ldots,\, f_s(X_1, \ldots, X_n)\}$ a polynomial system.

A solution of F is a common zero of all the polynomials f_i (be careful: depends on the field extension).

Let $x = (x_1, \ldots, x_n)$ be a solution of F (in a field extension of $\mathbb{k}$).

Then for any polynomial $f \in \langle f_1, \ldots, f_s \rangle$, x is also a solution of f.

Consequence: Looking for solutions of a polynomial system F is the same as looking for solution of the ideal $\langle F \rangle$ generated by F.

Comment: It is actually a bit more complicated (problem of multiplicities especially $\rightarrow$ Hilbert's Nullstellensatz).

Parts II & III: Division for multivariate polynomials

Introduction

Aim: Given $f, f_1, \ldots, f_s \in \Bbbk[X_1, \ldots, X_n]$, write:

$$f = a_1 f_1 + \cdots + a_s f_s + r, \tag{1}$$

with r have "smaller" monomials than those of $f_1, \ldots, f_s$.
→ monomial orders

Unicity of the remainder r in Equation (1) ?
→ **No** in general.
→ **Yes** if the polynomials $(f_i)_i$ are ordered.

Ideal Membership: if $f \in \langle f_1, \ldots, f_s \rangle$, so we have $r = 0$?
→ **No** in general.
→ **Yes** if the polynomials $(f_i)_i$ form a Gröbner basis.

Part II: Monomial orders

Definition 1 *A* monomial order *(or* ordering*)* $\prec$ *on* $\Bbbk[X_1, \ldots, X_n]$*, is a relation on the set of monomials* X^α*,* $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$*, such that:*

(i) $\prec$ *is a* total order *(2 monomials can always be compared: if* $\alpha \neq \beta$*, then either* $X^\alpha \prec X^\beta$*, or* $X^\beta \prec X^\alpha$*).*

(ii) *if* $X^\alpha \prec X^\beta$*, then* $X^\alpha X^\gamma \prec X^\beta X^\gamma$*, for all* $\gamma \in \mathbb{N}^n$*.*

(iii) $\prec$ *is a* well-order*: any non-empty subset of monomials has a smallest element.*

Before giving examples, an useful lemma.

Lemma 2 *An order relation* $\prec$ *on the monomials of* $\Bbbk[X_1, \ldots, X_n]$ *is a well-order iff every strictly decreasing sequence*

$$X^{\alpha(1)} \succ X^{\alpha(2)} \succ X^{\alpha(3)} \succ \cdots$$

eventually terminates ($\iff \exists \ell \mid \alpha(N) = \alpha(\ell)\ \forall N \geq \ell$*).*

Example I: lexicographic orders

Let us order the n variables: $X_n \prec X_{n-1} \prec \cdots \prec X_1$ (there are $n!$ such possible orders: $X_{n-1} \prec X_n \prec \cdots \prec X_2 \prec X_1$ is another one, corresponding to the permutation $(n-1\,,\,n)$, while $X_n \prec X_{n-1} \prec \cdots \prec X_1 \prec X_2$ corresponds to the permutation $(1\,,\,2)$).

Definition 2 *The* lexicographic order $\prec_{lex}$ *on the monomials of* $\mathbb{k}[X_1, \ldots, X_n]$ *relatively to* $\prec$ *is characterized by: For all multi-integers* $\alpha \neq \beta$,

$$X^\alpha \prec_{lex} X^\beta \Leftrightarrow \text{ if } \ell := \min\{1 \leq i \leq n \,|\, \alpha_i \neq \beta_i\}, \text{ then } \alpha_\ell < \beta_\ell.$$

Example: $X_1^2 X_2^3 \prec_{lex} X_1^2 X_2^4$, since $(2,3) - (2,4) = (0,-1)$ and $-1 < 0$

Proposition 2 *The lex order is a monomial order.*

Proof:(i) and (ii) of Definition 1 are clearly verified, (iii) is proved using Lemma 2. □

Example II: graded lex orders

The next two orders are called *degree* orders, or they are said to *refine the degree*. Recall that for a multi-integer $\alpha = (\alpha_1, \ldots, \alpha_n)$, we have $|\alpha| = \sum_{i=1}^{n} \alpha_i = \deg(X^\alpha)$.

Definition 3 *Given two* distinct *multi-integers* $\alpha = (\alpha_i)_{1 \le i \le n}$ *and* $\beta = (\beta_i)_{1 \le i \le n} \in \mathbb{N}^n$, *the* graded lex order *is characterized by*

$$X^\alpha \prec_{grlex} X^\beta \Leftrightarrow |\alpha| < |\beta|, \text{ or } |\alpha| = |\beta| \text{ and } \alpha \prec_{lex} \beta.$$

Example: $X_1^4 \prec_{grlex} X_1^3 X_2^3$, while $X_1^3 X_2^3 \prec_{lex} X_1^4$.

! A grlex order relies on a choice of a lex order $\prec_{lex}$ among the $n!$ possible. In the example, it is the one for which $X_2 \prec X_1$. **!**

Proposition 3 *The graded lex orders are monomial orders.*

Counter-example: revlex order

We give an example of total order on the monomials, that *is not* a monomial order.

Definition 4 *Given two* distinct *multi-integers α and β, the* revlex *order is defined by:*

$$X^\alpha \prec_{revlex} X^\beta \Leftrightarrow \textit{if} \ \ell := \max\{1 \leq i \leq n \mid \alpha_i \neq \beta_i\}, \ \textit{then} \ \alpha_\ell > \beta_\ell,$$

Example: $X_2^2 \prec_{revlex} X_1^2 X_2 \prec_{revlex} X_1 X_2 \prec_{revlex} X_2 \prec_{revlex} X_1^3$

Proposition 4 *The revlex order* is not *a monomial order.*

PROOF:The strictly decreasing $(X_2^i)_{i \geq 1}$ does not terminate. With Lemma 2, this contradicts Property (iii) of Definition 1. □

Example III: graded reverse lex order

Definition 5 *Let two* distinct *multi-integers* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *and* $\beta = (\beta_1, \ldots, \beta_n)$ *in* $\mathbb{N}^n$*; we define the* graded reverse lex *order as:*

$$X^\alpha \prec_{grevlex} X^\beta \Leftrightarrow |\alpha| < |\beta| \text{ or } |\alpha| = |\beta| \text{ and } \alpha \prec_{revlex} \beta$$

Example: $X_3^3 \prec X_2 X_3^2 \cdots \prec X_1 X_2 X_3 \prec X_1^2 X_3 \cdots \prec X_2^3 \cdots \prec X_1^3$.

Proposition 5 *The grevlex order is a monomial order.*

PROOF:It is a degree refinement of the revlex order. This prevents infinite decreasing sequences as in Proposition 4 □

Other monomial orders: Weighted degree orders, block orders...

Remark: A monomial order $\prec$ defines an order relation on the multi-integer of $\mathbb{N}^n$ (by taking the exponent). We may use freely the notation:

$$\alpha\,,\,\beta \in \mathbb{N}^n \quad \alpha \prec \beta \iff X^\alpha \prec X^\beta.$$

Multi-degree. Leading term, monomial, coefficient...

Let $\prec$ be a monomial order on $\Bbbk[X_1, \ldots, X_n]$.

Let $f \in \Bbbk[X_1, \ldots, X_n]$ (as usual given a multi-integer α, $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$).

Multi-degree: $\mathsf{mdeg}_\prec(f) = \max_\prec\{\alpha \in \mathbb{N}^n \mid \text{the monomial } X^\alpha \text{ occurs in } f\}$.

Let $\beta = \mathsf{mdeg}_\prec(f) \in \mathbb{N}^n$. We write $f = \sum_{\alpha \in \mathbb{N}^n} f_\alpha X^\alpha$.

Leading monomial: $\mathrm{LM}_\prec(f) := X^\beta$.

Leading coefficient: $\mathrm{LC}_\prec(f) := p_\beta$.

Leading term: $\mathrm{LT}_\prec(f) := p_\beta X^\beta$ $(= \mathrm{LC}_\prec(f)\,\mathrm{LM}_\prec(f))$.

!!: These 4 definitions **depend** on the monomial order $\prec$.

If it is **clear** what is $\prec$, we write simply: $\mathsf{mdeg}(f), \mathrm{LM}(f), \mathrm{LC}(f), \mathrm{LT}(f)$.

Multi-degree. Leading term... (examples)

$f = x^2z^2 + xy^2z + xyz^2 + x^3 + y^3$

	order $\prec$	$\mathsf{mdeg}_\prec(f)$	$\mathrm{LM}_\prec(f)$
1	$lex(x, y, z)$	$(3, 0, 0)$	x^3
2	$lex(y, x, z)$	$(3, 0, 0)$	y^3
3	$grlex(x, y, z)$	$(2, 0, 2)$	x^2z^2
4	$grlex(z, y, x)$	$(2, 1, 1)$	z^2yx
5	$grevlex(x, y, z)$	$(1, 2, 1)$	xy^2z
6	$grevlex(z, y, x)$	$(2, 1, 1)$	z^2yx

Exercise: Over $\Bbbk[X_1, \ldots, X_n]$, prove that

$$X^\alpha \prec_{revlex(X_1,\ldots,X_n)} X^\beta \iff X^\alpha \succ_{lex(X_n,\ldots,X_1)} X^\beta.$$

Part III: The division algorithm

1 variable: The Euclidean algorithm works because a degree is strictly decreasing.

Multivariate polynomials: the monomial order permits to have a similar decreasing property.

Let $\prec$ be a monomial order.

\# Inputs: f and $[f_1, \ldots, f_s]$ polynomial in $\mathbb{k}[X_1, \ldots, X_n]$
(the sequence $[f_1, \ldots, f_s]$ is ordered, it is not a set)

\# Outputs: $r, [a_1 \ldots, a_s]$ such that (a) $f = a_1 f_1 + \cdots a_s f_s + r$
(b) $\mathrm{LM}(f_i) \nmid m$, for any monomial m occuring in r
(c) if $a_i f_i \neq 0$, then $\mathrm{LM}(f) \succcurlyeq \mathrm{LM}(a_i f_i)$

When $n = s = 1$, it is the Euclidean algorithm (by conditions (a) and (b)).

$[a_1, \ldots, a_s] \leftarrow [0, \ldots, 0]$

$p \leftarrow f \; ; r \leftarrow 0$

while $(p \neq 0)$ **do**

  $i \leftarrow 1$

  while $(i \leq s$ **and** $\mathrm{LM}(f_i) \nmid \mathrm{LM}(p))$ **do:** $i \leftarrow i + 1;$ **end while**

  if $(i \leq s)$ **then** //$\mathrm{LM}(f_i)$ divides $\mathrm{LM}(p)$

    $a_i \leftarrow a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$

    $p \leftarrow p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$

  else //there is no $\mathrm{LM}(f_i)$ that divides $\mathrm{LM}(p)$

    $r \leftarrow r + \mathrm{LT}(p)$ // the remainder is updated

    $p \leftarrow p - \mathrm{LT}(p)$

  end if

end while

return $[a_1, \ldots, a_s], r$

About unicity (1/3)

Δ-sets: The exponents of the monomials in r and in $a_1, \ldots, a_s$ are constrained to take certain values, defined by the following Δ-sets.

Let $\alpha(i) := \mathsf{mdeg}_{\prec}(f_i) \in \mathbb{N}^n$. We define the following partition of $\mathbb{N}^n$:

$$\Delta_1 = \alpha(1) + \mathbb{N}^n \ , \ \Delta_2 = \alpha(2) + \mathbb{N}^n - \Delta_1 \ , \ \ldots \ ,$$

$$\Delta_i = \alpha(i) + \mathbb{N}^n - \left(\cup_{j=1}^{i-1} \Delta_j\right) \ , \ \ldots \ , \ \Delta_s = \alpha(s) + \mathbb{N}^n - \left(\cup_{j=1}^{s-1} \Delta_j\right) .$$

and finally $\overline{\Delta} = \mathbb{N}^n - \cup_{j=1}^{s} \Delta_j$. We have $\mathbb{N}^n = \cup_{j=1}^{s} \Delta_j \cup \overline{\Delta}$

Proposition 6 *Any monomial* X^α *occuring in the remainder* r *verifies* $\alpha \in \overline{\Delta}$. *If* X^β *is a monomial occuring in* a_i, *then* $\beta + \alpha(i) \in \Delta_i$.

PROOF: *(On the blackboard...)* ☐

About unicity (2/3)

Corollary 1 *Let $\prec$ be a monomial order on a polynomial algebra in n variables $\Bbbk[X_1, \ldots, X_n]$. Given a polynomial f and a sequence of polynomials $[f_1, \ldots, f_s]$, the remainder r and the sequence $[a_1, \ldots .a_s]$ computed by the division algorithm, are unique.*

PROOF:*(On the blackboard…)* □

Corollary 2 *If we fix the sequence $[f_1, \ldots, f_s]$ as above, then the map:*

$$\begin{array}{rcl} \Bbbk[X_1, \ldots, X_n] & \to & \Bbbk[X_1, \ldots, X_n] \\ f & \mapsto & r, \end{array}$$

is well-defined (unicity of the previous Corollary) and linear.

PROOF:*(On the blackboard…)* □

About unicity (3/3)

Let $I = \langle f_1, \ldots, f_s \rangle$ be the ideal generated by the polynomial system $(f_i)_{1 \le i \le s}$ (as in the previous slide).

Aim: Like for the Euclidean division, we would like a linear map

$$\begin{array}{rcl} \mathbb{k}[X_1, \ldots, X_n]/I & \longrightarrow & \mathbb{k}[X_1, \ldots, X_n] \\ f + I & \longmapsto & r. \end{array} \qquad \textit{(this map is not correct in general!)}$$

The ideal I would be the kernel of the map of Corollary 2.

But it **doesn't work** in general: the remainder r depends on the sequence $[f_1, \ldots, f_s]$ and not on the ideal $\langle f_1, \ldots, f_s \rangle$ (easy counter-examples).

Also, if $r = 0$ then $f \in I$, but there are some $g \in I$ whose division by $[f_1, \ldots, f_s]$ does **not** give a remainder $r = 0$.

However, if $f_1, \ldots, f_s$ is a **Gröbner basis**, it is OK...