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 IV: Gröbner bases

May, 20th 2010. Part I: Monomial ideals

May, 27th 2010. Part II: Definition and first properties

Part I: Monomial ideals

Definition 1 *An ideal I of $\Bbbk[X_1, \ldots, X_n]$ is a* monomial ideal *if it is generated by some monomials: $I = \langle X^\alpha \mid \alpha \in \mathcal{A} \rangle$, where $\mathcal{A} \subset \mathbb{N}^n$ is a subset, non necessarily finite, of multi-integers.*

Example: $x^2 + xy^3 \in \langle x^2, y^3 \rangle$.

Lemma 1 • *A monomial X^β belongs to a monomial ideal $\langle X^\alpha \mid \alpha \in \mathcal{A} \rangle$ iff there exists $\alpha \in \mathcal{A}$, such that $X^\alpha | X^\beta$.*

• *A polynomial $f \in \langle X^\alpha \mid \alpha \in \mathcal{A} \rangle$, iff each monomial occuring in f is in $\langle X^\alpha \mid \alpha \in \mathcal{A} \rangle$.*

Proof: *(On the blackboard. . .)* □

Corollary 1 *Let $I = \langle X^{\alpha(1)}, \ldots, X^{\alpha(s)} \rangle$, be a finitely generated monomial ideal. The remainder of the division of a polynomial $f \in I$ by the monomials $X^{\alpha(1)}, \ldots, X^{\alpha(s)}$, is* always *null (*whatever *the sequence order these monomials are taken to perform the division).*

Dickson's lemma

Corollary 2 *Two monomial ideals are equal if and only they contain the same monomials.*

PROOF:Exercise 5 of Practice test II. □

Actually, all monomial ideals are finitely generated.

Theorem 1 (Dickson's lemma) *Let I be a monomial ideal, generated by an* infinite *family $\{X^\alpha \mid \alpha \in \mathcal{A}\}$ of monomials. There exists a* finite *subfamily $\mathcal{A}' \subset \mathcal{A}$ such that $I = \langle X^\alpha \mid \alpha \in \mathcal{A}' \rangle$.*

PROOF:We must show that there exists some multi-integers $\alpha(1), \ldots, \alpha(s) \in \mathcal{A}$ such that $I = \langle X^{\alpha(1)}, \ldots, X^{\alpha(s)} \rangle$.

By induction on the number of variables n. If $n = 1$, then the monomial of minimal degree generates the ideal.
If $n > 1$ …… *(the end on the blackboard)* □

New definition of monomial orders

Definition 2 *A* monomial order $\prec$ *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.*

(iii') *For all monomials* X^α*,* $\alpha \in \mathbb{N}^n$*, holds:* $\alpha \succcurlyeq (0, \ldots, 0)$*.*

Proof:(iii) $\Rightarrow$ (iii'). The whole set of monomials admit a smallest element, denoted α_0. If $\alpha_0 \prec 0$, then by Property (ii), $2\alpha_0 \prec \alpha_0$ is even smaller, contradicts the minimality of α_0.

(iii') $\Rightarrow$ (iii) ...... *(on the blackboard)* $\square$

Ideal of leading terms

Definition 3 *Let $\prec$ be a monomial order, and $I \subset \Bbbk[X_1, \ldots, X_n]$ be a non-zero ideal. Let*

$$\text{LM}_\prec(I) := \{X^\alpha \textit{ s.t. } \exists f \in I \textit{ with } \text{LM}_\prec(f) = X^\alpha\}$$

The monomial ideal $\langle \text{LM}_\prec(I) \rangle$ is called the ideal of leading terms *of I.*

! Leading terms? It is possible to define similarly the ideal $\langle \text{LT}(I) \rangle$. Over a field $\Bbbk$, $\langle \text{LM}(I) \rangle = \langle \text{LT}(I) \rangle$ since the leading coefficient $\text{LC}(f)$ of the leading term $\text{LT}(f)$ of a polynomial in $f \in I$ can be inverted.

!! If $I = \langle f_1, \ldots, f_s \rangle$, then $\langle \text{LM}(f_1), \ldots, \text{LM}(f_s) \rangle \subsetneq \langle \text{LM}(I) \rangle$ (in general)

Example: $f_1 = X^3 - 2XY$ and $f_2 = X^2Y - 2Y^2 + X$, $\prec$ is the grlex monomial ordering. . . . . .

Hilbert's finite basis theorem

Theorem 2 *Every ideal* $I \subset \Bbbk[X_1, \ldots, X_n]$ *admits a finite basis.*

Proof:If $I = \{0\}$, there is nothing to do. If $\{0\} \subsetneq I$ ... *(on the blackboard)*

Definition 4 *A* Nœtherian ring *is a (commutative) ring* R *verifying the* ascending chain condition *(ACC):*

(ACC) All increasing sequences $(I_j)_{j \in \mathbb{N}}$ *of ideals of* R *stabilize:*

$\exists n \in \mathbb{N}$ *such that* $I_n = I_{n+1} = I_{n+2} = \cdots$.

Theorem 3 *The ring* $\Bbbk[X_1, \ldots, X_n]$ *is Nœtherian.*

Proof:Consider an increasing sequence $(I_j)_{j \in \mathbb{N}}$ of ideals and take $I = \bigcup_{j \in \mathbb{N}} I_j$. This is an ideal, it admits a finite basis by Theorem 1 etc......

Part II: Gröbner bases

Definition

Definition 5 *For a monomial order $\prec$ on a polynomial algebra $\Bbbk[X_1, \ldots, X_n]$ and an ideal I, a family $\{g_1, \ldots, g_s\}$ of polynomials in I is a* Gröbner basis *if:*

$$\langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s) \rangle = \langle \mathrm{LM}(I) \rangle. \qquad (\textit{correction}: \ \mathrm{LM} \textit{ not } \mathrm{LT})$$

Corollary 3 *Given a monomial order $\prec$, every non-zero ideal admits a Gröbner basis for $\prec$.*

Normal form (1/3)

Let $G = [g_1, \ldots, g_s]$ be some polynomials, $\prec$ a monomial order.

For any polynomial $f \in \mathbb{k}[X_1, \ldots, X_n]$ let $\text{NF}_\prec(f, G)$ denotes the remainder of the division of f by the sequence $[g_1, \ldots, g_s]$ with respect to (w.r.t.) the order $\prec$ (uniquely determined $\rightarrow$ Corollary 1).

If G is a Gröbner basis for $\prec$ of the ideal $I := \langle G \rangle$ it generates, then:

For all permutation $\sigma \in \mathfrak{S}_n$, we have:

$$\text{NF}_\prec(f, G) = \text{NF}_\prec(f, [g_{\sigma(1)}, \ldots, g_{\sigma(n)}]). \tag{1}$$

$\rightarrow$ the remainder does not depend on the order of the sequence of polynomials by which f is divided.

!! But if $f = a_1 g_1 + \cdots + a_s g_s + \text{NF}_\prec(f, G)$, and if $f = b_1 g_{\sigma(1)} + \cdots + b_s g_{\sigma(s)} + \text{NF}_\prec(f, G)$, then $b_i \neq a_{\sigma(i)}$, in general.

Normal form (2/3)

PROOF:Let r and r' be the remainders of the division of f by two differently ordered sequences of the same set of polynomials $\{g_1, \ldots, g_s\}$.

Then $r - r' \in I$, so if $r \neq r'$ then $\text{LM}(r - r') \in \text{LM}(I) \subset \langle \text{LM}(I) \rangle = \langle \text{LM}(g_1), \ldots, \text{LM}(g_s) \rangle$. By Lemma 1, there exists i such that $\text{LM}(g_i) | \text{LM}(r - r')$.

But both r and r' being remainders, all their terms are not divisible by any of the $\text{LM}(g_j)$, which contradicts $\text{LM}(g_i) | \text{LM}(r - r')$. Hence, $r = r'$. $\square$

Example: $G = \{x + y, y - z\}$ is a Gröbner basis for $x \succ_{lex} y$ (to check). The divisions of xy by $[x + y, y - z]$ and by $[y - z, x + y]$ are not the same (but the remainder $\text{NF}(xy, G) = -z^2$ is, verifying Equation (1)).

Practical consequence of the Normal Form (3/3)

Theorem 4 (ideal membership) *Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal of $\mathbb{k}[X_1, \ldots, X_n]$, $f \in \mathbb{k}[X_1, \ldots, X_n]$, and $\prec$ any monomial order on $\mathbb{k}[X_1, \ldots, X_n]$. Let G be a Gröbner basis of I w.r.t. to $\prec$. We have:*

$$f \in I \iff \mathrm{NF}_{\prec}(f, G) = 0.$$

PROOF: $\Leftarrow$ trivial. For $\Rightarrow$, see Exercise 6 of Practice test II. $\square$

Canonical representation of f mod I: With the notations above, the map:

$$\begin{array}{rcccc} \phi_G & : & \mathbb{k}[X_1, \ldots, X_n] & \longrightarrow & \mathbb{k}[X_1, \ldots, X_n] \\ & & f & \longmapsto & \mathrm{NF}_{\prec}(f, G), \end{array}$$

is linear (Lect. III, Slide 22). If we define $\phi_G(g_1 g_2) := \phi_G(\phi_G(g_1)\phi_G(g_2))$, then ϕ_G is a ring homomorphism.

By Theorem 4, $\boxed{\ker \phi_G = I} \overset{\text{Lect. II,Slide 11}}{\Longrightarrow} \mathbb{k}[X_1, \ldots, X_n]/I \hookrightarrow \mathbb{k}[X_1, \ldots, X_n]$.

Minimal Gröbner basis

Fact: According to the definition, if $\{g_1, \ldots, g_s\}$ is a Gröbner basis, then any $\{g_1, \ldots, g_s\} \cup \{g_i + g_j\}$ is also a Gröbner basis. Of course, $g_i + g_j$ is useless !

We have $g_i + g_j \in \langle g_1, \ldots, g_s \rangle = I$, so
$\text{LM}(g_1 + g_2) \in \langle \text{LM}(I) \rangle = \langle \text{LM}(g_1), \ldots, \text{LM}(g_s) \rangle$.

So $\{g_1, \ldots, g_s, g_i + g_j\}$ is a non-minimal Gröbner basis.

$\longrightarrow$ Refinement of the definition of Gröbner bases:

Definition 6 *A* minimal Gröbner basis *of a polynomial ideal I (for a given monomial order) is a Gröbner basis G of I such that:*

(i) For all $p \in G$, $\text{LM}(p) \notin \langle \text{LM}(G - \{p\}) \rangle$

If the additional condition,

(ii) $\text{LC}(P) = 1$ for all $P \in G$.

holds, then the minimal Gröbner basis G is monic.

Extraction of a minimal Gröbner basis

In practice: Very easy to remove redundant polynomials of a Gröbner basis: check only the leading monomials.

Extraction: Given a Gröbner basis G, how to compute the a minimal Gröbner basis G' from G ?

Let $p \in G$. If $\mathrm{LM}(p) \in \langle \mathrm{LM}(G - \{p\}) \rangle$ then we can remove p from G:
$\langle \mathrm{LM}(G - \{p\}) \rangle = \langle \mathrm{LM}(G) \rangle \overset{\text{by\_def}}{=} \langle \mathrm{LM}(I) \rangle$. OK !

Algorithm of extraction.

`# Input:` A Gröbner basis $G = \{g_1, \ldots, g_s\} \subset \mathbb{k}[X_1, \ldots, X_n]$ of an ideal I, for a monomial order $\prec$.

`# Output:` A minimal Gröbner basis $G' = \{g'_1, \ldots, g'_t\}$ of I such that: $t \leq s$ and for $i = 1, \ldots, t$ holds $g'_i \in G$.

1: $G' \leftarrow [g_1]$; $s' \leftarrow 1$ // s' is the caridnal of G'

2: **for** $i = 2, \ldots, s$ **do**

3:   $j \leftarrow 1$; $g' \leftarrow G'[j]$ // given a list $L = [L_1, \ldots, L_t]$, $L[j]$ means L_j

4:   **while** $(j \leq s'$ **and** $\mathrm{LM}(g_i) \nmid \mathrm{LM}(g')$ **and** $\mathrm{LM}(g') \nmid \mathrm{LM}(g_i))$ **do**

    $j \leftarrow j + 1$; $g' \leftarrow G'[j]$

  end while

5:   **if** $(j = s' + 1)$ **then** $G' \leftarrow G'$ cat $[g_i]$; $s' \leftarrow s' + 1$ // "cat" means...

    else // ...concatenate. Example: [1,3,6] cat [4]=[1,3,6,4]

6:     **if** $(\mathrm{LM}(g_i) | \mathrm{LM}(g'))$ **then** $G' \leftarrow (G' - g')$ cat $[g_i]$ // the symbol $-$ ...

    end if // ...means "remove". Example $[1, 3, 6, 4] - [3] = [1, 6, 4]$

  end if

end for

7: **return** G'

Reduced Gröbner bases

Question: Given a polynomial ideal I, is a minimal Gröbner basis of I (for a given monomial order) unique ? No! For example $\{y, x - \frac{b}{a}y\}$, for any b and any $a \neq 0$ are all minimal Gröbner bases for $y \prec_{lex} x$.
$\rightarrow$ another refinement of the definition of Gröbner basis:

Definition 7 *A Gröbner basis G is* reduced *if:*
(ii) $\forall p \in G$, all monomials m occurring in p, $m \notin \langle \mathrm{LM}(G - \{p\}) \rangle$.
Moreover, it is a reduced monic *Gröbner basis if:*
(ii) $\mathrm{LC}(p) = 1$ for all $p \in G$.

Lemma 2 *There exists a reduced Gröbner basis, and a* unique monic *one.*

Proof:Existence: Modify the initial Gröbner basis (that we can assume to be *minimal*) until each of its element is reduced ($g \in G'$ is reduced $\overset{\text{def}}{\Leftrightarrow}$ no monomials occurring in g are in $\langle \mathrm{LM}(G') \rangle$) ... *(end on the blackboard)* □