Gröbner deformations

Matteo Varbaro (University of Genoa, Italy)

CIME-CIRM Course on
Recent Developments in Commutative Algebra
Levico Terme, 1-5/7/2019

Notation and basic definitions

- $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- K any field.
- $R = K[X_1, \ldots, X_n]$ the polynomial ring in n variables over K.
- A *monomial* of R is an element $X^u := X_1^{u_1} \cdots X_n^{u_n} \in R$, where $u = (u_1, \ldots, u_n) \in \mathbb{N}^n$.
- $\mathrm{Mon}(R)$ is the set of monomials of R.
- A *term* of R is an element of the form $a\mu \in R$ where $a \in K$ and μ is a monomial.

Notice that every $f \in R$ can be written as a sum of terms: there exists a unique (finite) subset $\mathrm{supp}(f) \subset \mathrm{Mon}(R)$ such that:

$$f = \sum_{\mu \in \mathrm{supp}(f)} a_\mu \mu, \qquad a_\mu \in K \setminus \{0\}.$$

In the above representation, the only lack of uniqueness is the order of the terms.

Definition

A *monomial order* on R is a total order $<$ on $\mathrm{Mon}(R)$ such that:

(i) $1 \leq \mu$ for every $\mu \in \mathrm{Mon}(R)$;

(ii) If $\mu_1, \mu_2, \nu \in \mathrm{Mon}(R)$ such that $\mu_1 \leq \mu_2$, then $\mu_1\nu \leq \mu_2\nu$.

Notice that, if $<$ is a monomial order on R and μ, ν are monomials such that $\mu|\nu$, then $\mu \leq \nu$: indeed $1 \leq \nu/\mu$, so

$$\mu = 1 \cdot \mu \leq (\nu/\mu) \cdot \mu = \nu.$$

Notation and basic definitions

Typical examples of monomial orders are the following: given monomials $\mu = X_1^{u_1} \cdots X_n^{u_n}$ and $\nu = X_1^{v_1} \cdots X_n^{v_n}$ we define:

- The *lexicographic order* (Lex) by $\mu <_{\text{Lex}} \nu$ iff $u_k < v_k$ for some k and $u_i = v_i$ for any $i < k$.
- The *degree lexicographic order* (DegLex) by $\mu <_{\text{DegLex}} \nu$ iff $\deg(\mu) < \deg(\nu)$ or $\deg(\mu) = \deg(\nu)$ and $\mu <_{Lex} \nu$.
- The *(degree) reverse lexicographic order* (RevLex) by $\mu <_{\text{RevLex}} \nu$ iff $\deg(\mu) < \deg(\nu)$ or $\deg(\mu) = \deg(\nu)$ and $u_k > v_k$ for some k and $u_i = v_i$ for any $i > k$.

Example

In $K[X, Y, Z]$, assuming $X > Y > Z$, we have $X^2 >_{\text{Lex}} XZ >_{\text{Lex}} Y^2$, while $X^2 >_{\text{RevLex}} Y^2 >_{\text{RevLex}} XZ$.

Proposition

A monomial order on R is a well-order on $\mathrm{Mon}(R)$. That is, any nonempty subset of $\mathrm{Mon}(R)$ has a minimum. Equivalently, all descending chains of monomials in R terminate.

Proof: Let $\emptyset \neq N \subset \mathrm{Mon}(R)$, and $I \subset R$ be the ideal generated by N. By Hilbert basis theorem, I is generated by a finite number of monomials of N. Since a monomial order refines divisibility, the minimum of such finitely many monomials is also the minimum of N. $\square$

Notation and basic definitions

From now on, we fix a monomial order $<$ on R, so that every polynomial $0 \neq f \in R$ can be written uniquely as

$$f = a_1\mu_1 + \ldots + a_k\mu_k$$

with $a_i \in K \setminus \{0\}$, $\mu_i \in \mathrm{Mon}(R)$ and $\mu_1 > \mu_2 > \ldots > \mu_k$.

Definition

The *initial monomial* of f is $\mathrm{in}(f) = \mu_1$. Furthermore, its *initial coefficient* is $\mathrm{inic}(f) = a_1$ and its *initial term* is $\mathrm{init}(f) = a_1\mu_1$.

Notice that, for all $f, g \in R$:

- $\mathrm{inic}(f)\,\mathrm{in}(f) = \mathrm{init}(f)$.
- $\mathrm{in}(fg) = \mathrm{in}(f)\,\mathrm{in}(g)$.
- $\mathrm{in}(f+g) \leq \max\{\mathrm{in}(f), \mathrm{in}(g)\}$.

Notation and basic definitions

Example

If $f = X_1 + X_2X_4 + X_3^2$, we have:

- $\mathrm{in}(f) = X_1$ with respect to Lex.
- $\mathrm{in}(f) = X_2X_4$ with respect to DegLex.
- $\mathrm{in}(f) = X_3^2$ with respect to RevLex.

Example

If $f = X^2 + XY + Y^2 \in K[X, Y]$, then we have:

- $\mathrm{in}(f) = X^2$ if $X > Y$.
- $\mathrm{in}(f) = Y^2$ if $Y > X$.

In particular, $XY \neq \mathrm{in}(f)$ for all monomial orders.

Gröbner bases and Buchberger algorithm

Definition

If I is an ideal of R, then the monomial ideal $\mathrm{in}(I) \subset R$ generated by $\{\mathrm{in}(f) : f \in I\}$ is named the *initial ideal* of I.

Definition

Polynomials $f_1, \ldots, f_m$ of an ideal $I \subset R$ are a *Gröbner basis* of I if $\mathrm{in}(I) = (\mathrm{in}(f_1), \ldots, \mathrm{in}(f_m))$.

Example

Consider the ideal $I = (f_1 = X^2 - Y^2, f_2 = XZ - Y^2)$ of $K[X, Y, Z]$. For Lex with $X > Y > Z$ the polynomials f_1, f_2 are not a Gröbner basis of I, indeed $XY^2 = \mathrm{in}(Zf_1 - Xf_2)$ is a monomial of $\mathrm{in}(I)$ which is not in $(\mathrm{in}(f_1) = X^2, \mathrm{in}(f_2) = XZ)$. For RevLex with $X > Y > Z$, it turns out that $\mathrm{in}(I) = (X^2, Y^2)$, so f_1 and f_2 are a Gröbner basis of I in this case.

Remark

The Noetherianity of R implies that any ideal in R has a finite Gröbner basis.

There is a way to compute a Gröbner basis of an ideal I starting from a system of generators of I, namely the *Buchsberger algorithm*; it also checks if such a system of generators is already a Gröbner basis. We will develop the algorithm in the next few slides:

Definition

Let $f_1, \ldots, f_m \in R$. A polynomial $r \in R$ is a *reduction of* $g \in R$ *modulo* $f_1, \ldots, f_m$ if there exist $q_1, \ldots, q_m \in R$ satisfying:

- $g = q_1 f_1 + \ldots + q_m f_m + r$;
- $\mathrm{in}(q_i f_i) \leq \mathrm{in}(g)$ for all $i = 1, \ldots, m$;
- For all $i = 1, \ldots, m$, $\mathrm{in}(f_i)$ does not divide $\mu \ \forall \ \mu \in \mathrm{supp}(r)$.

Lemma

Let $f_1, \ldots, f_m \in R$. Every polynomial $g \in R$ admits a reduction modulo $f_1, \ldots, f_m$.

Proof: Let $J = (\mathrm{in}(f_1), \ldots, \mathrm{in}(f_m))$. We start with $r = g$ and apply the *reduction algorithm*:

(1) If $\mathrm{supp}(r) \cap J = \emptyset$, we are done: r is the desired reduction.

(2) Otherwise choose $\mu \in \mathrm{supp}(r) \cap J$ and let $b \in K$ be the coefficient of μ in the monomial representation of r. Choose i such that $\mathrm{in}(f_i) \mid \mu$ and set $r' = r - a\nu f_i$ where $\nu = \mu / \mathrm{in}(f_i)$ and $a = b / \mathrm{inic}(f_i)$. Then replace r by r' and go to (1).

This algorithm terminates after finitely many steps since it replaces the monomial μ by a linear combination of monomials that are smaller in the monomial order, and all descending chains of monomials in R terminate. $\square$

Example

Once again, we take $R = K[X, Y, Z]$, $f_1 = X^2 - Y^2$ and $f_2 = XZ - Y^2$, and we consider Lex with $X > Y > Z$. Set $g = X^2Z$. Then $g = Zf_1 + Y^2Z$, but $g = Xf_2 + XY^2$ as well. Both these equations yield reductions of g, namely XY^2 and Y^2Z. Thus a polynomial can have several reductions modulo f_1, f_2.

The reduction of $g \in R$ modulo $f_1, \ldots, f_m$ is unique when $f_1, \ldots, f_m$ is a Gröbner basis...

Proposition

Let I be an ideal of R, $f_1, \ldots, f_m \in I$ and $J = (\mathrm{in}(f_1), \ldots, \mathrm{in}(f_m))$. Then the following are equivalent:

(a) $f_1, \ldots, f_m$ form a Gröbner basis of I;

(b) every $g \in I$ reduces to 0 modulo $f_1, \ldots, f_m$;

(c) the monomials μ, $\mu \notin J$, are linearly independent modulo I.

If the equivalent conditions (a), (b), (c) hold, then:

(d) Every element of R has a unique reduction modulo $f_1, \ldots, f_m$.

(e) The reduction depends only on I and the monomial order.

Proof: Check (a) $\Longrightarrow$ (c) $\Longrightarrow$ (b) as an exercise.

(b) $\Longrightarrow$ (a) Let $g \in I$, $g \neq 0$. If g reduces to 0, then we have

$$g = q_1 f_1 + \cdots + q_m f_m$$

such that $\mathrm{in}(q_i f_i) \leq \mathrm{in}(g)$ for all i. But the monomial $\mathrm{in}(g)$ must appear on the right hand side as well, and this is only possible if $\mathrm{in}(g) = \mathrm{in}(q_i f_i) = \mathrm{in}(q_i)\,\mathrm{in}(f_i)$ for at least one i. In other words, $\mathrm{in}(g)$ must be divisible by $\mathrm{in}(f_i)$ for some i. Hence $\mathrm{in}(I) = J$.

Check (c) $\Longrightarrow$ (d), (e) as an exercise. $\square$

Corollary

If $f_1, \ldots, f_m$ is a Gröbner basis of an ideal $I \subset R$ then $I = (f_1, \ldots, f_m)$.

Corollary

Let $I \subset R$ be an ideal and $<_1, <_2$ monomial orders of R. If $\text{in}_{<_1}(I) \subset \text{in}_{<_2}(I)$, then $\text{in}_{<_1}(I) = \text{in}_{<_2}(I)$.

Proof: By the previous proposition, the sets A_i of monomials of R not in $\text{in}_{<_i}(I)$ are K-bases of R/I for each $i = 1, 2$. Since $A_1 \supset A_2$, we must have $A_1 = A_2$. $\square$

Corollary

Let $I_1, I_2 \subset R$ be ideals and $<$ a monomial order of R. If $I_1 \subset I_2$ and $\text{in}_<(I_1) = \text{in}_<(I_2)$, then $I_1 = I_2$.

Proof: By the previous proposition, the set A of monomials of R not in $\text{in}_<(I_1) = \text{in}_<(I_2)$ are K-bases of R/I_i for each $i = 1, 2$. Since $I_1 \subset I_2$, we must have $I_1 = I_2$. $\square$

Definition

The *S-polynomial* of two elements $f, g \in R$ is defined as

$$S(f,g) = \frac{\operatorname{lcm}(\operatorname{in}(f), \operatorname{in}(g))}{\operatorname{init}(f)} f - \frac{\operatorname{lcm}(\operatorname{in}(f), \operatorname{in}(g))}{\operatorname{init}(g)} g$$

Proposition

Let $f_1, \ldots, f_m \in R$ and $I = (f_1, \ldots, f_m)$. Then the following are equivalent:

(a) $f_1, \ldots, f_m$ form a Gröbner basis of I.

(b) For all $1 \leq i < j \leq m$, $S(f_i, f_j)$ reduces to 0 modulo $f_1, \ldots, f_m$.

Proof: (a) $\implies$ (b): It follows since $S(f_i, f_j) \in I$.

(b) $\Longrightarrow$ (a): We need to show that every $g \in I$ reduces to 0 modulo the f_k's. Since $g \in I$, we have $g = a_1 f_1 + \ldots + a_m f_m$ for some $a_k \in R$. Among such representations, we can choose one minimizing $\mu := \max\{\mathrm{in}(a_i f_i) : i = 1, \ldots, m\}$ and, among these, minimizing $s := |\{i = 1, \ldots, m | \, \mathrm{in}(a_i f_i) = \mu\}|$. By contradiction, suppose $\mu > \mathrm{in}(g)$. In this case $s \geq 2$, so there exist $i < j$ such that $\mathrm{in}(a_i f_i) = \mathrm{in}(a_j f_j) = \mu$. Set $c := \mathrm{inic}(a_i f_i)$ and notice that $\mu = \nu \cdot \mathrm{lcm}(\mathrm{in}(f_i), \mathrm{in}(f_j))$ for some $\nu \in \mathrm{Mon}(R)$. Let

$$S(f_i, f_j) = q_1 f_1 + \ldots + q_m f_m$$

the reduction of $S(f_i, f_j)$ (so that $\mathrm{in}(q_k f_k) \leq \mathrm{in}(S(f_i, f_j))$ which is less than $\alpha_{ij} := \mathrm{lcm}(\mathrm{in}(f_i), \mathrm{in}(f_j))$ for all k). From this we get a representation $g = a'_1 f_1 + \ldots + a'_m f_m$ contradicting the minimality of μ and s where $a'_i = a_i - \frac{c\nu\alpha_{ij}}{\mathrm{init}(f_i)} + c\nu q_i$, $a'_j = a_j + \frac{c\nu\alpha_{ij}}{\mathrm{init}(f_j)} + c\nu q_j$ and $a'_k = a_k + c\nu q_k$ for $i \neq k \neq j$. $\square$