Involutive Bases and Its Applications

Amir Hashemi

Isfahan University of Technology & IPM

Seminar on Commutative Algebra and Related Topics, November 16, 2016

Outline of talk

1. Introduction
2. Gröbner bases
   - Monomial Orderings
   - Gröbner Bases
   - Computation of Gröbner Bases
   - History of Gröbner Bases
   - Applications
3. Involutive Bases
   - Involutive Division
   - Involutive Bases
   - Applications

What is algebraic geometry?

Studying geometric objects by means of algebraic tools and in particular studying polynomial systems

$$\begin{cases} f_1 &= 0 \\ & \vdots \\ f_k &= 0. \end{cases}$$

This is a well-known geometric object. In this direction, we introduce *Gröbner bases* and *involutive bases*.

Notations

- K; a field e.g. $K = \mathbb{R}, \mathbb{Q}, \ldots$
- $x_1, \ldots, x_n$; a sequence of variables
- A polynomial is a sum of products of numbers and variables, e.g.

$$f = x_1 x_2 + 12x_1 - x_2^3$$

- $R = K[x_1, \ldots, x_n]$; set of all polynomials
- $f_1, \ldots, f_k \in R$ and $F = \{f_1, \ldots, f_k\}$
- $I = \langle F \rangle = \{p_1 f_1 + \cdots + p_k f_k \mid p_i \in R\}$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x-1, x^2-1 \rangle = \langle x-1 \rangle$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \dots, f_k \in K[x]$ then $\langle f_1, \dots, f_k \rangle = \langle gcd(f_1, \dots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x - 1, x^2 - 1 \rangle = \langle x - 1 \rangle$
- Thus, gcd computations (using Euclid algorithm) can solve many problems in $K[x]$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x-1, x^2-1 \rangle = \langle x-1 \rangle$
- Thus, gcd computations (using Euclid algorithm) can solve many problems in $K[x]$
- Suppose that

$$f := x^3 - 6x^2 + 11x - 6$$
$$g := x^3 - 10x^2 + 29x - 20$$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x-1, x^2-1 \rangle = \langle x-1 \rangle$
- Thus, gcd computations (using Euclid algorithm) can solve many problems in $K[x]$
- Suppose that

$$f := x^3 - 6x^2 + 11x - 6$$
$$g := x^3 - 10x^2 + 29x - 20$$

- Since $gcd(f,g) = x - 1$,
  every information about $\langle f, g \rangle$ is given by $\langle x - 1 \rangle$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x-1, x^2-1 \rangle = \langle x-1 \rangle$
- Thus, gcd computations (using Euclid algorithm) can solve many problems in $K[x]$
- Suppose that

$$f := x^3 - 6x^2 + 11x - 6$$
$$g := x^3 - 10x^2 + 29x - 20$$

- Since $gcd(f, g) = x - 1$,
  every information about $\langle f, g \rangle$ is given by $\langle x - 1 \rangle$
- For example, the only solution of $f = g = 0$ is $x = 1$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x-1, x^2-1 \rangle = \langle x-1 \rangle$
- Thus, gcd computations (using Euclid algorithm) can solve many problems in $K[x]$
- Suppose that

$$f := x^3 - 6x^2 + 11x - 6$$

$$g := x^3 - 10x^2 + 29x - 20$$

- Since $gcd(f, g) = x - 1$,
  every information about $\langle f, g \rangle$ is given by $\langle x - 1 \rangle$
- For example, the only solution of $f = g = 0$ is $x = 1$
- Membership Problem: $x^2 - 1 \in \langle f, g \rangle$ because $x - 1 \mid x^2 - 1$.

Two Questions

- ☞ $R = K[x_1, \ldots, x_n]$; a multivariate polynomial ring
- ☞ $\{f_1, \ldots, f_k\} \subset R$; a finite set of polynomials
- ☞ $I \subset R$; an ideal
  - Solving polynomial systems $f_1 = \cdots = f_k = 0$?
  - Membership problem: $h \in I$?
  - In practice, the answer to these questions is not easy!

Two Questions

- $R = K[x_1, \ldots, x_n]$; a multivariate polynomial ring
- $\{f_1, \ldots, f_k\} \subset R$; a finite set of polynomials
- $I \subset R$; an ideal
  - Solving polynomial systems $f_1 = \cdots = f_k = 0$?
  - Membership problem: $h \in I$?
  - In practice, the answer to these questions is not easy!
  - Gröbner bases can answer them!

Gröbner Bases

Polynomial Ring

☞ K a field

- ▷ We denote the *monomial* $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ by X^α with $\alpha = (\alpha_1, \ldots, \alpha_n)$
- ▷ $\{$monomials in $R\} \leftrightarrow \mathbb{N}^n$
- ▷ If X^α is a monomial and $a \in K$, then aX^α is a *term*
- ▷ A polynomial is a finite sum of terms.

☞ $R = K[x_1, \ldots, x_n]$; the ring of all polynomials.

Definition

A monomial ordering is a total ordering $\prec$ on the set of monomials $X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ such that,

- $X^\alpha \prec X^\beta \Rightarrow X^{\alpha+\gamma} \prec X^{\beta+\gamma}$ and
- $\prec$ is well-ordering.

Lexicographical Ordering

$X^\alpha \prec_{lex} X^\beta$ if leftmost nonzero of $\beta - \alpha$ is > 0

- Example
  $x_1^2 x_2^3 \prec_{lex} x_1^3 x_2^2$

Notations

- ☞ $R = K[x_1, \ldots, x_n], f \in R$
- ☞ $\prec$ a monomial ordering on R
- ☞ $I \subset R$ an ideal

$\mathrm{LM}(f)$: The greatest monomial (with respect to $\prec$) in f
$5x^3y^2 + 4x^2y^3 + xy + 1$

$\mathrm{LM}(I)$: $\langle \mathrm{LM}(f) \mid f \in I \rangle$; the leading monomial ideal of I.

Definition

- $I \subset K[x_1, \ldots, x_n]$
- $\prec$ A monomial ordering
- A finite set $\{g_1, \ldots, g_t\} \subset I$ is a Gröbner Basis for I w.r.t. $\prec$, if $\mathrm{LM}(I) = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t) \rangle$.

Existence of Gröbner bases

Each ideal has a Gröbner basis

Example

$I = \langle xy - x, x^2 - y \rangle$, $y \prec_{lex} x$
$\mathrm{LM}(I) = \langle xy, x^2, y^2 \rangle$
$\equiv \forall f \in I$ either $x^2 \mid \mathrm{LM}(f)$ or $xy \mid \mathrm{LM}(f)$ or $y^2 \mid \mathrm{LM}(f)$
A Gröbner basis is: $\{xy - x, x^2 - y, y^2 - y\}$.

Division Algorithm in $K[x_1, \ldots, x_n]$

Theorem

Fix a monomial ordering $\prec$ and let $F := (f_1, \ldots, f_k)$ be an ordered $k-$tuple of polynomials in $K[x_1, \ldots, x_n]$ Then, every $f \in K[x_1, \ldots, x_n]$ can be written as

$$f = q_1 f_1 + \cdots + q_k f_k + r$$

where $q_i, r \in K[x_1, \ldots, x_n]$ and either $r = 0$ or no term of r is divisible by any of $\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_k)$. We call r, the remainder on division of f by F.

Algorithm 1 DIVISION ALGORITHM

Require: $f, f_1, \ldots, f_k$ and $\prec$
Ensure: $q_1, \ldots, q_k, r$

$q_1 := 0; \cdots ; q_k := 0;$
$p := f;$
while $\exists f_i$ s.t. $\mathrm{LM}(f_i)$ divides a term m in p **do**
    $q_i := q_i + \frac{m}{\mathrm{LM}(f_i)}$
    $p := p - (\frac{m}{\mathrm{LM}(f_i)})f_i$
end while
return $q_1, \ldots, q_k, p$

Example

- Divide $f = xy^2 + 1$ by $f_1 = xy + 1, f_2 = y + 1$ and $y \prec_{lex} x$

Example

- Divide $f = xy^2 + 1$ by $f_1 = xy + 1, f_2 = y + 1$ and $y \prec_{lex} x$
- $f \to (xy^2 + 1) - y(xy + 1) = 1 - y \to (1 - y) + (y + 1) = 2$

Example

- Divide $f = xy^2 + 1$ by $f_1 = xy + 1, f_2 = y + 1$ and $y \prec_{lex} x$
- $f \to (xy^2 + 1) - y(xy + 1) = 1 - y \to (1 - y) + (y + 1) = 2$
- So we can write $f = y(xy + 1) + (-1)(y + 1) + 2$

Buchberger's Criterion

Definition

S-polynomial

$$\mathrm{Spoly}(f,g) = \frac{x^\gamma}{\mathrm{LM}(f)}f - \frac{x^\gamma}{\mathrm{LM}(g)}g$$

$$x^\gamma = lcm(\mathrm{LM}(f), \mathrm{LM}(g))$$

$$\mathrm{Spoly}(x^3y^2+xy^3, xyz-z^3) = z(x^3y^2+xy^3) - x^2y(xyz-z^3) = zxy^3 + x^2yz^3$$

Buchberger's Criterion

- G is a Gröbner basis for $\langle G \rangle$
- $\forall g_i, g_j \in G$, remainder$((\mathrm{Spoly}(g_i,g_j), G) = 0$

Algorithm 2 BUCHBERGER'S ALGORITHM

Require: $F := (f_1, \ldots, f_s)$ and $\prec$

Ensure: A Gröbner basis for the ideal $\langle f_1, \ldots, f_s \rangle$ w.r.t. $\prec$

$G := F$

$B := \{\{f, g\} | f, g \in F\}$

while $B \neq \emptyset$ **do**

Select and remove a pair $\{f, g\}$ from B

Let r be the remainder of $\mathrm{Spoly}(f, g)$ by F

if $r \neq 0$ **then**

$B := B \cup \{\{h, r\} \mid h \in G\}$

$G := G \cup \{r\}$

end if

end while

return G

Example

$I = \langle f_1, f_2 \rangle = \langle xy - x, x^2 - y \rangle \quad y \prec_{lex} x$

$G := \{f_1, f_2\}$

$\text{Spoly}(f_1, f_2) = xf_1 - yf_2 = y^2 - x^2 \xrightarrow{f_2} y^2 - y = f_3$

$G := \{f_1, f_2, f_3\}$

$\text{Spoly}(f_i, f_j) \xrightarrow{G} 0$

$G := \{f_1, f_2, f_3\}$ is a Gröbner basis for I

Buchberger, 65 :

- Developing the theory of Gröbner bases
- Buchberger criteria

Lazard, 83 :

- Using linear algebra

Gebauer, Möller, 88 :

- Installing Buchberger criteria

Faugère, 99, 02 :

- F_4 algorithm (intensive linear algebra)
- F_5 algorithm

Basis for quotient rings

☞ $I \subset K[x_1, \ldots, x_n]$ an ideal and $\prec$ a monomial ordering on R

Theorem (Macaulay's theorem)

The set of all monomials m s.t. $m \notin \mathrm{LM}(I)$ is a basis for R/I as a K-vector space. Indeed, $R/I \simeq R/\mathrm{LM}(I)$ as K-vector space isomorphism.

Example

▷ $I = \langle xy - x, x^2 - y \rangle$, $y \prec_{lex} x$

Basis for quotient rings

☞ $I \subset K[x_1, \ldots, x_n]$ an ideal and $\prec$ a monomial ordering on R

Theorem (Macaulay's theorem)

The set of all monomials m s.t. $m \notin \mathrm{LM}(I)$ is a basis for R/I as a K-vector space. Indeed, $R/I \simeq R/\mathrm{LM}(I)$ as K-vector space isomorphism.

Example

- ▷ $I = \langle xy - x, x^2 - y \rangle$, $y \prec_{lex} x$
- ▷ The Gröbner basis of I is $G = \{xy - x, x^2 - y, y^2 - y\}$
- ⇒ $\mathrm{LM}(I) = \langle x^2, xy, y^2 \rangle$ and therefore $\{1, x, y\}$ is a basis for R/I as a K-vector space.

Ideal Membership

Theorem

$f \in I$ *iff* $f \rightsquigarrow_G 0$ *where* G *is a GB of* I

Example

- $I = \langle xy - x, x^2 - y \rangle$
- $y^2 + y \in I?$

Ideal Membership

Theorem

$f \in I$ *iff* $f \rightsquigarrow_G 0$ *where* G *is a GB of* I

Example

- ▷ $I = \langle xy - x, x^2 - y \rangle$
- ▷ $y^2 + y \in I$?
- ▷ $y \prec_{lex} x$
- ▷ The Gröbner basis of I is $G = \{xy - x, x^2 - y, y^2 - y\}$

⇒ $y^2 + y \rightsquigarrow_G 2y \neq 0$, and thus $y^2 + y \notin I$.

Ideal Membership (cont.)

Theorem (Weak Hilbert's Nullstellensätz)

$f_1 = \cdots = f_k = 0$ *has no solution iff* $\Leftrightarrow 1 \in \langle f_1, \ldots, f_k \rangle \Leftrightarrow 1 \in G$

Example

- ▷ $\{x^2+3y+z-1, x-3y^2-z^2, x-y, y^2-zxy-x, x^2-y\}$
- ▷ $I = \langle f_1, f_2, f_3, f_4 \rangle$
- ▷ $z \prec_{lex} y \prec_{lex} x$
- ▷ The Gröbner basis of I is $= \{1\}$
- $\Rightarrow$ The system $f_1 = f_2 = f_3 = f_4 = 0$ has no solution!

Radical Membership

☞ $I = \langle f_1, \ldots, f_k \rangle \subset K[x_1, \ldots, x_n]$

Theorem

$$f \in \sqrt{I} \text{ iff } 1 \in \langle f_1, \ldots, f_k, 1 - wf \rangle \subset K[x_1, \ldots, x_n, w]$$

Example

- ▷ $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle$
- ▷ $f = y - x + 1 \in \sqrt{I}$?

Radical Membership

☞ $I = \langle f_1, \dots, f_k \rangle \subset K[x_1, \dots, x_n]$

Theorem

$$f \in \sqrt{I} \text{ iff } 1 \in \langle f_1, \dots, f_k, 1 - wf \rangle \subset K[x_1, \dots, x_n, w]$$

Example

▷ $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle$

▷ $f = y - x + 1 \in \sqrt{I}$?

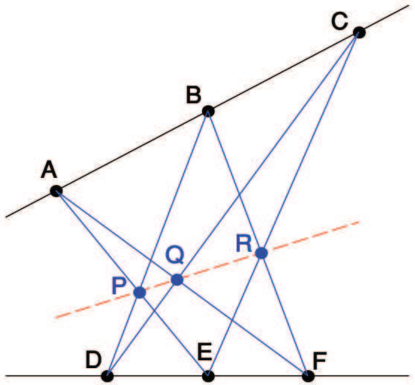
▷ The Gröbner basis of $I + \langle 1 - wf \rangle$ is $\{1\}$

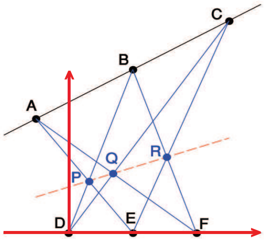
$\Rightarrow$ $f \in \sqrt{I}$ (indeed $f^3 \in I$).

Automatic Geometry Theorem Proving

Example

Pappus theorem: P, Q and R are collinear





Coordinate of points:

$$D := (0,0) \quad E := (u_1, 0) \quad F := (u_2, 0)$$
$$A := (u_3, u_4) \; B := (u_5, u_6) \; C := (u_7, x_1)$$
$$P := (x_2, x_3) \; Q := (x_4, x_5) \; R := (x_6, x_7)$$

- Since A, B, C are collinear, we have $\frac{u_5-u_3}{u_6-u_4} = \frac{u_7-u_3}{x_1-u_4}$ and so from the collinearity of points we obtain:

- Since A, B, C are collinear, we have $\frac{u_5-u_3}{u_6-u_4} = \frac{u_7-u_3}{x_1-u_4}$ and so from the collinearity of points we obtain:
- Hypothesis polynomials

$$
\begin{aligned}
h_1 &:= x_1u_3 + u_6u_7 - u_6u_3 - x_1u_5 - u_4u_7 + u_4u_5 = 0 \\
h_2 &:= u_4u_1 + x_3u_3 - x_3u_1 - u_4x_2 = 0 \\
h_3 &:= u_5x_3 - u_6x_2 = 0 \\
h_4 &:= u_4u_2 + x_5u_3 - x_5u_2 - u_4x_4 = 0 \\
h_5 &:= u_7x_5 - x_1x_4 = 0 \\
h_6 &:= u_6u_2 + x_7u_5 - x_7u_2 - u_6x_6 = 0 \\
h_7 &:= x_1u_1 + x_7u_7 - x_7u_1 - x_1x_6 = 0
\end{aligned}
$$

- Since A, B, C are collinear, we have $\frac{u_5-u_3}{u_6-u_4} = \frac{u_7-u_3}{x_1-u_4}$ and so from the collinearity of points we obtain:
- Hypothesis polynomials

$$
\begin{aligned}
h_1 &:= x_1u_3 + u_6u_7 - u_6u_3 - x_1u_5 - u_4u_7 + u_4u_5 = 0\\
h_2 &:= u_4u_1 + x_3u_3 - x_3u_1 - u_4x_2 = 0\\
h_3 &:= u_5x_3 - u_6x_2 = 0\\
h_4 &:= u_4u_2 + x_5u_3 - x_5u_2 - u_4x_4 = 0\\
h_5 &:= u_7x_5 - x_1x_4 = 0\\
h_6 &:= u_6u_2 + x_7u_5 - x_7u_2 - u_6x_6 = 0\\
h_7 &:= x_1u_1 + x_7u_7 - x_7u_1 - x_1x_6 = 0
\end{aligned}
$$

- Conclusion polynomial

$f := x_7x_2 + x_5x_6 - x_5x_2 - x_7x_4 - x_3x_6 + x_3x_4 = 0$

▷ $I := \langle h_1, \ldots, h_r \rangle \subset \mathbb{C}[x_1, \ldots, x_n, u_1, \ldots, u_m]$

- $I := \langle h_1, \ldots, h_r \rangle \subset \mathbb{C}[x_1, \ldots, x_n, u_1, \ldots, u_m]$

▷ $I := \langle h_1, \ldots, h_r \rangle \subset \mathbb{C}[x_1, \ldots, x_n, u_1, \ldots, u_m]$

Theorem

Conclusion is true iff $f \in \sqrt{I}$ *iff the Gröbner basis of*

$$\langle h_1, \ldots, h_r, 1 - wf \rangle \subset \mathbb{C}(u_1, \ldots, u_m)[x_1, \ldots, x_n, w]$$

equals to $\{1\}$

▷ $I := \langle h_1, \dots, h_r \rangle \subset \mathbb{C}[x_1, \dots, x_n, u_1, \dots, u_m]$

Theorem

Conclusion is true iff $f \in \sqrt{I}$ iff the Gröbner basis of

$$\langle h_1, \dots, h_r, 1 - wf \rangle \subset \mathbb{C}(u_1, \dots, u_m)[x_1, \dots, x_n, w]$$

equals to $\{1\}$

The Gröbner basis of

$$\langle h_1, \dots, h_7, 1 - wf \rangle \subset \mathbb{C}(u_1, \dots, u_7)[x_1, \dots, x_7, w]$$

is $\{1\}$, and therefore the Pappus theorem is true.

Involutive Bases

Involutive division

☞ $R = K[x_1, \ldots, x_n]$ a polynomial ring, $u, v \in U$ set of monomials

Definition (Gerdt-Blinkov, 1998)

An *involutive division* $\mathcal{L}$ (denoted by $|_{\mathcal{L}}$) on monomials of R is a separation $M_{\mathcal{L}}(u, U) \cup NM_{\mathcal{L}}(u, U) = \{x_1, \ldots, x_n\}$:

$\mathcal{L}(u, U)$: set of all monomials in $M_{\mathcal{L}}(u, U)$

$u\mathcal{L}(u, U) \cap v\mathcal{L}(v, U) \neq \emptyset \Longrightarrow u \in v\mathcal{L}(v, U)$ or $v \in u\mathcal{L}(u, U)$,

$v \in U,\ v \in u\mathcal{L}(u, U) \Longrightarrow \mathcal{L}(v, U) \subset \mathcal{L}(u, U)$,

$u \in V$ and $V \subset U \Longrightarrow \mathcal{L}(u, U) \subset \mathcal{L}(u, V)$,

Main idea

The idea is to partition $\{x_1, \ldots, x_n\}$ into two subsets of

1. Multiplicative variables
2. Non-multiplicative variables

Main idea

The idea is to partition $\{x_1, \ldots, x_n\}$ into two subsets of

1. Multiplicative variables
2. Non-multiplicative variables

$\Downarrow$

We restrict the usual division

$u|_{\mathcal{L}}v$ if $u|v$ and $\frac{v}{u}$ contains only multiplicative variables

Example

☞ $M_{\mathcal{P}}(x_1^{\alpha_1} \cdots x_k^{\alpha_k}) = \{x_k, \dots x_n\}$

Example (Pommaret division)

$U = \{x_1^2 x_3, x_1 x_2, x_1 x_3^2\}$, $u = x_1 x_2$, $R = K[x_1, x_2, x_3]$

- $\{x_2, x_3\}$ multiplicative
- $\{x_1\}$ non-multiplicative
- $x_1 x_2 |_{\mathcal{P}} x_1 x_2^2$ because $x_1 x_2^2 / x_1 x_2 = x_2$ is in terms of $\{x_2, x_3\}$
- $x_1 x_2 \not|_{\mathcal{P}} x_1^2 x_2$ because $x_1^2 x_2 / x_1 x_2 = x_1$ is not in terms of multiplicative

Example

☞ $M_{\mathcal{P}}(x_1^{\alpha_1} \cdots x_k^{\alpha_k}) = \{x_k, \ldots x_n\}$

Example (Pommaret division)

$U = \{x_1^2 x_3, x_1 x_2, x_1 x_3^2\}$, $u = x_1 x_2$, $R = K[x_1, x_2, x_3]$

- $\{x_2, x_3\}$ multiplicative
- $\{x_1\}$ non-multiplicative
- $x_1 x_2 |_{\mathcal{P}} x_1 x_2^2$ because $x_1 x_2^2 / x_1 x_2 = x_2$ is in terms of $\{x_2, x_3\}$
- $x_1 x_2 \not|_{\mathcal{P}} x_1^2 x_2$ because $x_1^2 x_2 / x_1 x_2 = x_1$ is not in terms of multiplicative

Example

Different kinds of involutive divisions have been proposed such as Janet, Thomas, (depending on the set U), Pommaret and Noether.

Involutive bases

Definition

$G \subset I$ a *Gröbner basis* for I if $\forall f \in I, \exists g \in G, \mathrm{LM}(g) | \mathrm{LM}(f)$

Involutive bases

Definition

$G \subset I$ a *Pommaret basis* for I if $\forall f \in I, \exists g \in G, \mathrm{LM}(g)|_{\mathcal{P}}\mathrm{LM}(f)$

Involutive bases

Definition

$G \subset I$ a *Pommaret basis* for I if $\forall f \in I, \exists g \in G, \mathrm{LM}(g)|_{\mathcal{P}}\mathrm{LM}(f)$

Example

$I = \langle x_1^2, x_2^2 \rangle$, then $\{x_1^2, x_2^2, x_1x_2^2\}$ is the Pommaret basis.

Involutive bases

Definition

$G \subset I$ a *Pommaret basis* for I if $\forall f \in I, \exists g \in G, \mathrm{LM}(g)|_{\mathcal{P}}\mathrm{LM}(f)$

Example

$I = \langle x_1^2, x_2^2 \rangle$, then $\{x_1^2, x_2^2, x_1 x_2^2\}$ is the Pommaret basis.

Theorem

Pommaret bases do not always exist but only in a generic position.

Quasi stable ideals

Definition (Quasi-stable ideal)

A monomial ideal $J \subset R$ is called *quasi-stable* if
$\forall m \in J$, $\forall i$ with $x_i^s \mid m$, $\exists t$ s.t. $x_j^t(m/x_i^s) \in J$ for all $j < i$.

Example

$I = \langle x_1^2, x_2^2 \rangle$ is quasi-stable because $x_1^2(x_2^2/x_2^2) \in J$.

Theorem (Seiler, 2009)

An ideal has a finite Pommaret basis iff it is quasi-stable.

History of involutive bases

[Zharkov and Blinkov, 96] :

- involutive polynomial bases
- the first algorithm

[Gerdt and Blinkov, 98] :

- general concept of involutive division

[Seiler, 09] :

- comprehensive study (of PB) and applications

Gröbner bases vs. involutive bases

1. Gröbner bases
   - Basis for R/I as a K-vector space
   - Hilbert function
   - Elimination Theory
2. Pommaret bases (due to its generic nature)
   - $\supset$ a Gröbner basis
   - Stanley decomposition
   - depth of ideal
   - satiety
   - Castelnuovo-Mumford regularity.

Stanley decomposition

☞ $M_{\mathcal{P}}(x_1^{\alpha_1} \cdots x_k^{\alpha_k}) = \{x_k, \dots x_n\}$

Definition

A Stanley decomposition for R/I is a K-linear isomorphism

$$R/I \simeq \bigoplus_{t \in T} K[X_t].t$$

where T is a finite set of monomials and $X_t \subset \{x_1, \dots, x_n\}$

Example

$I = \langle f_1 = x_1^3, f_2 = x_1^2 x_2 - x_1^2 x_3, f_3 = x_2^2 - x_2 x_3, f_4 = x_1 x_2^2 - x_1 x_2 x_3 \rangle$
$I = K[x_1, x_2, x_3].f_1 \oplus K[x_2, x_3].f_2 \oplus K[x_2, x_3].f_3 \oplus K[x_2, x_3].f_4$

Stanley decomposition

☞ $M_{\mathcal{P}}(x_1^{\alpha_1} \cdots x_k^{\alpha_k}) = \{x_k, \ldots x_n\}$

Definition

A Stanley decomposition for R/I is a K-linear isomorphism

$$R/I \simeq \bigoplus_{t \in T} K[X_t].t$$

where T is a finite set of monomials and $X_t \subset \{x_1, \ldots, x_n\}$

Example

$I = \langle f_1 = x_1^3, f_2 = x_1^2 x_2 - x_1^2 x_3, f_3 = x_2^2 - x_2 x_3, f_4 = x_1 x_2^2 - x_1 x_2 x_3 \rangle$
$R/I \simeq K \oplus K.x_1 \oplus K.x_2 \oplus K.x_3 \oplus K.x_1^2 \oplus K.x_1 x_2 \oplus K[x_3].x_3^3 \oplus K[x_3].x_1 x_3^2 \oplus K[x_3].x_2 x_3^2 \oplus K[x_3].x_1^2 x_3 \oplus K[x_3] x_1 x_2 x_3$

We can read off the dimension and Hilbert series of R/I.

Cohen-Macaulayness

Definition

The *depth* of I is the maximum integer λ so that there exists a a regular sequence of linear forms $y_1, \ldots, y_\lambda$ on R/I.

Theorem (Seiler, 2009)

The depth of an ideal generated by a Pommaret basis is $n - t$ *with* t *the maximum index of the elements of* H*. In addition,* $x_{t+1}, \ldots, x_n$ *form a regular sequence on* R/I

Example

$I = \langle x_1^3, x_1^2x_2 - x_1^2x_3, x_2^2 - x_2x_3, x_1x_2^2 - x_1x_2x_3 \rangle$. The maximum index is 2 and $\mathrm{depth}(I) = 3 - 2 = 1$. Since $\dim(I) = \mathrm{depth}(I)$ then R/I is Cohen-Macaulay and x_3 is regular on R/I.

Satiety

Definition

If $I^{\text{sat}} := I : \langle x_1, \ldots, x_n \rangle^{\infty}$ then $\text{sat}(I)$ is the smallest m so that for each $t \geq m$ we have $I_t^{\text{sat}} = I_t$.

Theorem (Seiler, 2009)

Let I be an ideal generated by a Pommaret basis H. Let $H_1 = \{h \in H | \ x_n$ divides $h\}$. Then, $\text{sat}(I) = \text{sat}(\text{LM}(I))$ and $\text{sat}(I) = \deg(H_1)$.

Example

$I = \langle x_1^3, x_1^2 x_2 - x_1^2 x_3, x_2^2 - x_2 x_3, x_1 x_2^2 - x_1 x_2 x_3 \rangle$. Since the Pommaret basis has no element divisible by x_3 then I is saturated and $\text{sat}(I) = 0$.

Castelnuovo-Mumford regularity

Definition

An ideal I is *m-regular*, if $\exists$ a minimal graded free resolution:
$0 \longrightarrow \bigoplus_j R(e_{rj}) \longrightarrow \cdots \longrightarrow \bigoplus_j R(e_{1j}) \longrightarrow \bigoplus_j R(e_{0j}) \longrightarrow I \longrightarrow 0$
of I such that $e_{ij} - i \leq m$ for each i, j. Then,
$\operatorname{reg}(I) = \min\{m \mid I \text{ is } m\text{-regular}\}$.

Theorem (Seiler, 2009)

Let I be an ideal generated by a Pommaret basis H. Then,
$\operatorname{reg}(I) = \operatorname{reg}(\operatorname{LM}(I)) = \max\{\deg(h) \mid h \in H\}$.

Example

$I = \langle x_1^3, x_1^2x_2 - x_1^2x_3, x_2^2 - x_2x_3, x_1x_2^2 - x_1x_2x_3\rangle$ and $\operatorname{reg}(I) = 3$.

References

[1] David Cox, John Little and Donal O'Shea:
Ideals, varieties, and algorithms.
Springer-Verlag, 2006.
[2] David Cox, John Little and Donal O'Shea:
Using algebraic geometry.
Springer-Verlag, 2005.
[3] Thomas Becker and Volker Weispfenning:
Gröbner bases, A computational approach to commutative algebra.
Springer-Verlag, 1993.
[4] Werner M. Seiler:
Involution.
Speringer-Verlag, 2010.