On lexicographic Gröbner bases in dimension zero

Xavier Dahan
GCOE Math-for-Industry
Kyûshû university

Workshop on Solving Multivariate Polynomial Systems and Related Topics

ISIT, Fukuoka, Japan, March 2-3, 2013

Introduction: Solving with Gröbner bases

Given a field $\mathbf{k}$, n variables $X_1, \ldots, X_n$

s polynomials $\mathbf{f} = (f_1, \ldots, f_s)$ in $\mathbf{k}[X_1, \ldots, X_n]$

If the solutions are **finite** then how to find them ?

Gröbner basis approach:

1) Compute a DRL Gröbner basis $\mathcal{G}_{drl}$ of $\mathbf{f}$

2) Change of order of $\mathcal{G}_{DRL}$ to obtain a LEX Gröbner basis $\mathcal{G}_{lex}$ of $\mathbf{f}$

3) Use the **elimination property** of the LEX order to find the solution

Comments:

1) DRL has been proved to be the most efficient order (Bayer-Stillman, *Duke Math J.*, 1987)

2) By using FGLM algorithm or recent improvements (Faugère *et al.*, 2012)

3) LEX Gröbner bases can be very large...

Lexicographic monomial order

Let $1 \leq s \leq n$, and I an ideal of $R[X_1, \ldots, X_n]$.

An s-elimination order $\prec$ on $X_1, \ldots, X_n$ is one for which any Gröbner basis $\mathcal{G}$ under $\prec$ verifies the:

s-elimination property: $\mathcal{G} \cap R[X_1, \ldots, X_s]$is a Gröbner basis of $I \cap R[X_1, \ldots, X_s]$.

If $R = \mathbf{k}$ is a field, equivalent to:

$$i > s \implies X_i \succ X_1^{\alpha_1} \cdots X_s^{\alpha_s}, \quad \forall \alpha \in \mathbb{N}^s.$$

Lexicographic order (definition): $X_1^{\alpha_1} \cdots X_n^{\alpha_n} \prec_{lex} X_1^{\beta_1} \cdots X_n^{\beta_n}$

$$\iff \quad \text{let } t := \max\{1 \leq j \leq n \ : \ \alpha_j \neq \beta_j\}, \text{ then } \quad \alpha_t < \beta_t.$$

A lexicographic order verifies the s-elimination property for any s.

Ideal of dimension 0

$R = \mathbf{k}$ is a field from now.

Let I be a zero-dimensional ideal of $\mathbf{k}[X_1, \ldots, X_n]$.

Then the set of solutions in $\bar{\mathbf{k}}^n$ is finite $\longrightarrow$ Find them .

Zero-dimensional ? $\mathcal{G} = (g_1, \ldots, g_s) \longrightarrow$ a lex. Gröbner basis of I

such that $\quad \mathrm{LM}(g_1) \prec \mathrm{LM}(g_2) \prec \cdots \prec \mathrm{LM}(g_s)$

$\Rightarrow$ there exists $1 = \ell_1 < \ell_2 < \cdots < \ell_n = s$ such that $\mathrm{LM}(g_{\ell_i}) = X_i^{e_i}$ ("pure power of X_i").

Equivalently, $\mathbf{k}[X_1, \ldots, X_n]/I$ is a finite dimensional vector space ($\dim_{\mathbf{k}} \mathbf{k}[\mathbf{X}]/I$ is the degree of I).

$$
\begin{aligned}
g_{\ell(n)}(x_1, x_2, x_3, \ldots, x_{n-2}, x_{n-1}, x_n) &= x_n^{d_{\ell(n)}} + \cdots \\
g_{\ell(n)-1}(x_1, x_2, \ldots, x_{n-2}, x_{n-1}) &= \mathrm{lc}_{n-1}(g_{s-1}) x_n^{d_{\ell(n)-1}} + \cdots \\
\ddots &\quad \vdots \quad \vdots \\
g_{\ell(n-1)}(x_1, \ldots, x_{n-1}) &= x_{n-1}^{d_{\ell(n-1)}} + \cdots \\
\ddots &\quad \vdots \quad \vdots \\
g_{\ell(2)}(x_1, x_2) &= x_2^{d_{\ell(2)}} + \cdots \\
g_{\ell(2)-1}(x_1, x_2) &= x_1^{n_{\ell(2)-1}} x_2^{d_{\ell(2)-1}} + \cdots \\
\ddots &\quad \vdots \quad \vdots \\
g_1(x_1) &= x_1^{d_1} + \cdots
\end{aligned}
$$

Shape lemma position

A lex. G.b. of a 0-dimensional and radical ideal can be much simpler...

Indeed, in most situations (*i.e.* random ideals) it will be in **shape lemma position**:

$$\begin{aligned} g_{\ell(n)}(x_1, x_2, x_3, \ldots, x_{n-2}, x_{n-1}, x_n) &= x_n + \cdots \\ g_{\ell(n-1)}(x_1, \ldots, x_{n-1}) &= x_{n-1} + \cdots \\ \ddots \quad \vdots & \quad \vdots \\ g_{\ell(2)}(x_1, x_2) &= x_2 + \cdots \\ g_1(x_1) &= x_1^{d_1} + \cdots \end{aligned}$$

with $\ell(i) = i$ and $d_1 = d(I)$, the degree of the ideal.

My talk will say nothing in such cases !

Triangular set

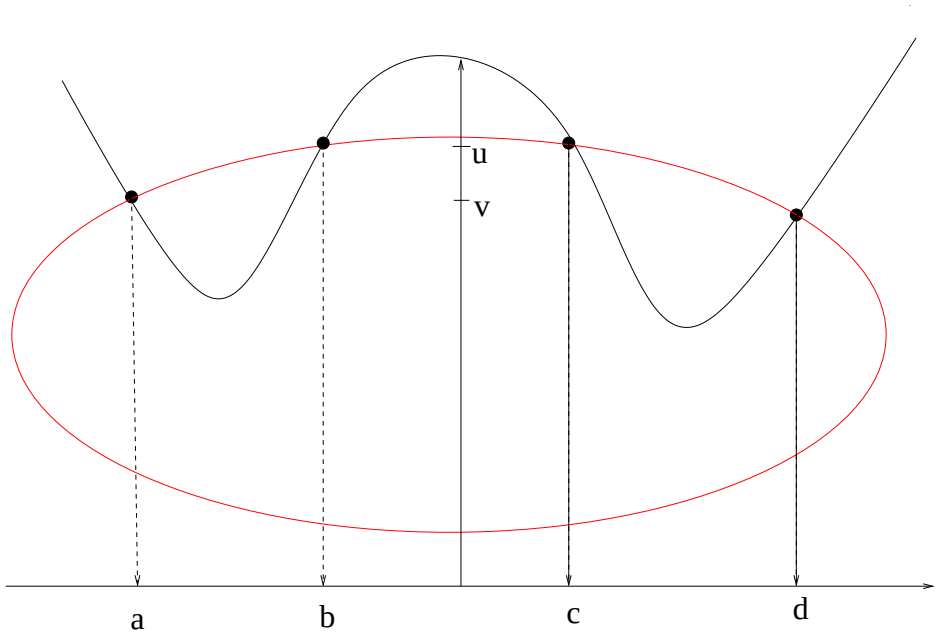
In some cases, like when I is the ideal defining a tour of field extensions, the lex. G.b. is a **triangular set**:

$$\begin{aligned}
g_{\ell(n)}(x_1, x_2, x_3, \ldots, x_{n-2}, x_{n-1}, x_n) &= x_n^{d_{\ell(n)}} + \cdots \\
g_{\ell(n-1)}(x_1, \ldots, x_{n-1}) &= x_{n-1}^{d_{\ell(n-1)}} + \cdots \\
\ddots \quad \vdots & \quad \vdots \\
g_{\ell(2)}(x_1, x_2) &= x_2^{d_{\ell(2)}} + \cdots \\
g_1(x_1) &= x_1^{d_1} + \cdots
\end{aligned}$$

with $\ell(i) = i$ and $d_1 + \cdots + d_{\ell(n)} = d(I)$, the degree of the ideal.

Still, my talk will say nothing in such cases !

Geometry: shape lemma



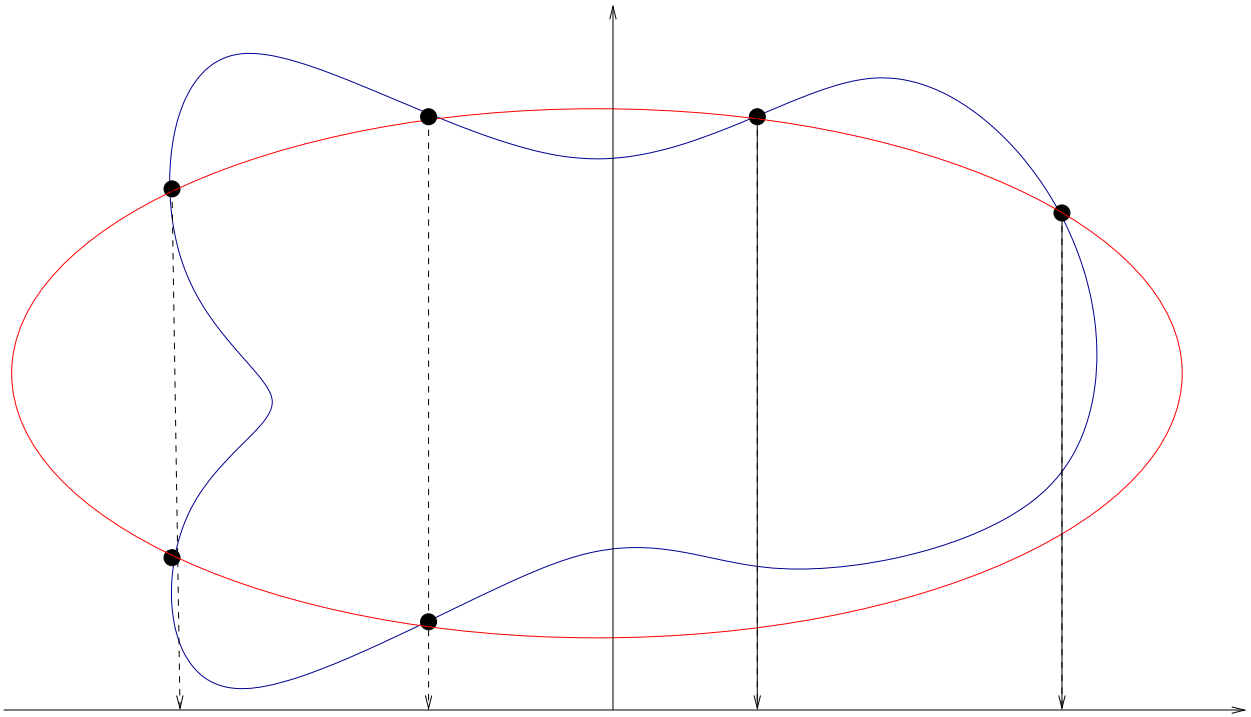
$$g_1(X_1) = (X_1 - a)(X_1 - b)(X_1 - c)(X_1 - d), \qquad \deg(g_1) = 4 = |V|.$$

$$g_2(a, X_2) = g_2(d, X_2) = X_2 - v \quad and \quad g_2(b, X_2) = g_2(c, X_2) = X_2 - u$$

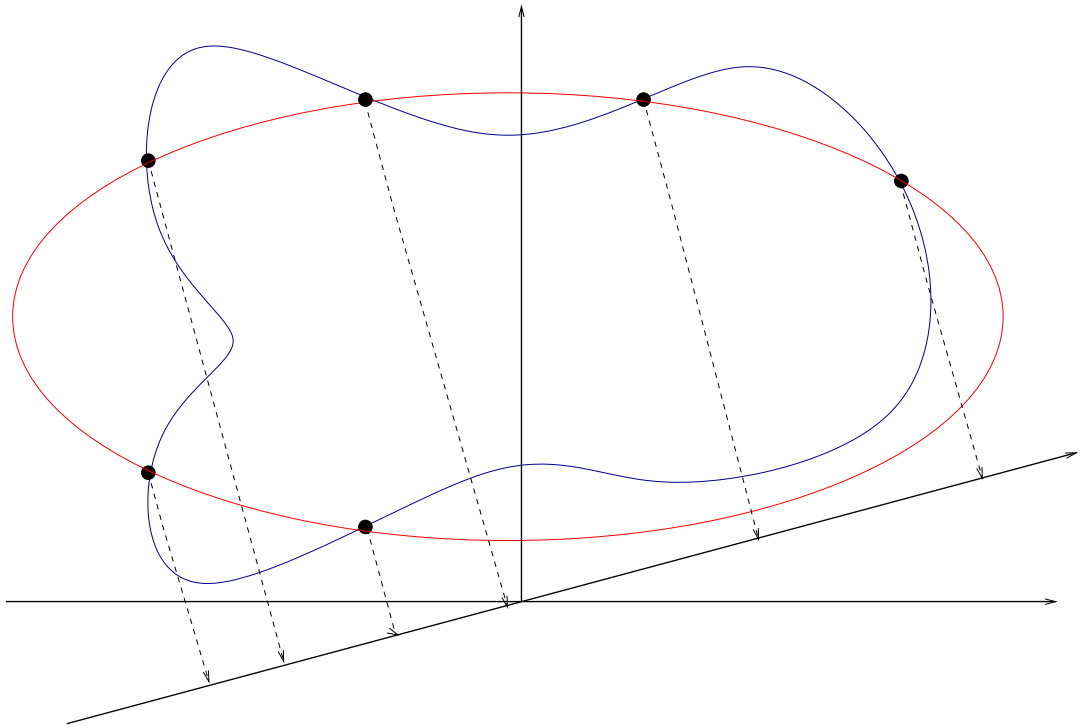
Lagrange interpolation: for $\alpha \in \{a, b, c, d\}$, $\ell_\alpha(X_1) = \prod_{\beta \neq \alpha} \frac{X_1 - \beta}{\alpha - \beta}$ $\quad (\ell_\alpha(\alpha) = 1, \quad \ell_\alpha(\beta) = 0)$

$g_2(X_1, X_2) = (X_2 - u)\,(\ell_a(X_1) + \ell_d(X_1)) + (X_2 - v)\,(\ell_b(X_1) + \ell_c(X_1)) =$
$X_2 + polynomial\ in\ X_1$

Not in shape Lemma

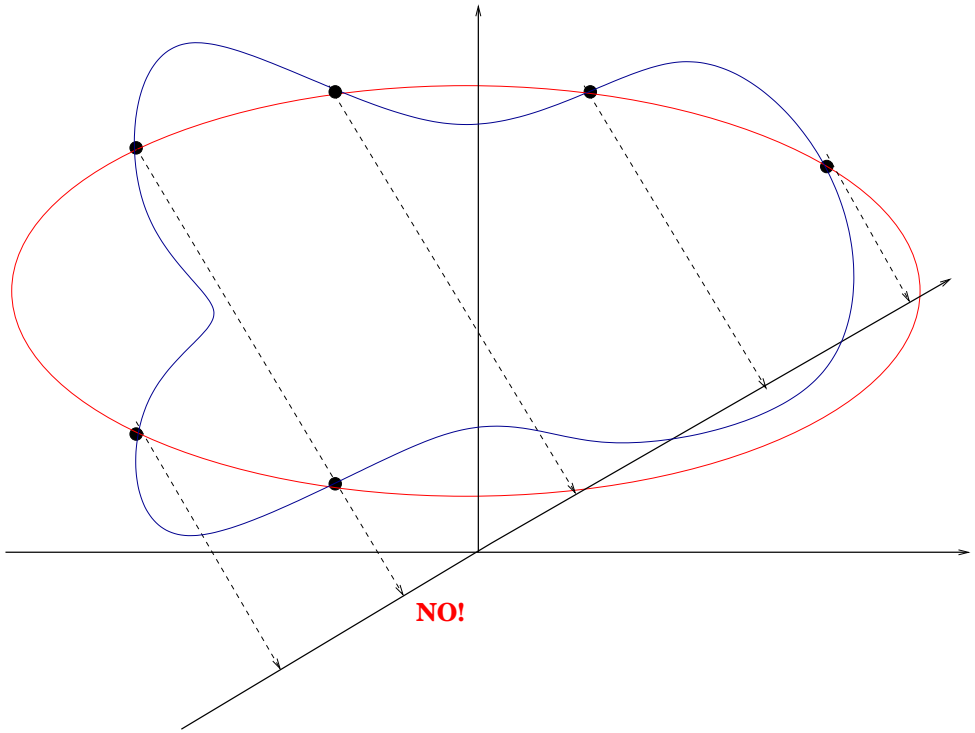


Not in shape Lemma: change of coordinate



If the field **k** is **infinite** almost all changes of coordinates will separate the roots.

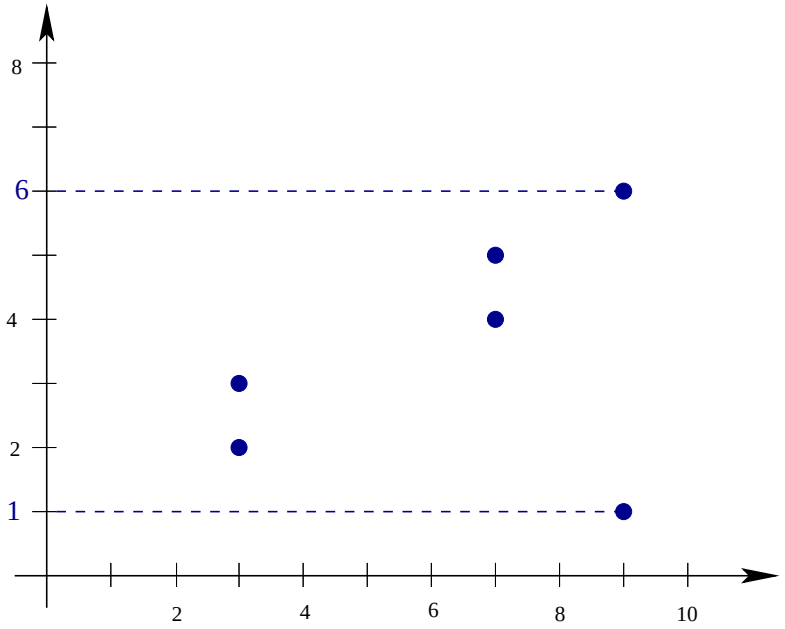
Not in shape Lemma: change of coordinate (2)



This does not always work. Especially if the field $\mathbf{k}$ is finite

Triangular set

Above each projection of a blue point on the X_1-axis, there are always 2 points in the fiber.



Lagrange interpolation:

$$q_3(X_2) = (X_2 - 2)(X_2 - 3)$$

$$q_7(X_2) = (X_2 - 4)(X_2 - 5)$$

$$q_9(X_2) = (X_2 - 1)(X_2 - 6).$$

$$g_2(X_1, X_2) = (q_3)\frac{(X_1 - 7)(X_1 - 9)}{(3 - 7)(3 - 9)} + (q_7)\frac{(X_1 - 3)(X_1 - 9)}{(7 - 3)(7 - 9)} + (q_9)\frac{(X_1 - 3)(X_1 - 7)}{(9 - 3)(9 - 7)}$$

$$\mathrm{LM}(q_3) = \mathrm{LM}(q_7) = \mathrm{LM}(q_9) = X_2^2 \quad \Longrightarrow \quad \mathrm{LM}(g_2) = X_2^2.$$

General lex. G.b.: geometry

$$
\begin{aligned}
g_{\ell(n)}(x_1, x_2, x_3, \ldots, x_{n-2}, x_{n-1}, x_n) &= x_n^{d_{\ell(n)}} + \cdots \\
g_{\ell(n)-1}(x_1, x_2, \ldots, x_{n-2}, x_{n-1}) &= \mathrm{lc}_{n-1}(g_{s-1}) x_n^{d_{\ell(n)-1}} + \ldots \\
\ddots \quad \vdots &\qquad \vdots \\
g_{\ell(n-1)}(x_1, \ldots, x_{n-1}) &= x_{n-1}^{d_{\ell(n-1)}} + \cdots \\
\ddots \quad \vdots &\qquad \vdots \\
g_{\ell(2)}(x_1, x_2) &= x_2^{d_{\ell(2)}} + \cdots \\
g_{\ell(2)-1}(x_1, x_2) &= x_1^{n_{\ell(2)-1}} x_2^{d_{\ell(2)-1}} + \cdots \\
\ddots \quad \vdots &\qquad \vdots \\
g_1(x_1) &= x_1^{d_1} + \cdots
\end{aligned}
$$

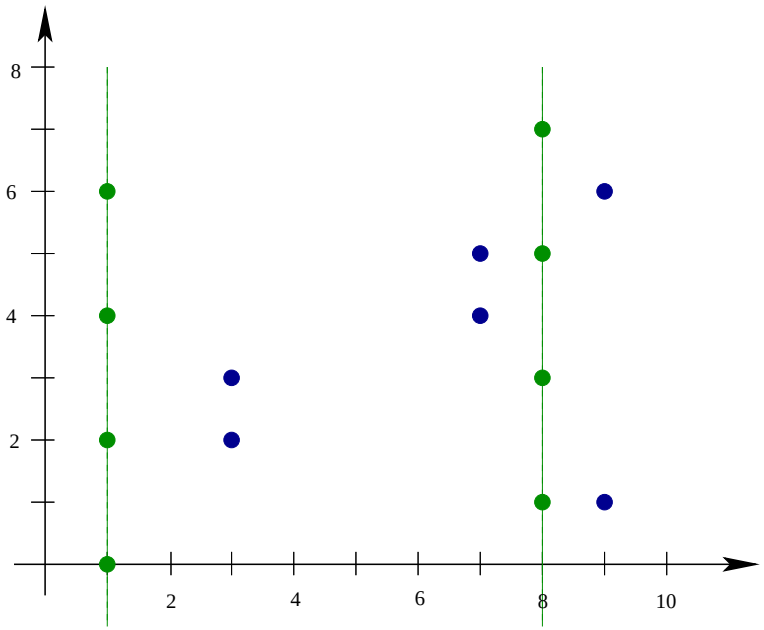
General lex. G.b.: geometry

This is when the number of polynomials in the lex GB is $> n$.

We have just computed the Gröbner basis of the blue points.

$g_1(X_1) = (X_1 - 3)(X_1 - 7)(X_1 - 9)$ $\qquad$ $g_2(X_1, X_2) = X_2^2 + \cdots$

Toy example in 2 variables:



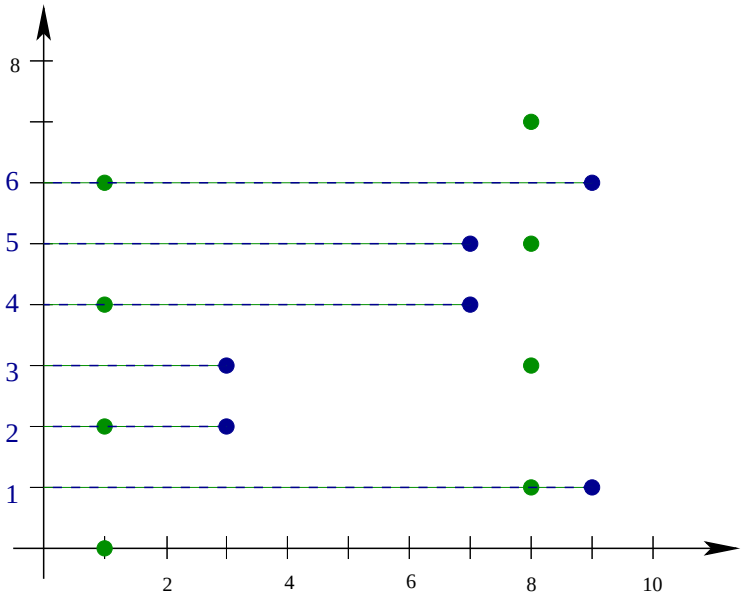
What is the Gröbner basis g_1, g_2, g_3
whose solutions are the green and blue points ?

$g_1 = (X_1 - 1)(X_1 - 8)g_1$
$g_2 = (X_1 - 1)(X_1 - 8)g_2$

General lex. G.b.: geometry

$g_1 = (X_1 - 1)(X_1 - 8)g_1$ $\qquad$ $g_2 = (X_1 - 1)(X_1 - 8)g_2$

Note that: $\qquad (X_1 - 1)(X_1 - 8) \,|\, g_2$



$$
\begin{aligned}
q_1(X_2) &= X_2(X_2-2)(X_2-4)(X_2-6) \\
q_8(X_2) &= (X_2-1)(X_2-3)(X_2-5)(X_2-7) \\
q_3(X_2) &= (X_2-2)(X_2-3) \\
q_7(X_2) &= (X_2-4)(X_2-5) \\
q_9(X_2) &= (X_2-1)(X_2-6)
\end{aligned}
$$

General lex. G.b.: geometry

Candidate for g_3:

$$g_3(X_1, X_2) =$$
$$(q_1)\frac{(X_1-3)(X_1-7)(X_1-8)(X_1-9)}{(1-3)(1-7)(1-8)(1-9)} + (q_8)\frac{(X_1-1)(X_1-7)(X_1-8)(X_1-9)}{(3-1)(3-7)(3-8)(3-9)}$$
$$+ (q_3)\frac{(X_1-1)(X_1-3)(X_1-8)(X_1-9)}{(7-1)(7-3)(7-8)(7-9)} + (q_7)\frac{(X_1-1)(X_1-3)(X_1-7)(X_1-9)}{(8-1)(8-3)(8-7)(8-9)}$$
$$+ (q_9)\frac{(X_1-1)(X_1-3)(X_1-7)(X_1-8)}{(9-1)(9-3)(9-7)(9-8)}$$

But $\text{LM}(q_1) = \text{LM}(q_8) = X_2^4$ while $\text{LM}(q_7) = \text{LM}(q_9) = \text{LM}(q_3) = X_2^2$ only.

So $\text{LM}(g_3) \succ X_2^4$. Not suitable for a Gröbner basis.

General lex. G.b.: geometry

Candidate for g_3:

$$g_3(X_1, X_2) =$$
$$(q_1)\frac{(X_1-3)(X_1-7)(X_1-8)(X_1-9)}{(1-3)(1-7)(1-8)(1-9)} + (q_8)\frac{(X_1-1)(X_1-7)(X_1-8)(X_1-9)}{(3-1)(3-7)(3-8)(3-9)}$$
$$+ (X_2^2 q_3)\frac{(X_1-1)(X_1-3)(X_1-8)(X_1-9)}{(7-1)(7-3)(7-8)(7-9)} + (X_2^2 q_7)\frac{(X_1-1)(X_1-3)(X_1-7)(X_1-9)}{(8-1)(8-3)(8-7)(8-9)}$$
$$+ (X_2^2 q_9)\frac{(X_1-1)(X_1-3)(X_1-7)(X_1-8)}{(9-1)(9-3)(9-7)(9-8)}$$

This time, $\mathrm{LM}(q_1) = \mathrm{LM}(q_8) = X_2^4 = \mathrm{LM}(X_2^2 q_7) = \mathrm{LM}(X_2^2 q_9) = \mathrm{LM}(X_2^2 q_3)$.

So, $\mathrm{LM}(g_3) = X_2^4$.

General lex G.b.

If there are many polynomials in a lex G.b. comparing to n, then there are many redundant (unnecessary) factors ! $\Rightarrow$ those lex G.b. are BIG.

More precisely: Notation: Given $g \in \mathbf{k}[X_1, \ldots, X_t] \setminus \mathbf{k}[X_1, \ldots, X_{t-1}]$, let $\mathrm{lc}_1(g), \ldots, \mathrm{lc}_{t-1}(g)$ be defined recursively as:

$$g := \mathrm{lc}_{t-1}(g) X_t^{\,d_t} + \text{terms of degree in } X_t < d_t,$$

$$\mathrm{lc}_{t-1}(g) := \mathrm{lc}_{t-2}(g) X_{t-1}^{d_{t-1}} + \text{terms of degree in } X_{t-1} < d_{t-1}$$

$$\vdots$$

$$\mathrm{lc}_2(g) := \mathrm{lc}_1(g) X_2^{d_2} + \text{terms of degree in } X_2 < d_2$$

Example: $g = 3x_1^2x_2x_3^2x_4^4 + 2x_1x_2^2x_3x_4^4 + 3x_1x_4 - x_1x_3$

Then $\mathrm{lc}_3(g) = 3x_1^2x_2x_3^2 + 2x_1x_2^2x_3$.

And $\mathrm{lc}_2(g) = 3x_1^2x_2$, then $\mathrm{lc}_1(g) = 3x_1^2$.

Structure theorem 1 (radical case)

$\mathcal{G} \subset \mathbf{k}[X_1, \ldots, X_n] \longrightarrow$ lex. G.b. of I (radical, 0-dim).

let $g \in \mathcal{G}$, such that $g \notin \mathbf{k}[X_1, \ldots, X_{n-1}]$.

let $I_j := (I \cap \mathbf{k}[X_1, \ldots, X_j])\mathbf{k}[X_1, \ldots, X_n]$.

- $g \in \langle \mathrm{lc}_1(g) \rangle \quad (\iff \mathrm{lc}_1(g) \mid g)$
- $g \in \langle \mathrm{lc}_2(g), g_1 \rangle = \langle \mathrm{lc}_2(g) \rangle + I_1 \quad (\iff \mathrm{lc}_2(g)$ divides $g \bmod I_1$.
- $\vdots$
- $g \in \langle \mathrm{lc}_{n-1}(g), g_1, g_2, \ldots, g_{\ell_{n-1}} \rangle = \langle \mathrm{lc}_{n-1}(g) \rangle + I_{n-1} \quad (\iff \mathrm{lc}_{n-1}(g)$ divides $g \bmod I_{n-1}$.

!! Not true if the ideal I is not radical.

But $\mathrm{lc}_1(g) | \mathrm{lc}_2(g)$ is always true.

Structure theorem 2 (radical case, 3 variables)

Let $g' \neq g$ both in $\mathbf{k}[X_1, \ldots, X_3] \setminus \mathbf{k}[X_1, \ldots, X_2]$,

- Assume that $\deg_3(g) = \deg_3(g')$ and that $\mathrm{LM}(g) \prec \mathrm{LM}(g')$.

Then $\mathrm{lc}_1(g')$ divides $\mathrm{lc}_1(g)$

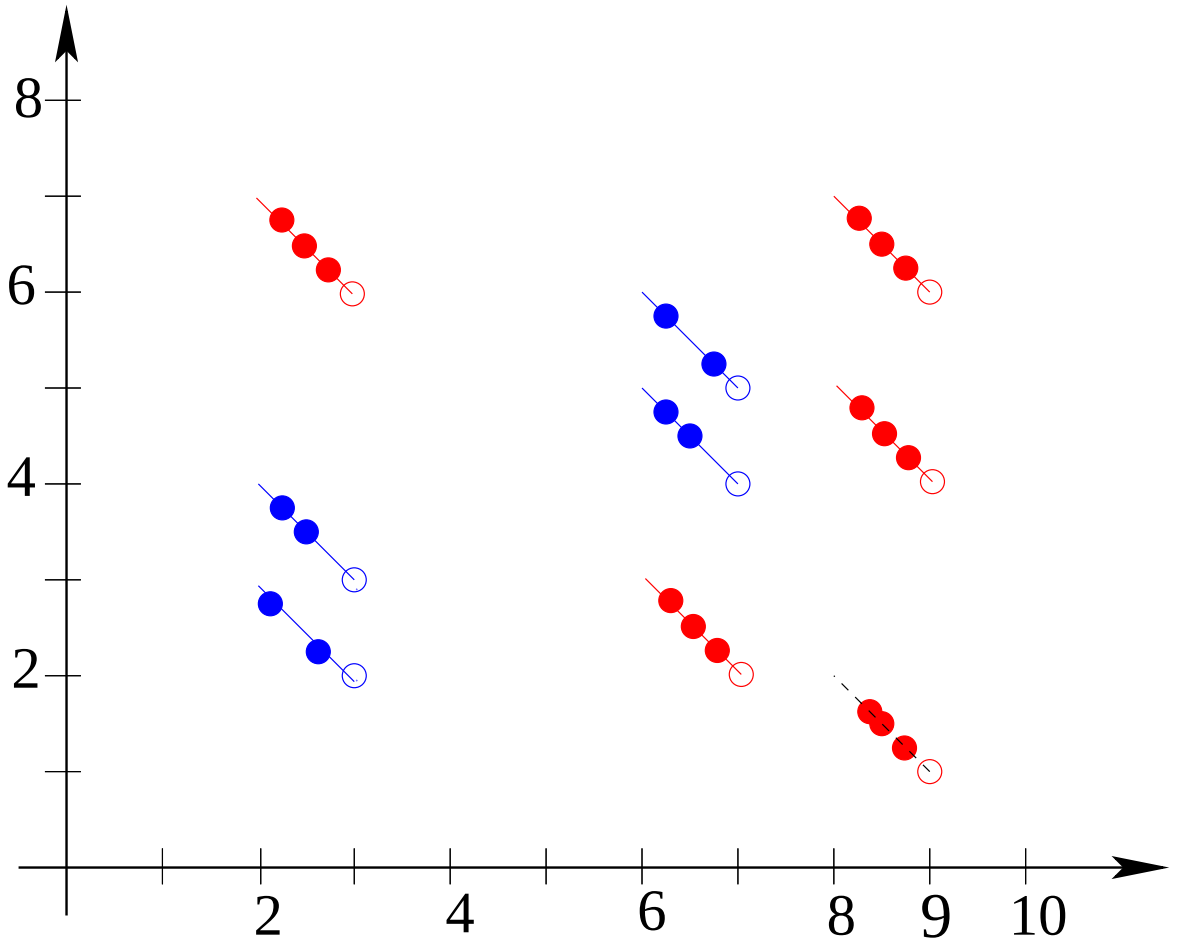
- Assume now that $\deg_3(g) < \deg_3(g')$. Let $\ell_{g,g'} := \mathrm{lcm}(\mathrm{lc}_1(g), \mathrm{lc}_1(g'))$.

Then $\frac{\mathrm{lc}_2(g')}{\mathrm{lc}_1(g')}$ divides $\frac{\mathrm{lc}_2(g)}{\mathrm{lc}_1(g)}$ mod $\frac{g_1}{\ell_{g,g'}}$.

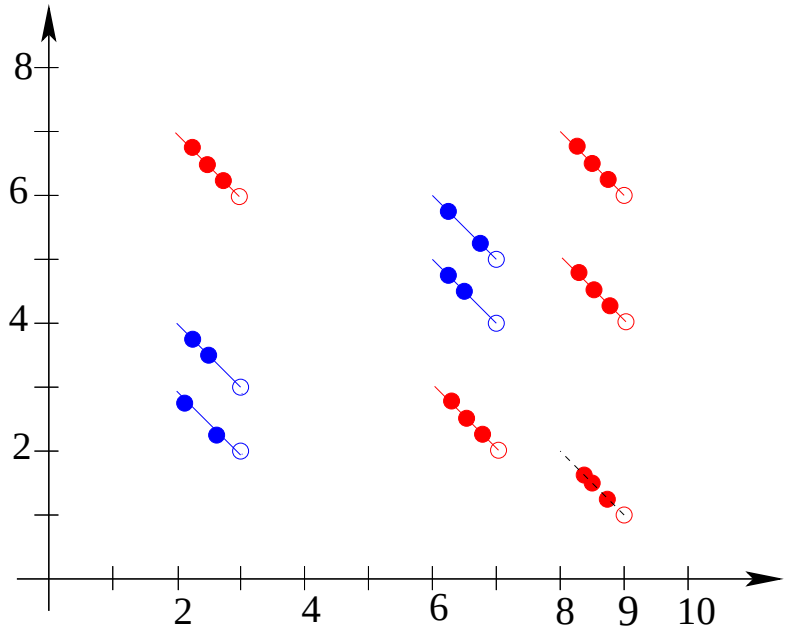
Division equality: $\frac{\mathrm{lc}_2(g)}{\mathrm{lc}_1(g)} = q \frac{\mathrm{lc}_2(g')}{\mathrm{lc}_1(g')} + r$.

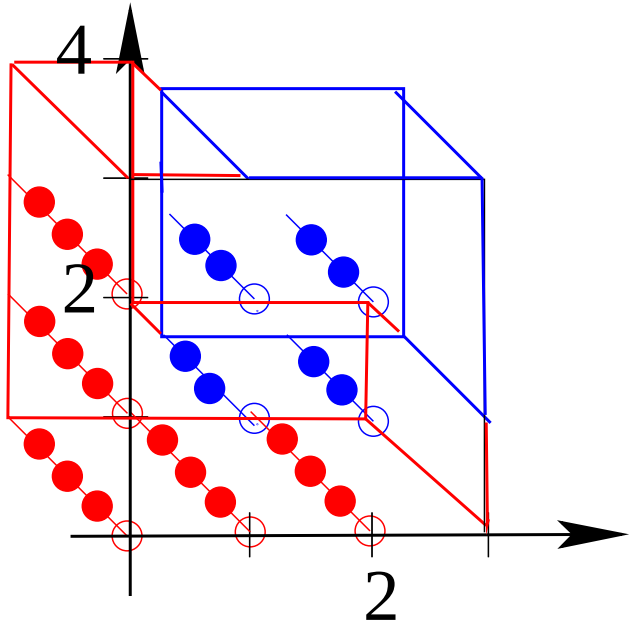
(Note that $q(X_1, X_2) = X_2^{\bullet} + \cdots$) Then $\frac{g_1}{\ell_{g,g'}}$ divides r.

Idea of proof: 3 variables



Looking for polynomials g_is in $\mathcal{G} \setminus \mathbb{Q}[x_1, x_2]$.





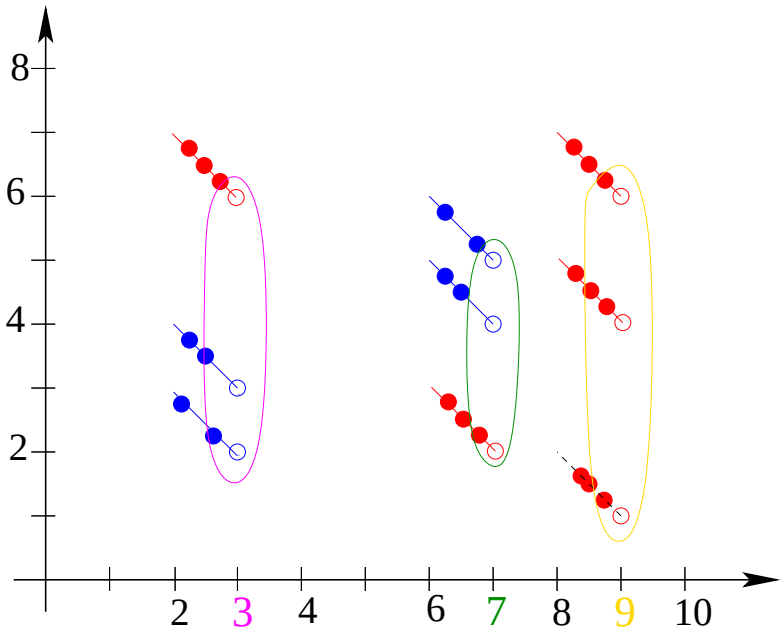
$$\text{LM}(\mathcal{G}) = \langle x_1^3 \ , \ x_2^3 \ , \ x_1 x_2 x_3^2 \ , \ x_3^3 \rangle$$

Why ?

1) By induction on the number of variables $\rightarrow$ we can assume that $\langle \text{LM}(\mathcal{G} \cap \mathbb{Q}[x_1, x_2]) \rangle = \langle x_1^3 \ , \ x_2^3 \rangle$.

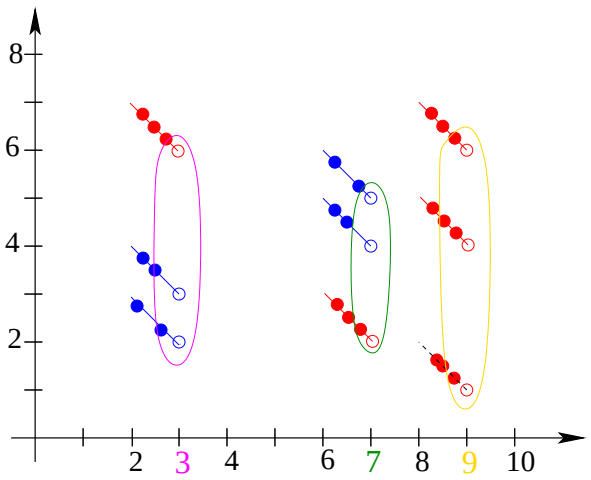
2) We only need to prove the part: $x_1 x_2 x_3^2 \ , \ x_3^3$

Interpolation: $\{x_1x_2x_3^2\ ,\ x_3^3\} \subset \langle \mathbf{lm}(\mathcal{G})\rangle$



$$f = (x_1 - 9)\left[(x_2 - 2)\left((x_3 - \bullet)(x_3 - \bullet)\frac{x_2 - 5}{6 - 5} + (x_3 - \bullet)(x_3 - \bullet)\frac{x_2 - 6}{5 - 6}\right)\frac{x_1 - 3}{7 - 3}\right.$$
$$\left. + (x_2 - 6)\left((x_3 - \bullet)(x_3 - \bullet)\frac{x_2 - 2}{3 - 2} + (x_3 - \bullet)(x_3 - \bullet)\frac{x_2 - 3}{2 - 3}\right)\frac{x_1 - 7}{3 - 7}\right].$$

$$\mathrm{LM}(f) = x_1x_2x_3^2$$

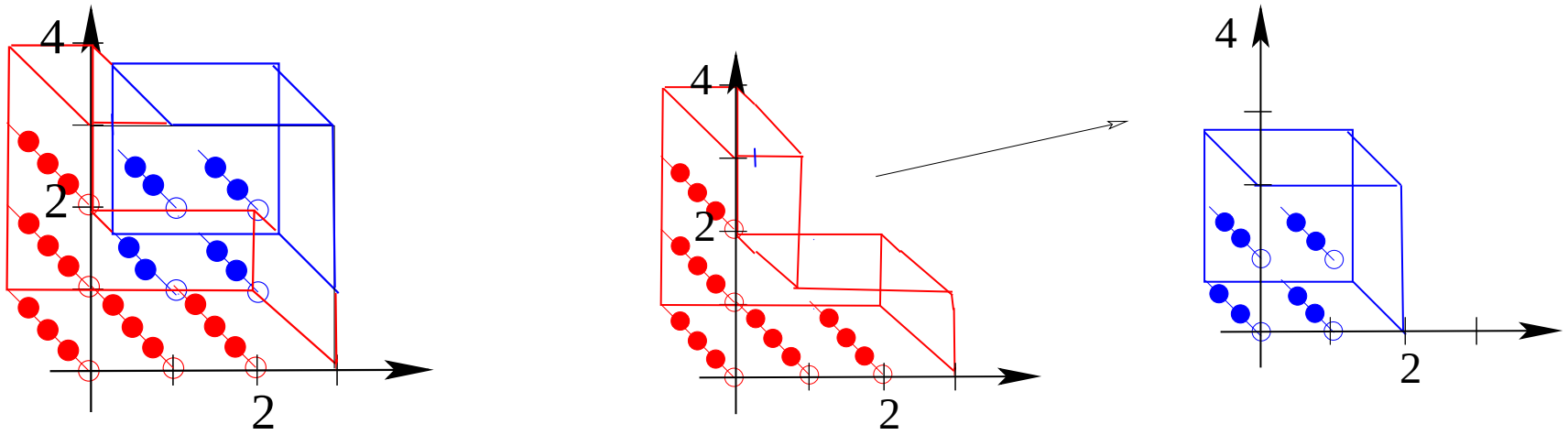


$$\operatorname{LM}(h) = x_3^3$$

$$h = \Big((x_3^3 + \cdots) \frac{(x_2-4)(x_2-1)}{(6-4)(6-1)} + (x_3^3 + \cdots) \frac{(x_2-6)(x_2-1)}{(4-6)(4-1)} + (x_3^3 + \cdots) \frac{(x_2-6)(x_2-4)}{(1-6)(1-4)} \Big) \frac{(x_1-7)(x_1-3)}{(9-7)(9-3)}$$
$$+ \Big((x_3^3 + \cdots) \frac{(x_2-4)(x_2-5)}{(2-4)(2-5)} + (x_3^2 + \cdots)(x_3 - ?) \frac{(x_2-2)(x_2-5)}{(4-2)(4-5)} + (x_3^2 + \cdots)(x_3 - ?) \frac{(x_2-2)(x_2-4)}{(5-2)(5-4)} \Big) \frac{(x_1-3)(x_1-9)}{(7-3)(7-3)}$$
$$+ \Big((x_3^3 + \cdots) \frac{(x_2-2)(x_2-3)}{(6-2)(6-3)} + (x_3^2 + \cdots)(x_3 - ?) \frac{(x_2-3)(x_2-6)}{(2-3)(2-6)} + (x_3^2 + \cdots)(x_3 - ?) \frac{(x_2-2)(x_2-6)}{(3-2)(3-6)} \Big) \frac{(x_1-7)(x_1-9)}{(3-7)(3-9)}.$$

Proof that $\langle \mathbf{lt}(I) \rangle = \langle x_1^3, x_2^3, x_1x_2x_3^2, x_3^3 \rangle$

Idea: By induction on the number of "blocks" of V.



Isomorpshism of vector space (next slide):

$$\mathbb{Q}[x_1,x_2,x_3]/\langle \mathrm{LT}(I(V \cup V))\rangle \simeq \mathbb{Q}[x_1,x_2,x_3]/\langle \mathrm{LT}(I(V))\rangle \times \mathbb{Q}[x_1,x_2,x_3]/\langle \mathrm{LT}(I(V))\rangle$$

$$m \mapsto (m \bmod x_1x_2 \ , \ m \text{ quo } x_1x_2)$$

By induction: $\mathrm{LT}(I(V)) = x_1^3, x_1x_2, x_2^3, x_3^3$ and $\mathrm{LT}(I(V)) = x_1^2, x_2^2, x_3^2$.

$\Rightarrow \ \langle \mathrm{LT}(I(V)) \cup x_1x_2\mathrm{LT}(I(V))\rangle = \langle x_1^3, x_1x_2, x_2^3, x_3^3, x_1^3x_2, x_1x_2^3, x_1x_2x_3^2\rangle = \langle x_1^3, x_2^3, x_1x_2x_3^2, x_3^3$

Structure of lex GB: previous work

- Lazard: 2 variables (1985) —> any 0-dim. ideal, radical or not.
- Gianni-Kalkbrener (1987)
- Becker (1994)
- Mora (Marinari *et al.*), 2004–2008 —> non-rigorous proofs of a somewhat weaker result.

Application to stability of lex. G.b. under specialization

Specialization? Given a lex order $\prec$ for which $X_1 \prec \cdots \prec X_n$ and for an $1 \leq \ell \leq n-1$ a point $\mathbf{a} = (a_1, \ldots, a_\ell) \in \bar{\mathbf{k}}^\ell$,

$$\begin{array}{rcl} \varphi : \bar{\mathbf{k}}[X_1, \ldots, X_n] & \longrightarrow & \bar{\mathbf{k}}[X_{\ell+1}, \ldots, X_n] \\ P(X_1, \ldots, X_n) & \longmapsto & P(a_1, \ldots, a_\ell, X_{\ell+1}, \ldots, X_n). \end{array}$$

Let $R = \bar{\mathbf{k}}[X_1, \ldots, X_\ell]$. Let $\prec_\ell$ be the lex order on $R[X_{\ell+1}, \ldots, X_n]$

Stability? $\phi(\mathrm{LT}_{\prec_\ell}(I)) = \mathrm{LT}_{\prec}(\phi(I))$

$\not\Leftarrow \Rightarrow \phi(\mathcal{G})$ is a Gröbner basis for $\phi(I)$.

Not true in general, true if $\ell = n-1$ (Gianni-Kalkbrener, '87).

If I is radical, (Becker, '94): $\phi(\mathcal{G})$ is a Gröbner basis of $\phi(I)$ (**no** stability)

If I is radical, the structure theorem implies the stability property.

Application to triangular decomposition

LEMMA: Let and $f = \mathrm{lc}_{\ell-1}(g)$ for $g \in \mathcal{G} \cap \mathbf{k}[X_1, \ldots, X_\ell] \setminus \mathbf{k}[X_1, \ldots, X_{\ell-1}]$. We have:

$$\begin{aligned} \mathbf{k}[X_1, \ldots, X_{\ell-1}]/I_{\ell-1} &\simeq \mathbf{k}[X_1, \ldots, X_{\ell-1}]/\langle I_{\ell-1} : \mathrm{lc}_{\ell-1}(g)^\infty \rangle \\ &\times \mathbf{k}[X_1, \ldots, X_{\ell-1}]/\langle \mathrm{lc}_{\ell-1}(g) \rangle + I_{\ell-1}. \end{aligned}$$

Remark: $\mathrm{lc}_{\ell-1}(g)^k \notin I_{\ell-1}$ is not nilpotent modulo $I_{\ell-1}$ because $I_{\ell-1}$ is radical.

Next: How to make this isomorphism effective ?

Application to triangular decomposition (2/2)

Next: How to make this isomorphism effective ?

Quite tricky. . . let's focus on a special case.

. . . 3 variables: x_1, x_2, x_3.

Let $g \in \{\ h \in \mathcal{G}\ :\ \deg_{x_3}(h) > 0\}$ such that $\mathrm{LM}(g)$ is minimal.

For $1 < i \leq \ell(2)$ (implies $\deg_{x_3}(g_i) = 0$), let:

$$p_i := \frac{\mathrm{lc}_1(g_{i-1})}{\mathrm{lc}_1(g_i)} \qquad p_g := \frac{g_1}{\mathrm{lc}_1(g)}.$$

$$h_{g,i} := \gcd(p_g, p_i) \qquad \ell_{g,i} := \mathrm{lcm}(\mathrm{lc}_1(g), \mathrm{lc}_1(g_i)) \qquad (\tfrac{g_1}{\ell_{i,g}} = h_{i,g}).$$

Structure $\Rightarrow$ $\frac{\mathrm{lc}_2(g)}{\mathrm{lc}_1(g)}$ divides $\frac{g_i}{\mathrm{lc}_1(g_i)}$ modulo $h_{g,i}$. Let q_i the quotient.

$$\iff \quad \frac{\ell_{i,g}}{\mathrm{lc}_1(g_i)} g_i = q_i \frac{\ell_{i,g}}{\mathrm{lc}_1(g)} \mathrm{lc}_2(g) + \alpha g_1.$$

Application to triangular decomposition (algorithm)

Split$(g, G_2 := \{g_1(X_1), g_2(X_1, X_2), \ldots, g_{\ell(2)}(X_1, X_2)\})$

For $1 \leq i \leq \ell(2)$ do

$h_{i,g} := \gcd\left(\frac{g_1}{\mathrm{lc}_1(g)}, \frac{\mathrm{lc}_1(g_{i-1})}{\mathrm{lc}_1(g_i)}\right)$ $\qquad$ $\ell_{i,g} := \frac{g_1}{h_{i,g}} = \mathrm{lcm}(\mathrm{lc}_1(g_i), \mathrm{lc}_1(g))$

if $h_{i,g} \neq 1$ then

division equality: $\frac{\ell_{i,g}}{\mathrm{lc}_1(g_i)} g_i = q_i \frac{\ell_{i,g}}{\mathrm{lc}_1(g)} \mathrm{lc}_2(g) + r$ (with $g_1 | r$) *// Fact:* $\mathrm{LM}(q_i) = X_2^{\bullet}$

division equality: $g = s_i \mathrm{lc}_2(g) + r'$ (with $g_1 | r'$) *// Fact:* $\mathrm{LM}(s_i) = X_3^{\bullet}$

$t^{(i)} \leftarrow (\ h_{i,g}(x_1)\ ,\ q_i(x_1, x_2)\ ,\ s_i(x_1, x_2, x_3)\ )$ *// this is a triangular set*

Update: For $2 \leq j \leq i$ do

$g_j \leftarrow \frac{g_j}{h_{g,j}}$ end for end if

end for

We obtain a family of triangular sets $\{t^{(i)}, i\}$ of the ideal $I : \mathrm{lc}_2(g)$

The polynomials $\{g_i\} \cup \{\mathrm{lc}_2(g)\}$ are a lex. G.b. of the ideal $I + \langle \mathrm{lc}_2(g) \rangle$.

Application to triangular decomposition (algorithm)

$\texttt{LexTrig}(G)$

$\mathcal{G} := G \setminus G_2$ // $G_2 := G \cap \mathbf{k}[X_1, \ldots, X_2]$

While $|\mathcal{G}| > 1$ do

  Let $g \in \mathcal{G}$ such that $\text{LM}_{\prec}(g) := \min_{\prec}(\mathcal{G})$

  $G_2, \mathbf{T} \leftarrow \texttt{Split}(g, G_2)$

  $\texttt{outT} \leftarrow \texttt{outT cat } [\mathbf{T}]$; $\mathcal{G} \leftarrow \mathcal{G} \setminus \{g\}$

end while

$\texttt{outT}_2 \leftarrow \texttt{LexTrig}(G_2)$ // *here* $|\mathcal{G}| = 1$. *Recurisve call*

For $\mathbf{t} \in \texttt{outT}_2$ do

  $\mathbf{t} \leftarrow \mathbf{t} \texttt{ cat } [g \bmod \mathbf{t}]$ // *g is the unique element of* $\mathcal{G}$

  $\texttt{outT} \leftarrow \texttt{outT cat } [\mathbf{t}]$

end for

Application to triangular decomposition (algorithm)

Termination is easily proved

Complexity can be made sub-quadratic w.r.t. to the degree $d(I)$ of the ideal, multiplied by the square of the number of polynomials in the Gröbner basis:

$$O(s^2 d(I)^2)$$

Better complexity estimates are possible

Comparison with Möller algorithm (1992)

- His algorithm **can handle** non-radical ideals.
- This allows to compute a family of triangular sets $\{\mathbf{t}^{(1)}, \ldots, \mathbf{t}^{(s)}\}$ such that:

$$I \subset \cap_{i=1}^{s} \langle \mathbf{t}^{i)} \rangle \qquad\qquad \sqrt{I} = \cap_{i=1}^{(s)} \langle \sqrt{\mathbf{t}^{(i)}} \rangle.$$

- In particular, it allows to find all the solutions, even in the non-radical case.
- **But** is based on Gröbner bases computations. GCDs are more efficient.
- No structural result was given. These expain somewhat why lex. G.b. are so big.

  This is useful for other applications (next slide)

Concluding Remarks

- In case of rationals coefficients. The structural result allows with the help of height theory to find upper bounds on the size of coefficients:

  Thm. (D. 2012) The number of digits of any digits in a radical, 0-dim. lex G.b. is :

  $$O(nd(I)^2h) \qquad \text{where } h \text{ is the size of the coefficient in input}$$

- Computing a triangular decomposition after having computed the whole lex. G.b. not very satisfactory.

  Future work would be to use the structural theorem to deduce directly the decomposition from a DRL Gröbner basis.