Size Of Coefficients Of Lexicographical Gröbner Bases

[For bivariate, zero-dimensional and radical systems]

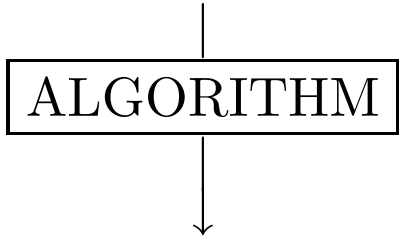
Xavier Dahan

Dep^{t}. of Mathematics, Kyûshû university, Fukuoka, Japan.

ISSAC conference, KIAS Seoul, Korea. July 28-31, 2009

Size of coefficients ?

Input Polynomial System P (over $\mathbb{Q}$): n variables, maximal (total) degree d, height* of coefficients h



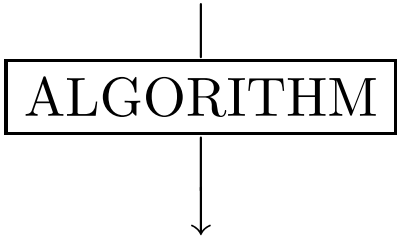
Gröbner basis of P: upper bound $B(n, d, h)$ on the height* **?**

---

* height: maximal number of digits of the coefficients

Size of coefficients ?

Input Polynomial System P (over $\mathbb{Q}$): n variables, maximal (total) degree d, height* of coefficients h



Gröbner basis of P: upper bound $B(n, d, h)$ on the height* **?**

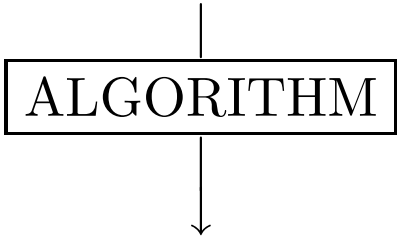
- Very general problem...

---

* height: maximal number of digits of the coefficients

Size of coefficients ?

Input Polynomial System P (over $\mathbb{Q}$): n variables, maximal (total) degree d, height* of coefficients h



Gröbner basis of P: upper bound $B(n, d, h)$ on the height* **?**

- Very general problem
- for which almost everything still needs to be done

---

* height: maximal number of digits of the coefficients

Motivations

- Understand a notoriously observed phenomenon: Gröbner bases may have large coefficients.
- **Modular computations of Gröbner bases over $\mathbb{Q}$:**
  1. Choose one or more "lucky" prime number
  2. Compute a Gröbner basis modulo the prime(s)
  3. Lift the coefficients to the integers

(Trinks, 1984) *On improving approximate results of Buchberger's algorithm by Newton's method.*

(Winkler, 1987) *A p-adic approach to the computation of Gröbner bases.*

(Arnold, 2003) *Modular algorithms for computing Gröbner bases.*

Motivations

- Understand a notoriously observed phenomenon: Gröbner bases may have large coefficients.
- **Modular computations of Gröbner bases over $\mathbb{Q}$:**
  1. Choose one or more "lucky" prime number
  2. Compute a Gröbner basis modulo the prime(s)
  3. Lift the coefficients to the integers

No estimate that permits to quantify the random choices:

$\rightarrow$ How to choose a prime in Step 1 ?

$\rightarrow$ When shall we stop the lifting at Step 3 ?

Restrictions, hypotheses, results

First step toward giving upper bounds:

(i) bivariate case*, lexicographical order $X < Y$

(ii) The input system $\mathbf{P}$ generates a radical ideal: $\sqrt{\langle \mathbf{P} \rangle} = \langle \mathbf{P} \rangle$.

(iii) The number of solutions of $\mathbf{P}$ is finite (0-dimensional ideal).

---

bivariate case*:The bivariate case is a prototype for the case $n \geq 2$: it can be generalized.

Restrictions, hypotheses, results

First step toward giving upper bounds:

(i) bivariate case, lexicographical order $X < Y$

(ii) The input system $\mathbf{P}$ generates a radical ideal: $\sqrt{\langle \mathbf{P} \rangle} = \langle \mathbf{P} \rangle$.

(iii) The number of solutions of $\mathbf{P}$ is finite (0-dimensional ideal).

For a **specific** Gröbner basis (not reduced) $\{g_1, g_2, \ldots, g_s\}$:

$$h(g_{\ell+1}) \leq 4hd^3 + 6d^4(\log d + 2) + O(d^3 \log d).$$

For the **reduced** Gröbner basis $\{g'_1, g'_2, \ldots, g'_s\}$:

$$h(g'_{\ell+1}) \leq 8hd^7 + 12d^8(\log d + 2) + O(d^8 \log d).$$

(NOT SHARP for most of the cases)

Restrictions, hypotheses, results

First step toward giving upper bounds:

For a **specific** Gröbner basis (not reduced) $\{g_1, g_2, \ldots, g_s\}$:

$$h(g_{\ell+1}) \leq 4hd^3 + 6d^4(\log d + 2) + O(d^3 \log d).$$

For the **reduced** Gröbner basis $\{g'_1, g'_2, \ldots, g'_s\}$: **(worst case)**

$$h(g'_{\ell+1}) \leq 8hd^7 + 12d^8(\log d + 2) + O(d^8 \log d).$$

(NOT SHARP for most of the cases)

For the **reduced** Gröbner basis $\{g'_1, g'_2, \ldots, g'_s\}$: **(median case)**

$$h(g'_{\ell+1}) \leq 8hd^5 + 12d^6(\log d + 2) + O(d^6 \log d).$$

(MORE REALISTIC in general)

What has been done so far ?

(Schost & D., ISSAC'2004) *Sharp estimates for triangular sets*

For lex. GB that are regular sequences (triangular sets), but valid for $n \geq 2$ variables:

$$B(n,d,h) \leq 2nhd^{2n-1} + 4n\log(n+1)d^{2n} + O(d^{2n}).$$

What has been done so far ?

(Schost & D., ISSAC'2004) *Sharp estimates for triangular sets*

For lex. GB that are regular sequences (triangular sets), but valid for $n \geq 2$ variables:

$$B(n,d,h) \leq 2nhd^{2n-1} + 4n\log(n+1)d^{2n} + O(d^{2n}).$$

Same result that for the **specific** GB

What has been done so far ?

(Schost & D., ISSAC'2004) *Sharp estimates for triangular sets*

For lex. GB that are regular sequences (triangular sets), but valid for $n \geq 2$ variables:

$$B(n,d,h) \leq 2nhd^{2n-1} + 4n\log(n+1)d^{2n} + O(d^{2n}).$$

Same result that for the **specific** GB

Explanation: Specific Gröbner basis = reconstructed basis from several triangular sets by the Chinese remaindering theorem...

Sharpness ?

Comparative example: Hadamard's inequality for the size of determinants.

Sharpness depends on the defect of orthogonality of the vector columns.

Here (for radical bivariate lex. GB),

the previous bounds, can not **always** be sharp...

...while (probably) nearly optimal for the specific Gröbner basis.

In fact: the bound is the same for all the polynomials appearing in the Gröbner basis, whatever their numbers.

Whereas experimentally, the largest polynomial in the basis has usually (much) larger coefficients than the first one.

Sharpness. . . depends on the structure

The geometry and the arithmetic of the (finite) set of solution points of the input system $\mathbf{P}$, determines the sharpness.

Fact: the number of polynomials in a lex GB depends on the number of "equiprojectable components" of the (finite) set of solutions.

The more there are, the less is the system generic

Consequence: Formula for sharp bounds must depend on the degrees and heights of these "equiprojectable components".

Sharpness. . . depends on the structure

The geometry and the arithmetic of the (finite) set of solution points of the input system $\mathbf{P}$, determines the sharpness.

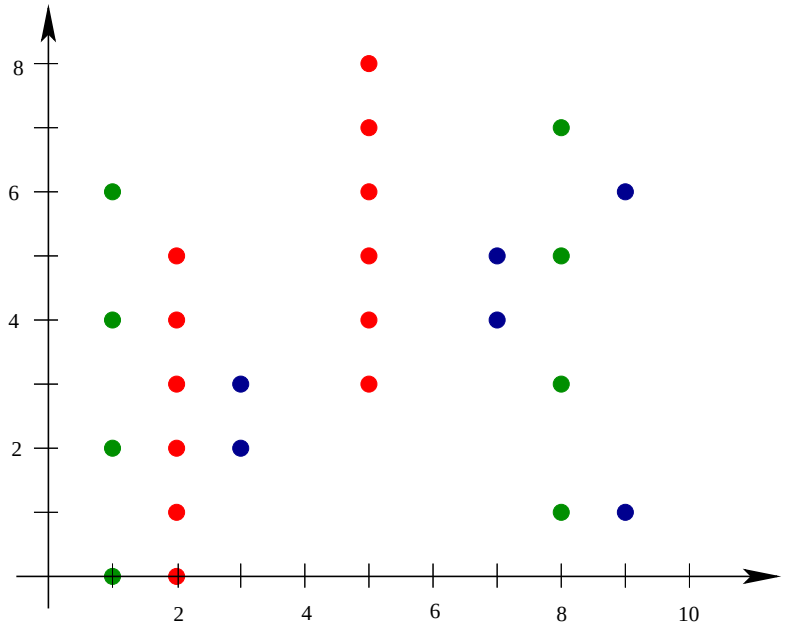
Fact: the number of polynomials in a lex GB depends on the number of "equiprojectable components" of the (finite) set of solutions.

The more there are, the less is the system generic

Consequence: Formula for sharp bounds must depend on the degrees and heights of these "equiprojectable components".

$$\begin{aligned} h(g_{\ell+1}) &\leq h(V) + (2d_{\leq\ell} - 3)\left(\sum_{i=1}^{\ell} \frac{h(V_i)}{e_i}\right) + \log d_{>\ell} \\ &+ (2d_{\leq\ell} - 2)\left(\sum_{i=1}^{\ell} \frac{1}{e_i}(2d_i \log 2 + (e_i + 1)\log d_i)\right) \\ &+ e_\ell \log 2 + (3d_{\leq\ell}^2 - 5d_{\leq\ell} + 9)\log d_{\leq\ell} \end{aligned}$$

Equiprojectable decomposition

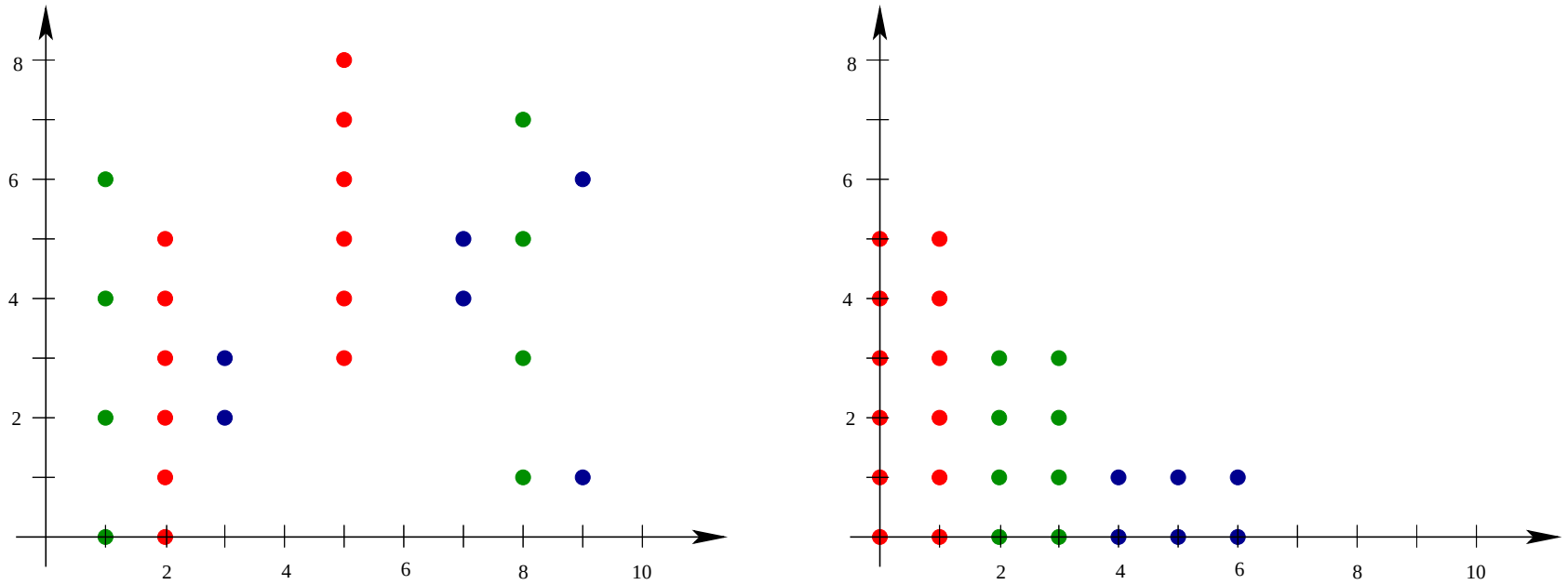


Recall: problem of sharpness of "general bound"

$\leftrightarrow$ non-generic points configuration

$\leftrightarrow$ many polynomials in the GB

Equiprojectable decomposition

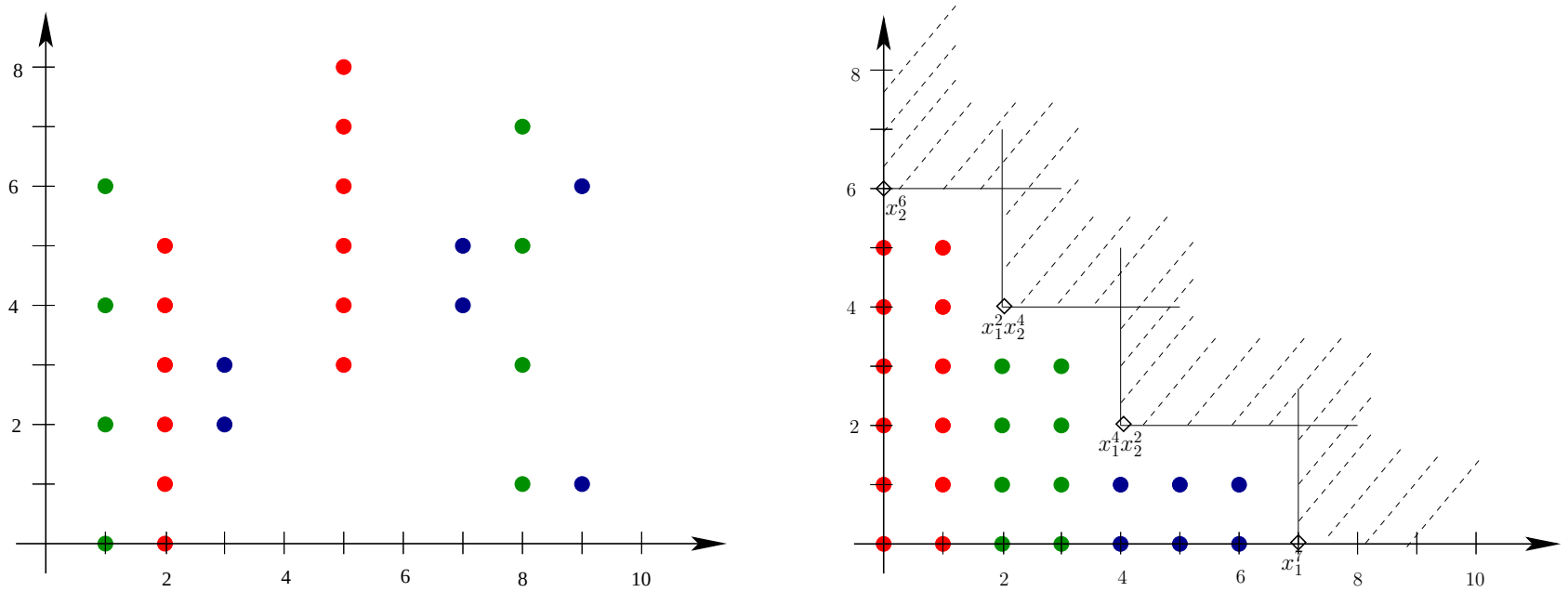


Decompose the set of points following the cardinalities of the fibers of the projection on the first axis.

Here, 3 equiprojectable components:

blue one has size $(3, 2)$, green one has size $(2, 4)$, red one has size $(2, 6)$

Equiprojectable decomposition



Leading monomials : $\langle X^7\,,\ X^4Y^2\,,\ X^2Y^4\,,\ Y^6\rangle$.

Equiprojectable decomposition

Formula for sharp bounds must depend on the degrees and heights of these "equiprojectable components".

$$\begin{aligned} h(g_{\ell+1}) &\leq h(V) + (2d_{\leq \ell} - 3)\left(\sum_{i=1}^{\ell} \frac{h(V_i)}{e_i}\right) + \log d_{>\ell} \\ &+ (2d_{\leq \ell} - 2)\left(\sum_{i=1}^{\ell} \frac{1}{e_i}(2d_i \log 2 + (e_i + 1)\log d_i)\right) \\ &+ e_\ell \log 2 + (3d_{\leq \ell}^2 - 5d_{\leq \ell} + 9)\log d_{\leq \ell} \end{aligned}$$

Equiprojectable decomposition: previous work

The **term** "equiprojetable": (Aubry-Valibouze, 2001) → context of computational Galois theory.

(Gao-Stroomer-Rodrigues, 2003) Preprint: Representation of equiprojectable components in a trie graph.

(Moreno Maza, Xie, Schost, Wu & D., ISSAC'2005) Algorithmic study, relevance for modular computations, probabilistic analysis.

(Lederer, 2008) , (Lundqvist, 2009) ... and certainly others.

Lagrange bases

Well-known in 1 variable:

k a field

$A \subset \bar{k}$, a finite Zariski closed subset: the nodes

$\{ \prod_{b \in A,\, b \neq a} \frac{X-b}{a-b} \}_{a \in A}$ is a basis of $k[X]_{<\#A}$

Lagrange bases

Well-known in 1 variable:

k a field

$A \subset \bar{k}$, a finite Zariski closed subset: the nodes

$\{\prod_{b \in A,\, b \neq a} \frac{X-b}{a-b}\}_{a \in A}$ is a basis of $k[X]_{<\#A}$

Scalar extension:

K is finite k-algebra then

$A \subset \bar{k}$, a finite Zariski closed subset: the nodes

$\{\prod_{b \in A,\, b \neq a} \frac{X-b}{a-b}\}_{a \in A}$ is a basis of $K[X]_{<\#A}$

Lagrange bases

Well-known in 1 variable:

k a field

$A \subset \bar{k}$, a finite Zariski closed subset: the nodes

$\{\prod_{b\in A,\, b\neq a} \frac{X-b}{a-b}\}_{a\in A}$ is a basis of $k[X]_{<\#A}$

Scalar extension:

K is finite k-algebra then

$A \subset \bar{k}$, a finite Zariski closed subset: the nodes

$\{\prod_{b\in A,\, b\neq a} \frac{X-b}{a-b}\}_{a\in A}$ is a basis of $K[X]_{<\#A}$

If $K = k[Y]$ we get:

$\{\prod_{b\in A,\, b\neq a} \frac{X-b}{a-b}\}_{a\in A}$ is a basis of $(k[Y])[X]_{<\#A}$.

Lagrange bases

2 consequences:

If $f(X,Y) \in k[X,Y]$, with $\deg_X f < \#A$, then:

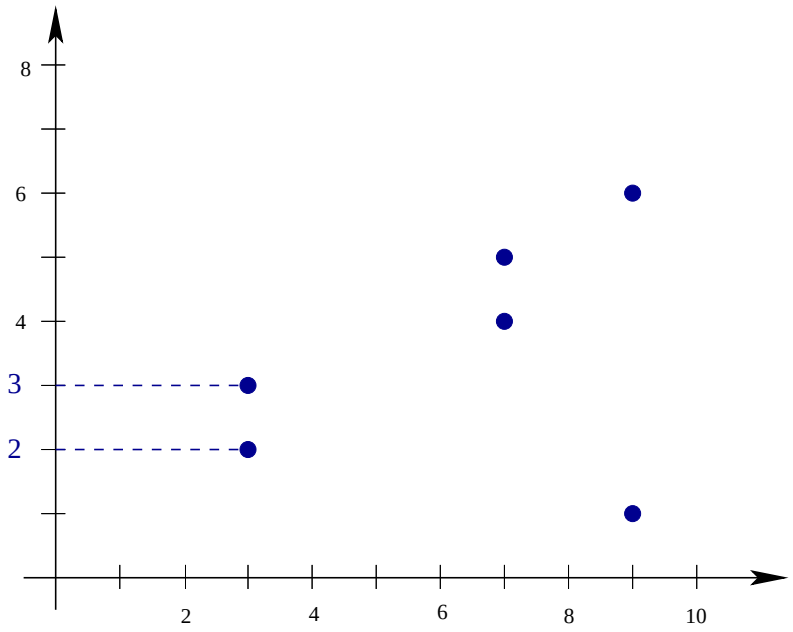
$$f(X,Y) = \sum_{a \in A} f(a,Y) \prod_{\substack{b \in A \\ a \neq b}} \frac{X-b}{a-b}.$$

If $\{g_a(Y)\}_{a \in A}$ is a family of monic polynomial of degree d then:

$$lt\left(\sum_{a \in A} g_a(Y) \prod_{\substack{b \in A \\ a \neq b}} \frac{X-b}{a-b} \right) = Y^d.$$

Equiprojectable variety & Lagrange interpolation

The blue variety is **equiprojectable**: above each projection of a blue point on the X-axis, there are always 2 points in the fiber.

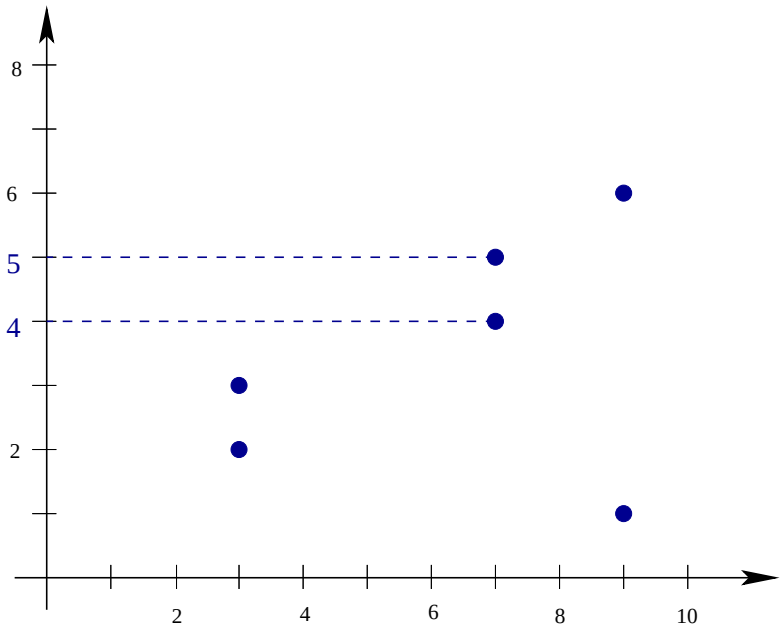


Lagrange interpolation:

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

Equiprojectable variety & Lagrange interpolation

The blue variety is **equiprojectable**: above each projection of a blue point on the X-axis, there are always 2 points in the fiber.



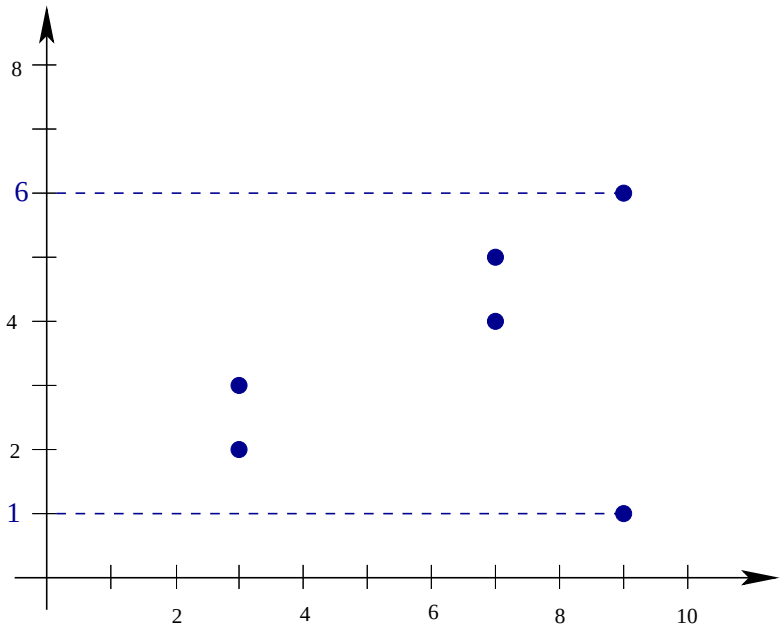
Lagrange interpolation:

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

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

Equiprojectable variety & Lagrange interpolation

The blue variety is **equiprojectable**: above each projection of a blue point on the X-axis, there are always 2 points in the fiber.



Lagrange interpolation:

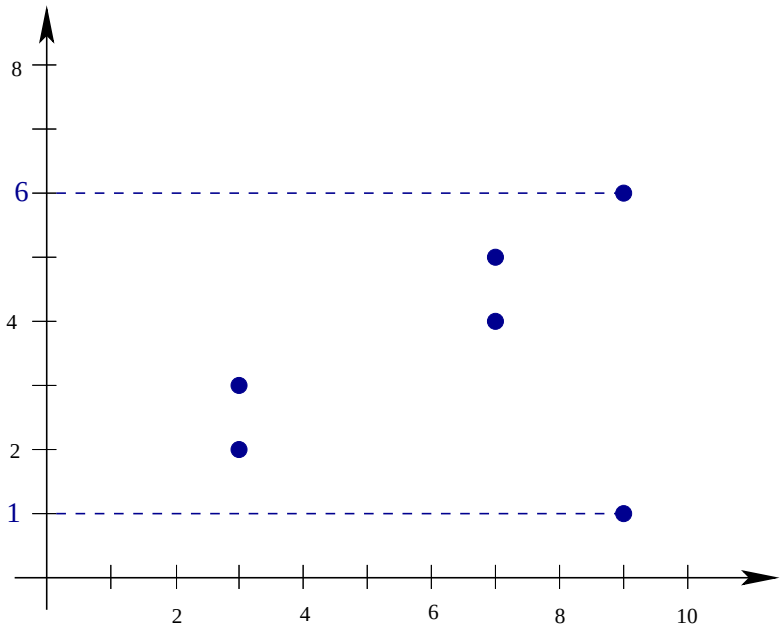
$$q_3(Y) = (Y-2)(Y-3)$$

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

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

Equiprojectable variety & Lagrange interpolation

The blue variety is **equiprojectable**: above each projection of a blue point on the X-axis, there are always 2 points in the fiber.



Lagrange interpolation:

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

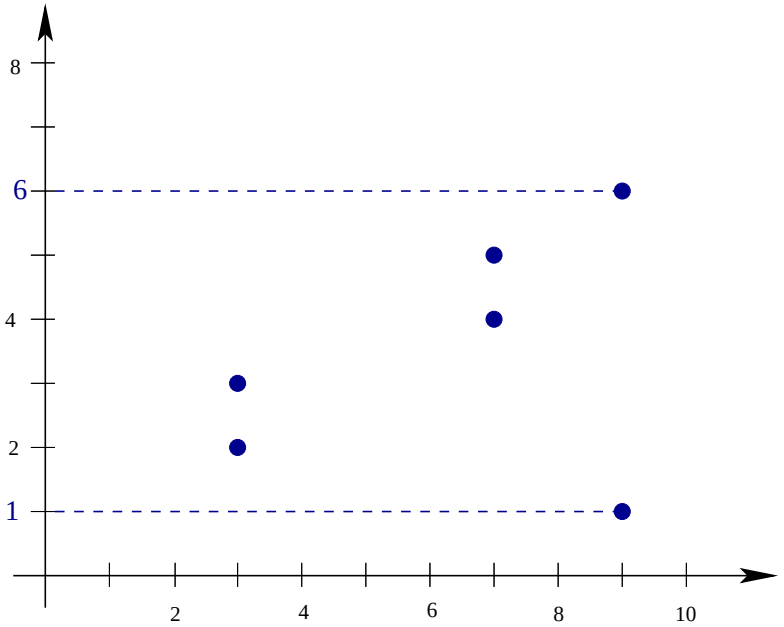
$$q_7(Y) = (Y-4)(Y-5)$$

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

$$f_2(X,Y) = (q_3)\frac{(X-7)(X-9)}{(3-7)(3-9)} + (q_7)\frac{(X-3)(X-9)}{(7-3)(7-9)} + (q_9)\frac{(X-3)(X-7)}{(9-3)(9-7)}$$

Equiprojectable variety & Lagrange interpolation

The blue variety is **equiprojectable**: above each projection of a blue point on the X-axis, there are always 2 points in the fiber.



Lagrange interpolation:

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

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

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

$$f_2(X,Y) = (q_3)\frac{(X-7)(X-9)}{(3-7)(3-9)} + (q_7)\frac{(X-3)(X-9)}{(7-3)(7-9)} + (q_9)\frac{(X-3)(X-7)}{(9-3)(9-7)}$$

$$lt(q_3) = lt(q_7) = lt(q_9) = Y^2 \quad \Longrightarrow \quad lt(f_2) = Y^2.$$

From equiprojectable to general varieties

(Schost & D., ISSAC'2004) *Sharp estimates for triangular sets*

For lex. GB that are regular sequences (triangular sets, corresponding to **equiprojectable varieties**), but valid for $n \geq 2$ variables:

$$B(n,d,h) \leq 2nhd^{2n-1} + 4n\log(n+1)d^{2n} + O(d^{2n}).$$

Sketch of Proof: Not hard with the good tools.

1) Interpolation: link between the points solution and the polynomials in the Gröbner basis.

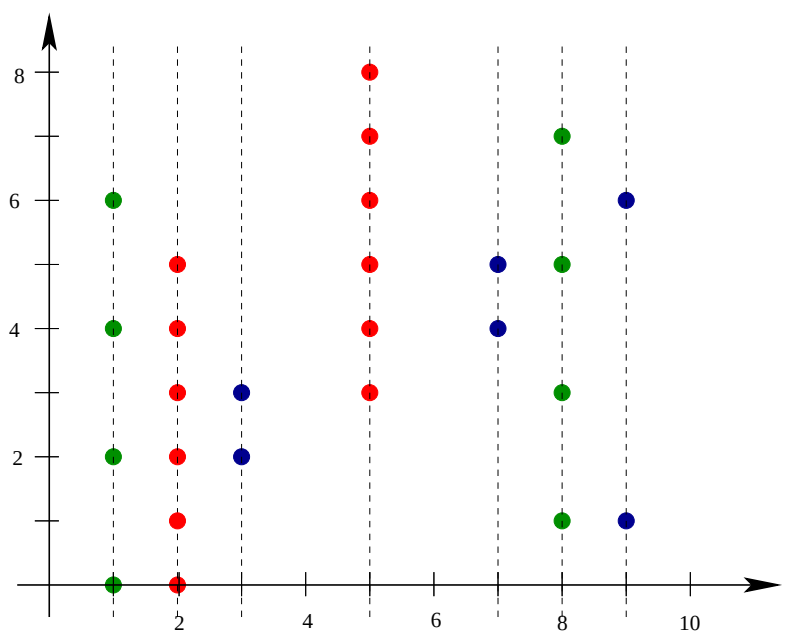
2) Elementary height theory from Diophantine approximation: height of varieties (with Chow form), inequalities, Arithmetic Bézout theorem.

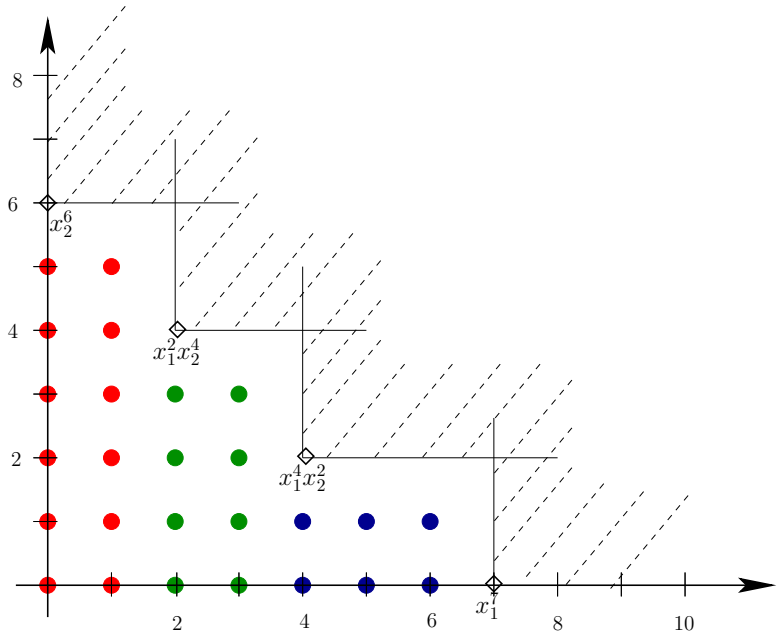
(Krick, Pardo & Sombra, 2001) *Sharp estimates for the arithmetic Nullstellensatz*

From equiprojectable to general varieties

We adapt the **same strategy for non-equiprojectable varieties**, a bit more tricky.

Use of Lagrange interpolation

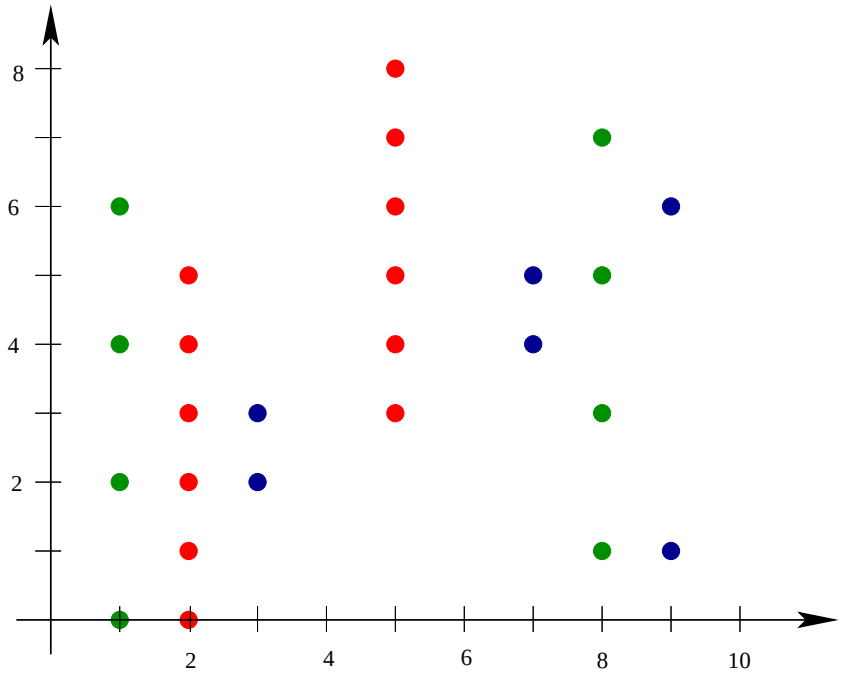




Leading monomials : $\langle X^7\,,\ X^4Y^2\,,\ X^2Y^4\,,\ Y^6\rangle$.

$$g_1(X) = (X-1)(X-2)(X-3)(X-5)(X-7)(X-8)(X-9) = X^7+\cdots$$

Use of Lagrange interpolation

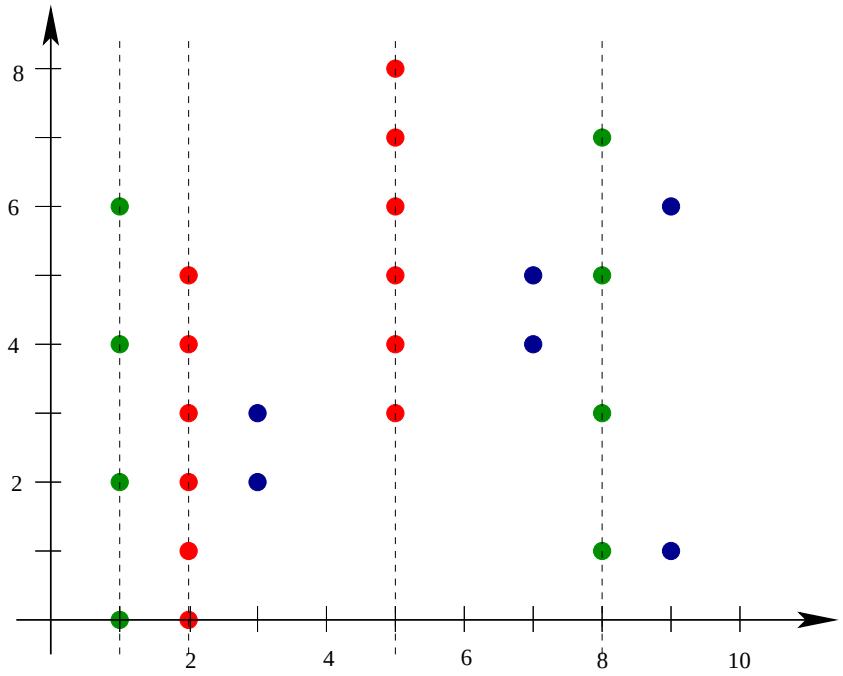


Leading monomials:

$\langle X^7, X^4Y^2, X^2Y^4, Y^6\rangle$.

$$g_1(X) = X^7 + \cdots$$

Computation of g_2



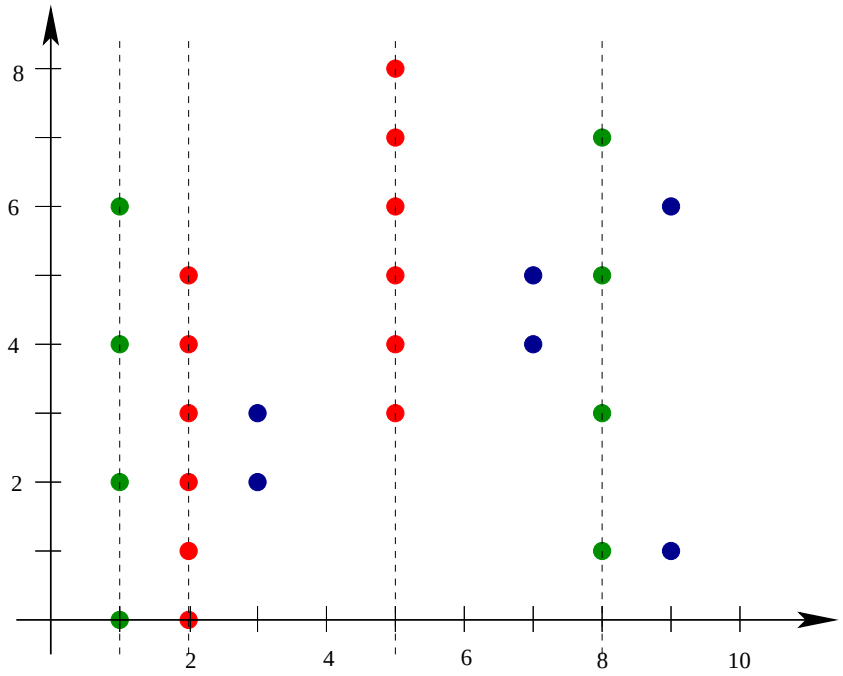
Leading monomials:

$\langle X^7\,,\, X^4Y^2\,,\, X^2Y^4\,,\, Y^6\rangle.$

$$g_1(X) = X^7 + \cdots$$

$$g_2(X,Y) = (X-1)(X-2)(X-5)(X-8)f_2(X,Y) = (X^4+\cdots)(Y^2+\cdots)$$

Computation of g_2



Leading monomials:

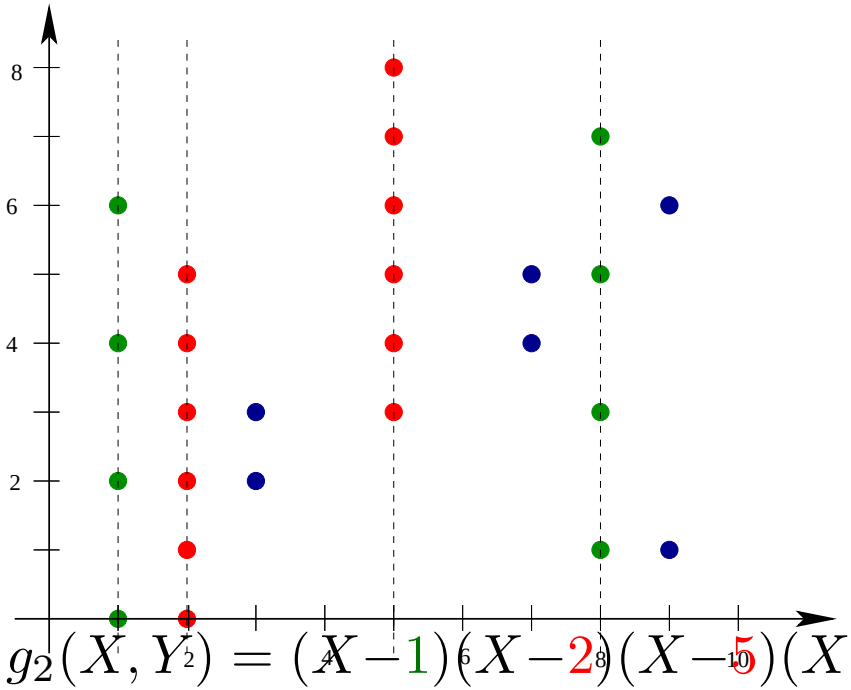
$\langle X^7\,,\, X^4Y^2\,,\, X^2Y^4\,,\, Y^6\rangle.$

$$g_1(X) = X^7 + \cdots$$

$$g_2(X,Y) = (X-1)(X-2)(X-5)(X-8)f_2(X,Y) = (X^4+\cdots)(Y^2+\cdots)$$

The polynomial f_2 should vanish only on the blue points.

Computation of g_2



Leading monomials:

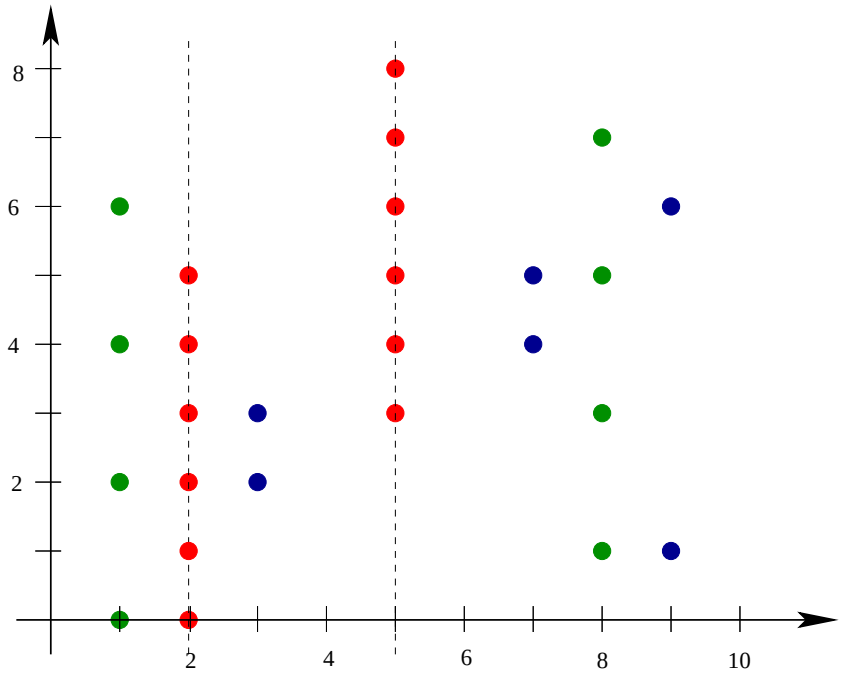
$\langle X^7\,,\ X^4Y^2\,,\ X^2Y^4\,,\ Y^6\rangle.$

$$g_1(X) = X^7 + \cdots$$

$$g_2(X,Y) = (X-1)(X-2)(X-5)(X-8)\,f_2(X,Y) = (X^4+\cdots)(Y^2+\cdots)$$

The polynomial f_2 should vanish only on the blue points: equiprojectable case. It has already been computed by Lagrange interpolation formula.

Computation of g_3



Leading monomials:

$\langle X^7, X^4Y^2, X^2Y^4, Y^6\rangle$.

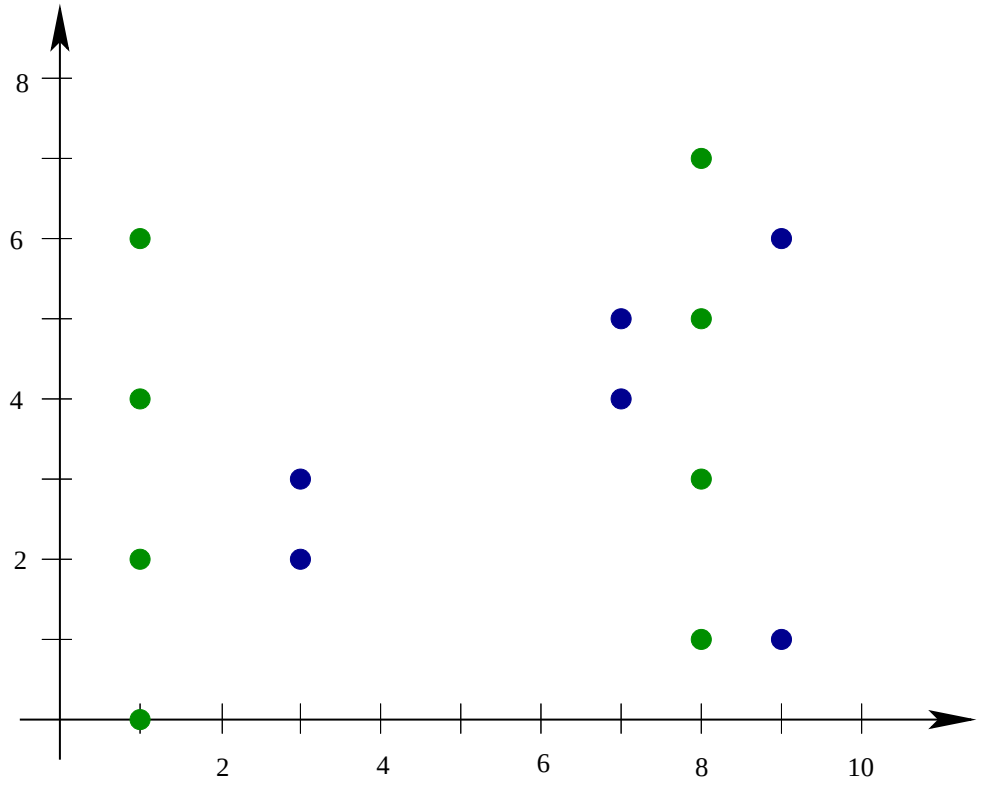
$$g_1(X) = X^7 + \cdots$$

$$g_2(X,Y) = X^4Y^2 + \cdots$$

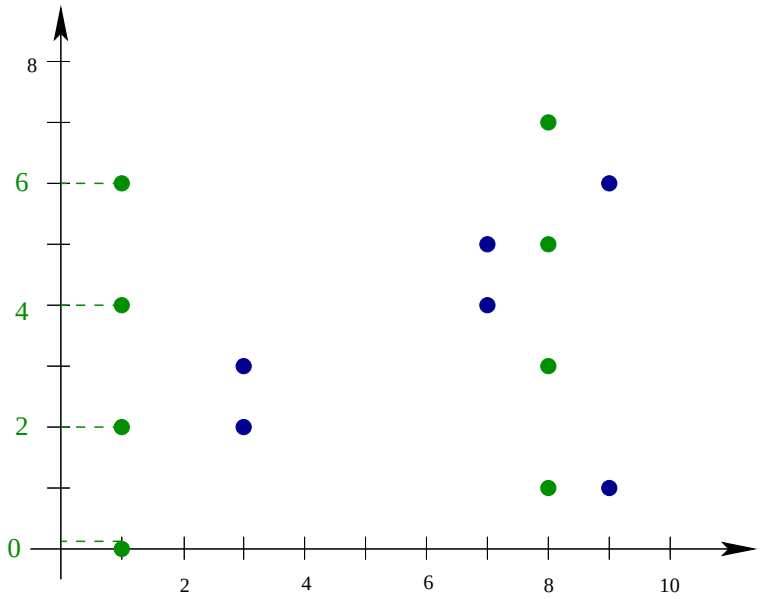
$$g_3(X,Y) = (X-2)(X-5)f_3(X,Y) = (X^2 + \cdots)(Y^4 + \cdots)$$

The polynomial f_3 should vanish on the blue and green points. Let us apply again Lagrange interpolation formula.

Lagrange formula on non-equiprojectable varieties

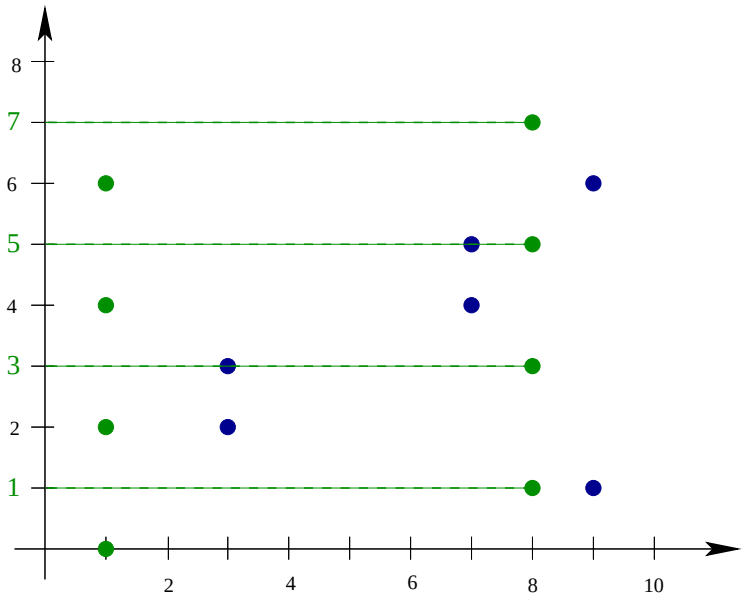


Lagrange formula on non-equiprojectable varieties



$$q_1(Y) = Y(Y-2)(Y-4)(Y-6)$$

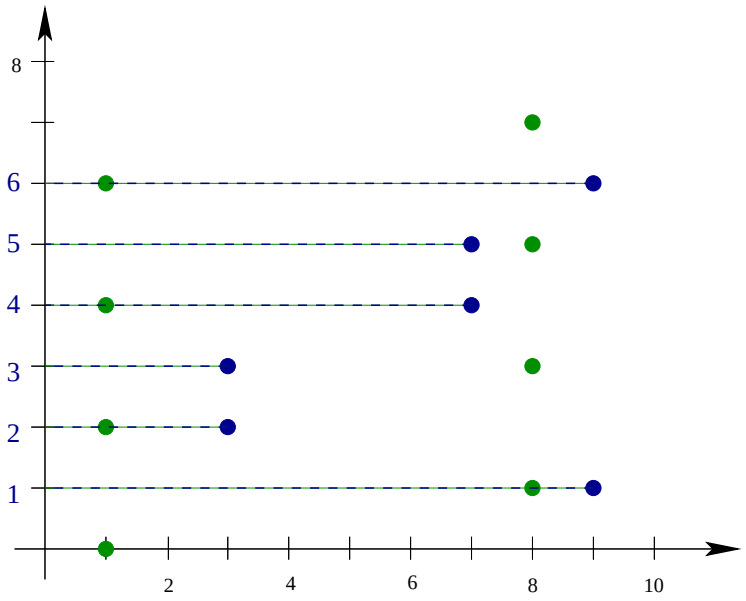
Lagrange formula on non-equiprojectable varieties



$$q_1(Y) = Y(Y-2)(Y-4)(Y-6)$$

$$q_8(Y) = (Y-1)(Y-3)(Y-5)(Y-7)$$

Lagrange formula on non-equiprojectable varieties



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

Lagrange formula on non-equiprojectable varieties

Candidate for f_3:

$$\begin{aligned} f_3(X,Y) &= (q_1)\frac{(X-3)(X-7)(X-8)(X-9)}{(1-3)(1-7)(1-8)(1-9)} + (q_2)\frac{(X-1)(X-7)(X-8)(X-9)}{(3-1)(3-7)(3-8)(3-9)} \\ &+ (q_3)\frac{(X-1)(X-3)(X-8)(X-9)}{(7-1)(7-3)(7-8)(7-9)} + (q_7)\frac{(X-1)(X-3)(X-7)(X-9)}{(8-1)(8-3)(8-7)(8-9)} \\ &+ (q_9)\frac{(X-1)(X-3)(X-7)(X-8)}{(9-1)(9-3)(9-7)(9-8)} \end{aligned}$$

But $lt(q_1) = lt(q_2) = Y^4$ while $lt(q_7) = lt(q_9) = lt(q_3) = Y^2$ only.

So $lt(f_3) > Y^4$. Not suitable for a Gröbner basis.

Needs a modification to have $lt(f_3) = Y^4$.

Good candidate for f_3

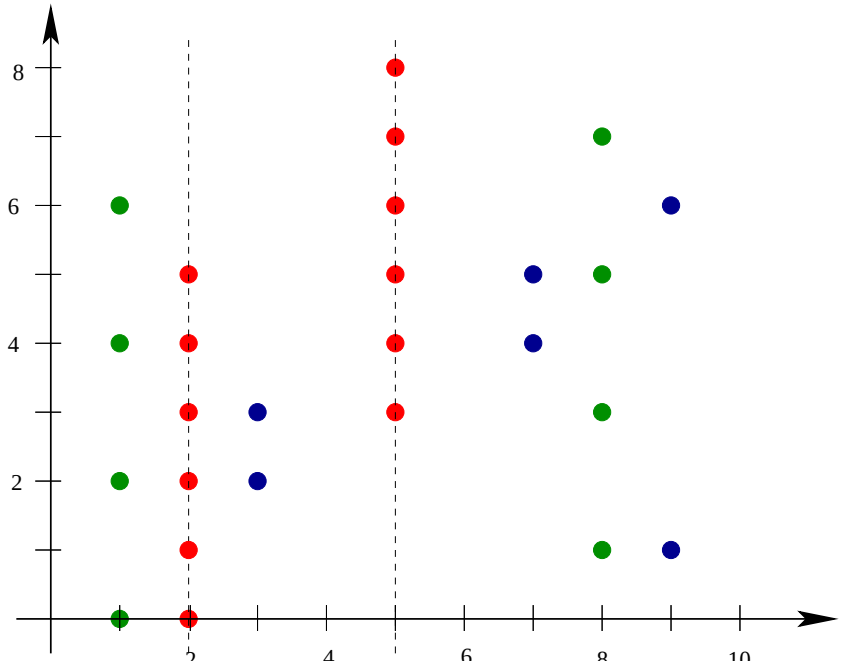
$$
\begin{aligned}
f_3(X,Y) \quad = \quad & (q_1)\frac{(X-3)(X-7)(X-8)(X-9)}{(1-3)(1-7)(1-8)(1-9)} + (q_2)\frac{(X-1)(X-7)(X-8)(X-9)}{(3-1)(3-7)(3-8)(3-9)} \\
+ \quad & (q_3 \times (Y^2 + a_3 Y + b_3))\frac{(X-1)(X-3)(X-8)(X-9)}{(7-1)(7-3)(7-8)(7-9)} \\
+ \quad & (q_7 \times (Y^2 + a_7 Y + b_7)\frac{(X-1)(X-3)(X-7)(X-9)}{(8-1)(8-3)(8-7)(8-9)} \\
+ \quad & (q_9 \times (Y^2 + a_9 Y + b_9))\frac{(X-1)(X-3)(X-7)(X-8)}{(9-1)(9-3)(9-7)(9-8)}
\end{aligned}
$$

Where $(a_i, b_i)_{i=3,7,9}$ are any coefficients in $\mathbb{Q}$.

Let $Q_i := q_i \times (Y^2 + a_i Y + b_i)$, $i = 3, 7, 9$.

This time: $lt(Q_i) = Y^4 \implies lt(f_3) = Y^4$.

About the choice of f_3



Leading monomials:

$\langle X^7\,,\, X^4Y^2\,,\, X^2Y^4\,,\, Y^6\rangle.$

$$g_1(X) = X^7 + \cdots$$

$$g_2(X,Y) = X^4Y^2 + \cdots$$

$$g_3(X,Y) = (X^6 - 2)(X^8 - 5)f_3(X,Y) = (X^2 + \cdots)(Y^4 + \cdots)$$

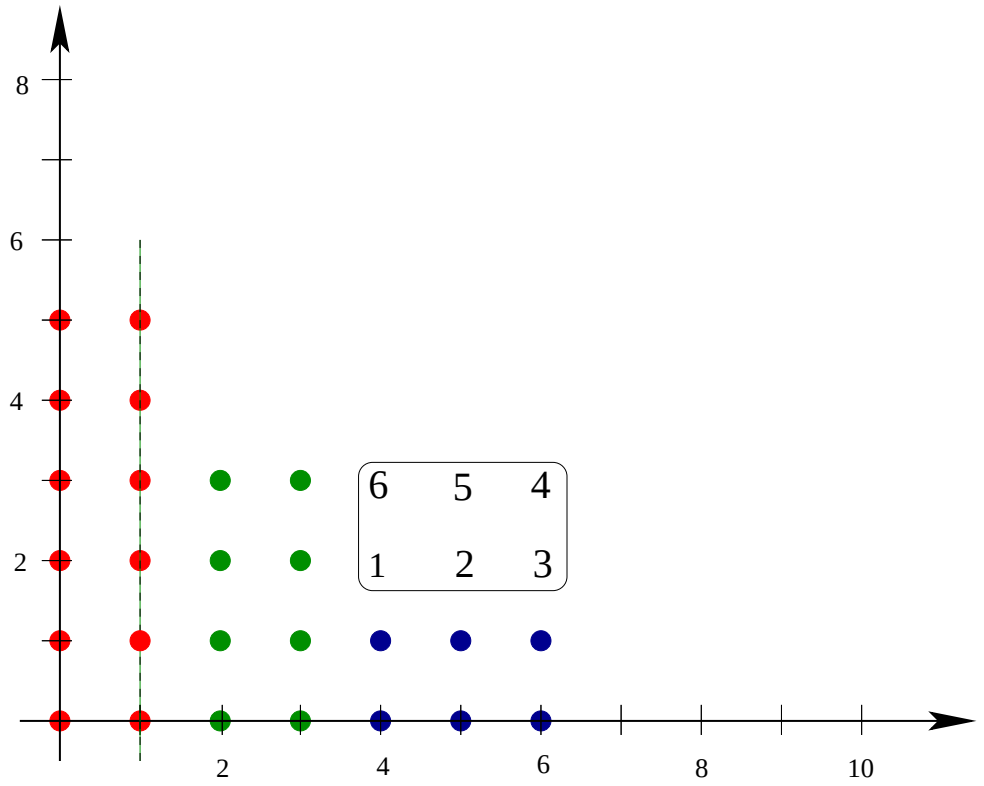
The polynomial f_3 should vanish on the blue and green points.

The choices for f_3 depend on 6 parameters: $(a_i, b_i)_{i=3,7,9}$.

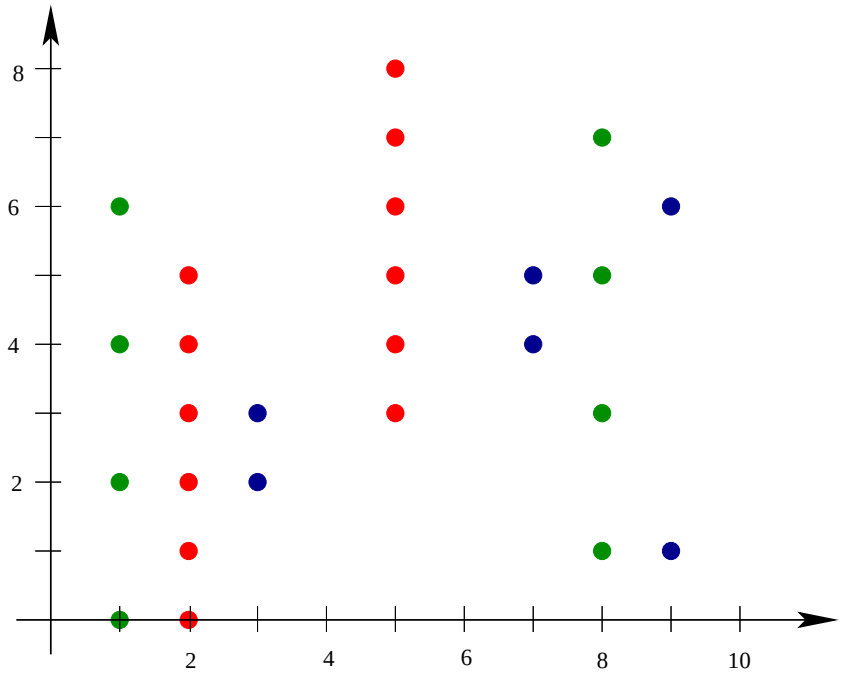
About the choices for f_3

Why 6 ?

Choice of 3 monic univariate polynomials of degree 2.



Computation of g_4



Leading monomials:

$\langle X^7\,,\ X^4Y^2\,,\ X^2Y^4\,,\ Y^6\rangle.$

$$g_1(X) = X^7 + \cdots$$

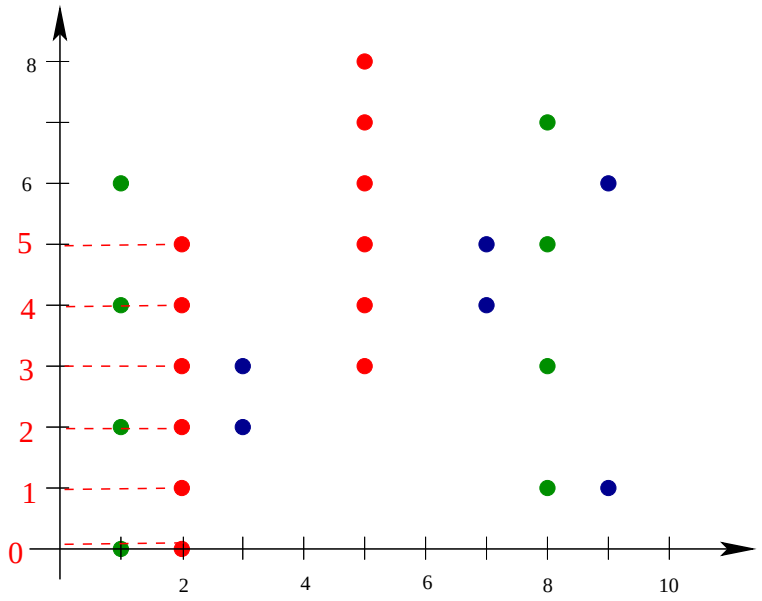
$$g_2(X,Y) = X^4Y^2 + \cdots$$

$$g_3(X,Y) = X^2Y^4 + \cdots$$

$$g_4(X,Y) = Y^6 + \cdots$$

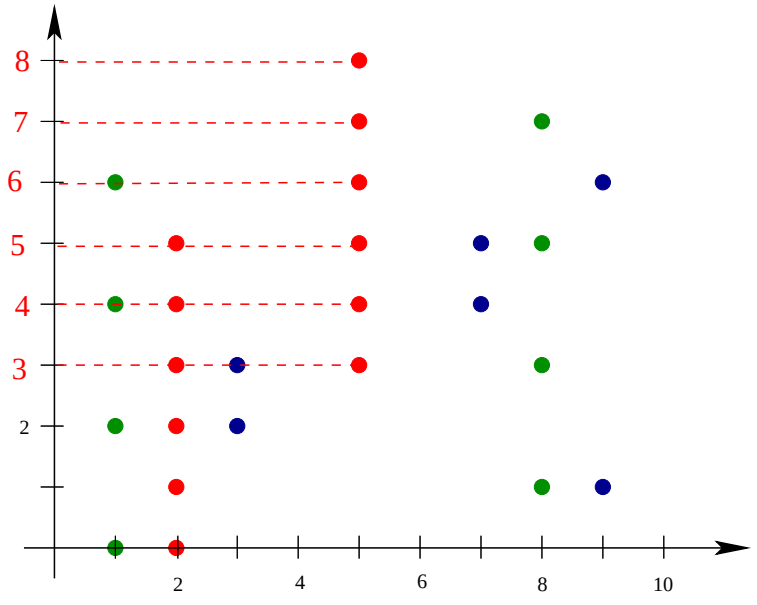
Same strategy as used for computing g_3.

Computation of g_4



$$
\begin{aligned}
q_1(Y) &= Y(Y-2)(Y-4)(Y-6) \\
q_8(Y) &= (Y-1)(Y-3)(Y-5)(Y-7) \\
q_3(Y) &= (Y-2)(Y-3) \\
q_7(Y) &= (Y-4)(Y-5) \\
q_9(Y) &= (Y-1)(Y-6) \\
q_2(Y) &= \prod_{i=0}^{5}(Y-i)
\end{aligned}
$$

Computation of g_4



$$
\begin{aligned}
q_1(Y) &= Y(Y-2)(Y-4)(Y-6) \\
q_8(Y) &= (Y-1)(Y-3)(Y-5)(Y-7) \\
q_3(Y) &= (Y-2)(Y-3) \\
q_7(Y) &= (Y-4)(Y-5) \\
q_9(Y) &= (Y-1)(Y-6) \\
q_2(Y) &= \prod_{i=0}^{5}(Y-i) \\
q_5(Y) &= \prod_{i=3}^{8}(Y-i)
\end{aligned}
$$

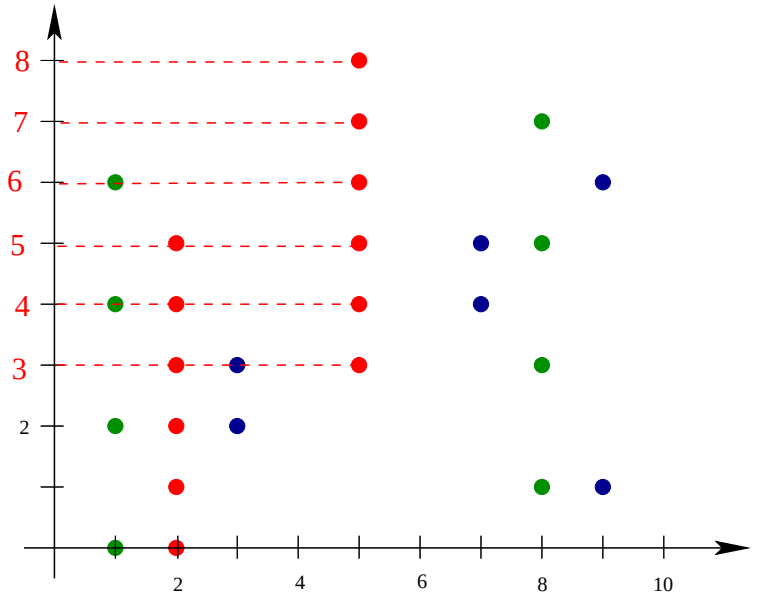
Lagrange formula on non-equiprojectable varieties

The interpolants **have not** the same degree:

$\Longrightarrow$ straightforward Lagrange interpolation $\rightarrow$ leading monomial $\neq Y^6$ as required.

Need to elevate the leading terms to Y^6

Computation of g_4



$$
\begin{aligned}
q_1(Y) &= Y(Y-2)(Y-4)(Y-6) \\
q_8(Y) &= (Y-1)(Y-3)(Y-5)(Y-7) \\
q_3(Y) &= (Y-2)(Y-3) \\
q_7(Y) &= (Y-4)(Y-5) \\
q_9(Y) &= (Y-1)(Y-6) \\
q_2(Y) &= \prod_{i=0}^{5}(Y-i) \\
q_5(Y) &= \prod_{i=3}^{8}(Y-i)
\end{aligned}
$$

Choosing g_4

$$
\begin{aligned}
Q_3(Y) &= (Y-2)(Y-3)(Y^4+\cdots) \\
Q_7(Y) &= (Y-4)(Y-5)(Y^4+\cdots) \\
Q_9(Y) &= (Y-1)(Y-6)(Y^4+\cdots) \\
Q_1(Y) &= Y(Y-2)(Y-4)(Y-6)(Y^2+\cdots) \\
Q_8(Y) &= (Y-1)(Y-3)(Y-5)(Y-7)(Y^2+\cdots)
\end{aligned}
$$

Whatever are the polynomials.

Choosing g_4

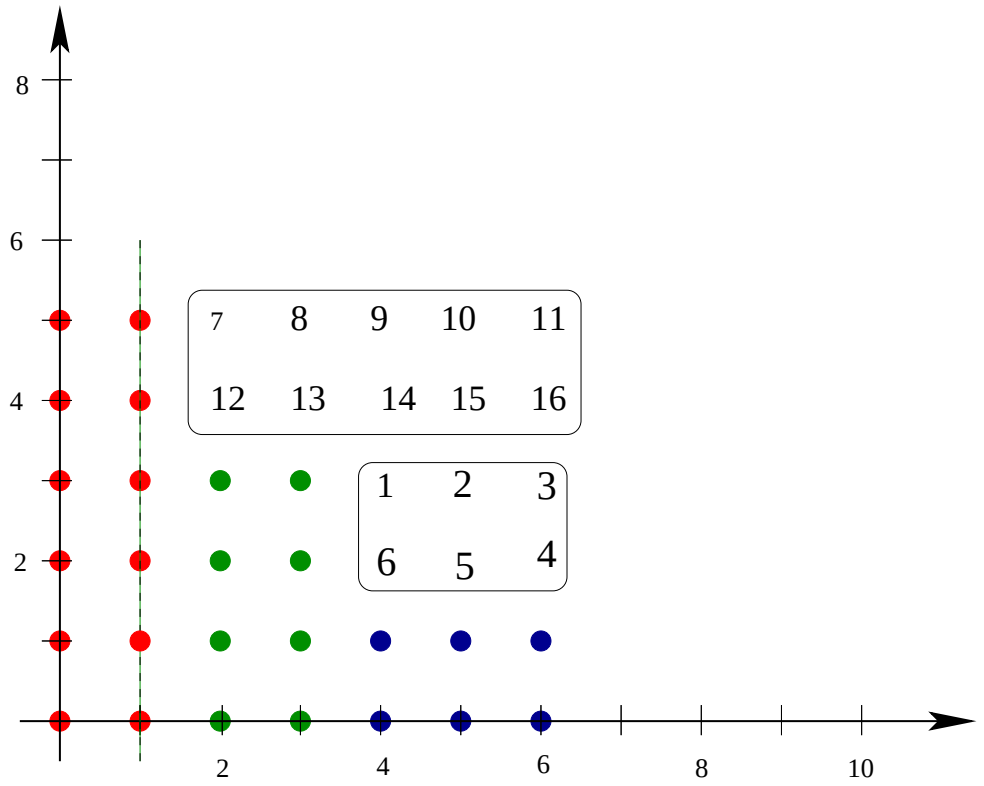
$$
\begin{aligned}
Q_3(Y) &= (Y-2)(Y-3)(Y^4+\cdots) \\
Q_7(Y) &= (Y-4)(Y-5)(Y^4+\cdots) \\
Q_9(Y) &= (Y-1)(Y-6)(Y^4+\cdots) \\
Q_1(Y) &= Y(Y-2)(Y-4)(Y-6)(Y^2+\cdots) \\
Q_8(Y) &= (Y-1)(Y-3)(Y-5)(Y-7)(Y^2+\cdots)
\end{aligned}
$$

Whatever are the polynomials.

There are 2x2+3x4=16 parameters above, that leads to a monic Gröbner basis.

Choosing g_4

Why 16 parameters ?



About the choices of polynomials

Fact: (non-generic) Gröbner bases depend on many "paramters" (making difficult to estimate the size of coefficients).

Small coefficients ? Choose polynomials only equal to the required power of Y $\rightarrow$ The Specific Gröbner basis

The reduced GB: Computed by solving a linear system:

unknowns $\rightarrow$ the coefficients of the complementary polynomials

equations $\rightarrow$ given by the monomial cancellations

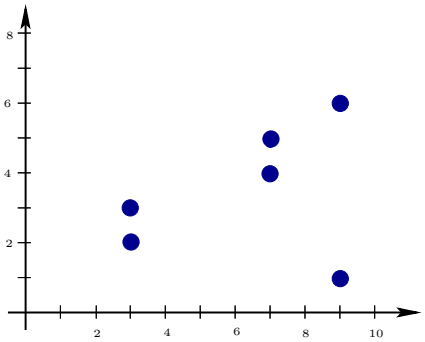
solvability $\rightarrow$ existence and unicity of the reduced GB

Implies an overgrowth of the coefficients

Quantifiable using Hadamard's inequality and Camer's rule.

Algorithmic consequence

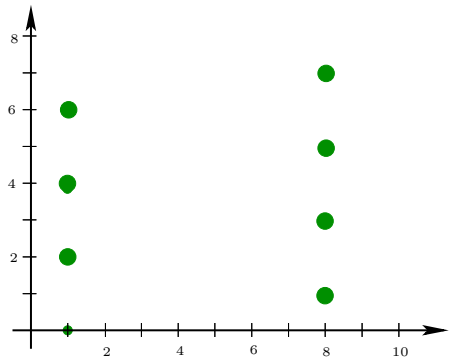
Chinese remaindering map for lex. GB:



Lex. GB of the green points:

$$c_2(X,Y) = Y^4 + \ldots$$

$$c_1(X) = X^2 + \ldots$$



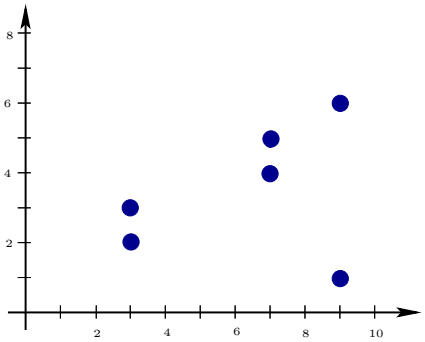
Lex. GB of the blue points:

$$b_2(X,Y) = Y^2 + \ldots$$

$$b_1(X) = X^3 + \ldots$$

Algorithmic consequence

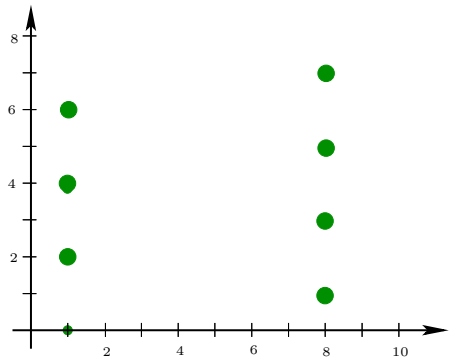
Chinese remaindering map for lex. GB:



Lex. GB of the green points:

$c_2(X,Y) = Y^4 + \ldots$

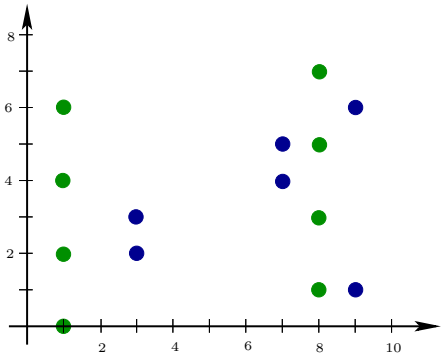
$c_1(X) = X^2 + \ldots$



Lex. GB of the blue points:

$b_2(X,Y) = Y^2 + \ldots$

$b_1(X) = X^3 + \ldots$



Let g_1, g_2, g_3 a GB of the blue and green points:

$g_1(X) = c_1(X)b_1(X)$

$g_3(X,Y) = b_2(X,Y) \bmod b_1(X)$

$g_3(X,Y) = c_2(X,Y) \bmod c_1(X)$

Algorithmic consequence

CRT algorithm:

$u(X), v(X) \leftarrow \text{BézoutCoefficients}(b_1(X), c_1(X))$

$g_2(X, Y) \leftarrow c_1(X)\, b_2(X, Y)$

$g_3(X, Y) \leftarrow c_2(X, Y) u(X) b_1(X) + b_2(X, Y)\, v(X)\, c_1(X) Y^2$

The Y^2 is essential! $lt(Y^2 b_2) = lt(c_2) = Y^4$, else $lt(g_3) \neq Y^4$.

Algorithmic consequence

CRT algorithm:

$u(X), v(X) \leftarrow \text{BézoutCoefficients}(b_1(X), c_1(X))$

$g_2(X, Y) \leftarrow c_1(X)\, b_2(X, Y)$

$g_3(X, Y) \leftarrow c_2(X, Y) u(X) b_1(X) + b_2(X, Y)\, v(X)\, c_1(X) Y^2$

The Y^2 is essential! $lt(Y^2 b_2) = lt(c_2) = Y^4$, else $lt(g_3) \neq Y^4$.

The GB g_1, g_2, g_3 henceforth obtained is the specific GB (not the reduced).

It is constructed from elementary pieces: coefficients **small** comparing to the reduced.

Algorithmic consequence

The reduced Gröbner basis:

No CRT.

Need to use **Lagrange inerpolation + linear algebra**.

Size of the system depends on the **monomial escalier**.

Restrictions, hypotheses, results

First step toward giving upper bounds:

For a **specific** Gröbner basis (not reduced) $\{g_1, g_2, \ldots, g_s\}$:

$$h(g_{\ell+1}) \leq 4hd^3 + 6d^4(\log d + 2) + O(d^3 \log d).$$

For the **reduced** Gröbner basis $\{g'_1, g'_2, \ldots, g'_s\}$: **(worst case)**

$$h(g'_{\ell+1}) \leq 8hd^7 + 12d^8(\log d + 2) + O(d^8 \log d).$$

(NOT SHARP for most of the cases)

For the **reduced** Gröbner basis $\{g'_1, g'_2, \ldots, g'_s\}$: **(median case)**

$$h(g'_{\ell+1}) \leq 8hd^5 + 12d^6(\log d + 2) + O(d^6 \log d).$$

(MORE REALISTIC in general)

Application to modular methods

Step 1: Estimate for lucky primes.

Bonus. Work already done* for the equiprojectable decomposition:

Equiprojectable decomp. $\Leftrightarrow$ lex. GB

There exists $A \in \mathbb{N}$,with $h(A) \leq 8d^4(h + 4(\log d) + 5)$ s.t.:
If p is a prime **not dividing** A, then p is lucky.

Bad: Very large in general $\rightarrow$ probabilistic choice : **99%** of success for p in the order of the **logarithm** of A.

---

*: (Moreno Maza, Schost, Xie, Wu & D., ISSAC'05)

Application to modular methods

Step 2: Computation of the lex GB modulo p

$\Leftrightarrow$ knowledge of the structure.

$\Leftrightarrow$ use of the sharp bounds for the **Step 3:**, to stop the lifting process.

$$\begin{aligned} h(g_{\ell+1}) &\leq h(V) + (2d_{\leq \ell} - 3)\left(\sum_{i=1}^{\ell} \frac{h(V_i)}{e_i}\right) + \log d_{>\ell} \\ &+ (2d_{\leq \ell} - 2)\left(\sum_{i=1}^{\ell} \frac{1}{e_i}(2d_i \log 2 + (e_i + 1)\log d_i)\right) \\ &+ e_\ell \log 2 + (3d_{\leq \ell}^2 - 5d_{\leq \ell} + 9)\log d_{\leq \ell} \end{aligned}$$

Triangular decomposition

Principle: Generalization of GCD computations for multivariate polynomials.

Cf. Talk at ISSAC'09: Moreno Maza, *GCD modulo Regular Chains*

Permits to compute the equiprojectable decomposition.

Using **CRT**: permits to compute the specific GB.

equiprojectable triangular dec. $\Leftrightarrow$ factors of the Specific GB

Triangular decomposition

Principle: Generalization of GCD computations for multivariate polynomials.

Cf. Talk at ISSAC'09: Moreno Maza, *GCD modulo Regular Chains*

Permits to compute the equiprojectable decomposition.

Using **CRT**: permits to compute the specific GB.

equiprojectable triangular dec. $\Leftrightarrow$ factors of the Specific GB

Faster compuations for triangular decomposition ?

Benchmarks in `RegularChains` in Maple 13:

YES. Even much faster for highly non-generic systems.

Conclusion

- New upper bounds on the size of coefficients of lex. GB.
- Complete study of the sharpness, in accordance with experimentations.
- CRT for lex GB. Link with non-reduced GB. Link with equiprojectable triangular decomposition.

Generalization: $n > 2$ possible: elimination property of lex. GB permits induction.

Deals with multiplicities... more tricky, but certainly possible: use of generalized equiprojectable decomposition.