Complexité du calcul de bases de Gröbner pour les systèmes quasi-homogènes

Jean-Charles Faugère[1] Mohab Safey El Din[1,2]

Thibaut Verron[1,3]

[1]Université Pierre et Marie Curie, Paris 6, France
INRIA Paris-Rocquencourt, Équipe PolSys
Laboratoire d'Informatique de Paris 6, UMR CNRS 7606

[2]Institut Universitaire de France

[3]École Normale Supérieure, Paris

16 mai 2013

Polynomial system solving

Applications:

- Cryptography
- Physics, industry...
- Theory (algo. geometry)

Polynomial system

$f_1(\mathbf{X}) = \cdots = f_m(\mathbf{X}) = 0$

Solutions

$\{P_1, \ldots, P_n\}$

- Numerical: give approximations of the solutions
  - Newton's method
  - Homotopy continuation method
- Symbolic: give exact solutions
  - Gröbner bases (Buchberger, Faugère...)
  - Resultant method
  - Triangular sets
  - Special algorithms for finite fields (exhaustive search, SAT-solvers, hybrid methods...)

Difficult problem

- NP-hard on finite fields
- Exponential number of solutions

Gröbner bases

Polynomial system

$$\begin{cases} f:\ X^2 + 2XY + Y^2 + X = 0 \\ g:\ X^2 - XY + Y^2 + Y - 1 = 0 \end{cases}$$

Macaulay matrix

$$\begin{array}{r} Xf \\ Yf \\ f \\ Xg \\ Yg \\ g \end{array} \begin{bmatrix} 1 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 1 & -1 \end{bmatrix}$$

Gröbner basis

$$\begin{cases} Y^3 + Y^2 - \frac{4}{9}X - \frac{2}{9}Y - \frac{4}{9} \\ X^2 + Y^2 + \frac{1}{3}X + \frac{2}{3}Y - \frac{2}{3} \\ XY + \frac{1}{3}X - \frac{1}{3}Y + \frac{1}{3} \end{cases}$$

Row-echelon form

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{8}{9} & -\frac{4}{9} & \frac{1}{9} \\ 0 & 1 & 0 & 0 & 0 & 0 & -\frac{1}{3} & \frac{1}{3} & -\frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 1 & 0 & 0 & 0 & -\frac{1}{3} & -\frac{1}{9} & \frac{4}{9} & -\frac{1}{9} \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & -\frac{4}{9} & -\frac{2}{9} & -\frac{4}{9} \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & \frac{1}{3} & \frac{2}{3} & -\frac{2}{3} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \frac{1}{3} & -\frac{1}{3} & \frac{1}{3} \end{bmatrix}$$

Polynomial system

$$\begin{cases} f: X^2 + 2XY + Y^2 + X = 0 \\ g: X^2 - XY + Y^2 + Y - 1 = 0 \end{cases}$$

Gröbner basis

$$\begin{cases} Y^3 + Y^2 - \frac{4}{9}X - \frac{2}{9}Y - \frac{4}{9} \\ X^2 + Y^2 + \frac{1}{3}X + \frac{2}{3}Y - \frac{2}{3} \\ XY + \frac{1}{3}X - \frac{1}{3}Y + \frac{1}{3} \end{cases}$$

Problematic

Structured systems
$\rightarrow$ Can we exploit it?

Successfully studied structures

- Bihomogeneous (Dickenstein, Emiris, Faugère, Safey, Spaenlehauer...)
- Group symmetries (Colin, Faugère, Gattermann, Rahmany, Svartz...)
- Quasi-homogeneous?

Quasi-homogeneous systems

Definition

System of weights: $W = (w_1, \ldots, w_n) \in \mathbb{N}^n$

Weighted degree: $\deg_W(X_1^{\alpha_1} \ldots X_n^{\alpha_n}) = \sum_{i=1}^{n} w_i \alpha_i$

Quasi-homogeneous polynomial: poly. containing only monomials of same W-degree

e.g. $X^2 + XY^2 + Y^4$ for $W = (2, 1)$

- Homogeneous systems are W-homogeneous with weights $(1, \ldots, 1)$.

Applications

Physical system

Volume $=$ Area $\times$ Height

Weight 3 Weight 2 Weight 1

Polynomial inversion

$$\begin{cases} X = T^2 + U^2 & \text{Weight 2} \\ Y = T^3 - TU^2 & \text{Weight 3} \\ Z = T + 2U & \text{Weight 1} \end{cases}$$

$\longrightarrow P(X, Y, Z) = 0$

Quasi-homogeneous systems

Definition

System of weights: $W = (w_1, \dots, w_n) \in \mathbb{N}^n$

Weighted degree: $\deg_W(X_1^{\alpha_1} \dots X_n^{\alpha_n}) = \sum_{i=1}^{n} w_i \alpha_i$

Quasi-homogeneous polynomial: poly. containing only monomials of same W-degree

e.g. $X^2 + XY^2 + Y^4$ for $W = (2, 1)$

- Homogeneous systems are W-homogeneous with weights $(1, \dots, 1)$.

Applications

Physical system

Volume $=$ Area $\times$ Height

Weight 3 Weight 2 Weight 1

Polynomial inversion

Weight 2

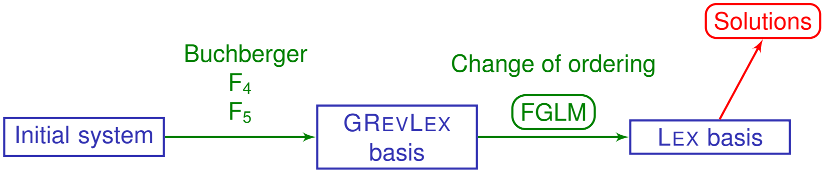
Weight 3

Weight 1

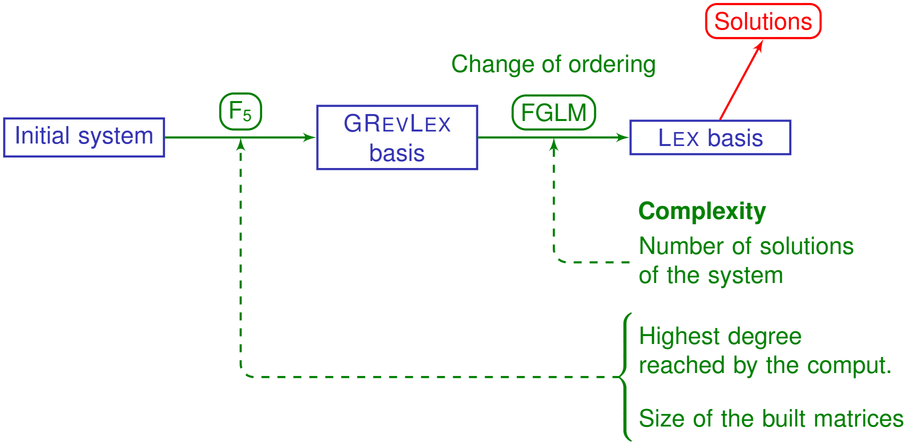
$$\left\{\begin{aligned} X &= T^2 + U^2 \\ Y &= T^3 - TU^2 \\ Z &= T + 2U \end{aligned}\right.$$

$\longrightarrow P(X, Y, Z) = 0$

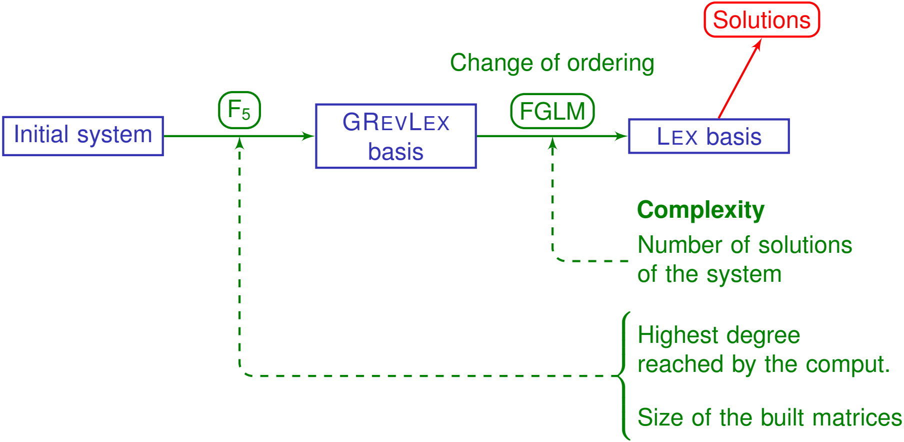
Usual two-steps strategy in the zero-dimensional case



Usual two-steps strategy in the zero-dimensional case



Usual two-steps strategy in the zero-dimensional case



Goal

Under generic assumptions, complexity polynomial in the number of solutions

Complexity for generic homogeneous systems

Homogeneous, generic, with degree $(d_1, \ldots, d_n)$

Initial system

F_5

Highest degree $\leq \sum_{i=1}^{n} (d_i - 1) + 1$

Size of the matrix at degree $d = \binom{n+d-1}{d}$

GRevLex basis

FGLM

Number of solutions $= \prod_{i=1}^{n} d_i$ (Bézout bound)

Lex basis

Main results: strategy and complexity results

$W = (w_1, \dots, w_n)$

Initial system ← W-Homogeneous, generic, with W-degree $(d_1, \dots, d_n)$

Modified system ← Homogeneous, with degree $(d_1, \dots, d_n)$

F_5 ← Highest W-degree

$$\leq \sum_{i=1}^{n}(d_i - 1) + 1 - \sum_{i=1}^{n}(w_i - 1) + \max\{w_j\} - 1$$

$$\leq \sum_{i=1}^{n}(d_i - w_i) + \max\{w_j\}$$

Size of the matrix at W-degree $d \simeq \frac{1}{\prod_{i=1}^{n} w_i}\binom{n+d-1}{d}$

W-GRevLex basis of F

FGLM ← Number of solutions $= \frac{\prod_{i=1}^{n} d_i}{\prod_{i=1}^{n} w_i}$ (weighted Bézout bound)

Lex basis

Roadmap

Input

- $W = (w_1, \ldots, w_n)$ system of weights.
- $F = (f_1, \ldots, f_n)$ generic sequence of W-homogeneous polynomials with W-degree $(d_1, \ldots, d_n)$.

General roadmap:

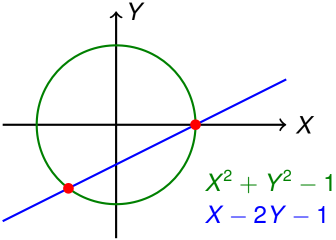
1. Find a generic property which rules out all reductions to zero
   - Regular sequences
2. Design new algorithms to take advantage of this structure
   - Adapt algorithms for the homogeneous case to the quasi-homogeneous case
3. Obtain complexity results

Regular sequences

Definition

$F = (f_1, \ldots, f_m)$ homo. $\in \mathbb{K}[\mathbf{X}]$ is regular iff

$$\begin{cases} \langle F \rangle \subsetneq \mathbb{K}[\mathbf{X}] \\ \forall i,\ f_i \text{ is no zero-divisor in } \mathbb{K}[\mathbf{X}]/\langle f_1, \ldots, f_{i-1} \rangle \end{cases}$$

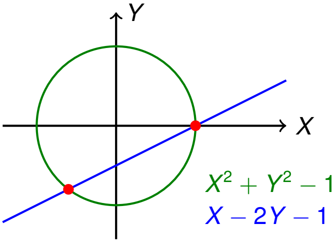


Regular sequences

Definition

$F = (f_1, \ldots, f_m)$ homo. $\in \mathbb{K}[\mathbf{X}]$ is regular iff

$$\begin{cases} \langle F \rangle \subsetneq \mathbb{K}[\mathbf{X}] \\ \forall i,\ f_i \text{ is no zero-divisor in } \mathbb{K}[\mathbf{X}]/\langle f_1, \ldots, f_{i-1} \rangle \end{cases}$$



Regular sequences of homo. polynomials → Generic

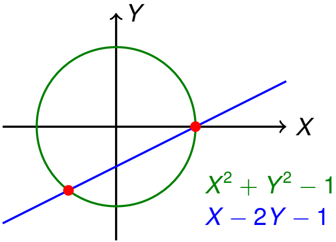
Regular sequences of homo. polynomials → Good properties → F_5-criterion, Hilbert series

Regular sequences

Definition

$F = (f_1, \ldots, f_m)$ quasi-homo. $\in \mathbb{K}[\mathbf{X}]$ is regular iff

$$\begin{cases} \langle F \rangle \subsetneq \mathbb{K}[\mathbf{X}] \\ \forall i,\ f_i \text{ is no zero-divisor in } \mathbb{K}[\mathbf{X}]/\langle f_1, \ldots, f_{i-1} \rangle \end{cases}$$



Result (Faugère, Safey, V.)

Regular sequences of quasi-homo. polynomials → Generic if $\neq \varnothing$

Regular sequences of quasi-homo. polynomials → Good properties → F_5-criterion, Hilbert series

From quasi-homogeneous to homogeneous

Transformation morphism

$$\begin{array}{rcccc} \mathrm{hom}_W : & (\mathbb{K}[\mathbf{X}], W\text{-deg}) & \rightarrow & (\mathbb{K}[\mathbf{X}], \mathrm{deg}) \\ & f & \mapsto & f(X_1^{w_1}, \ldots, X_n^{w_n}) \end{array}$$

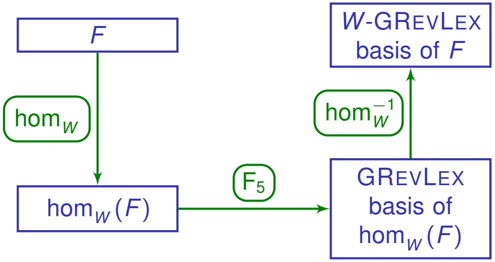
- Graded injective morphism.
- Sends regular sequences on regular sequences
- Good behavior w.r.t Gröbner bases (forth and back)

$$\begin{tikzcd}
\text{(Quasi-homogeneous)} & \boxed{F} \arrow[r, "\text{Gröbner}"] \arrow[d, "\mathrm{hom}_W"'] & \boxed{\begin{array}{c}\text{Basis of } F \\ \text{w.r.t } \mathrm{hom}_W^{-1}(\prec)\end{array}} \\
\text{(Homogeneous)} & \boxed{\mathrm{hom}_W(F)} \arrow[r, "\text{Gröbner}"] & \boxed{\begin{array}{c}\text{Basis of } \mathrm{hom}_W(F) \\ \text{w.r.t } \prec\end{array}} \arrow[u, "\mathrm{hom}_W^{-1}"']
\end{tikzcd}$$

Adapting the algorithms

Detailed strategy

- F_5 algorithm on the homogenized system
- FGLM algorithm on the quasi-homogeneous system



Adapting the algorithms

Detailed strategy

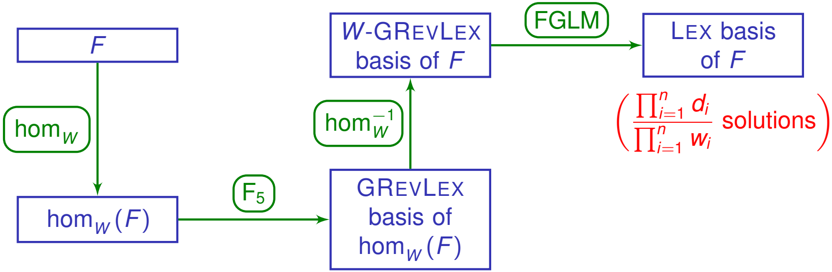
- F_5 algorithm on the homogenized system
- FGLM algorithm on the quasi-homogeneous system

$$
\begin{tikzcd}
\boxed{F} \arrow[d, "\mathrm{hom}_W"'] & & \boxed{\begin{array}{c} W\text{-GRevLex} \\ \text{basis of } F \end{array}} \arrow[r, dashed] & \dfrac{\prod_{i=1}^n d_i}{\prod_{i=1}^n w_i} \text{ solutions} \\
\boxed{\mathrm{hom}_W(F)} \arrow[rr, "F_5"] & & \boxed{\begin{array}{c} \text{GRevLex} \\ \text{basis of} \\ \mathrm{hom}_W(F) \end{array}} \arrow[u, "\mathrm{hom}_W^{-1}"] \arrow[r, dashed] & \prod_{i=1}^n d_i \text{ solutions}
\end{tikzcd}
$$

Adapting the algorithms

Detailed strategy

- F_5 algorithm on the homogenized system
- FGLM algorithm on the quasi-homogeneous system

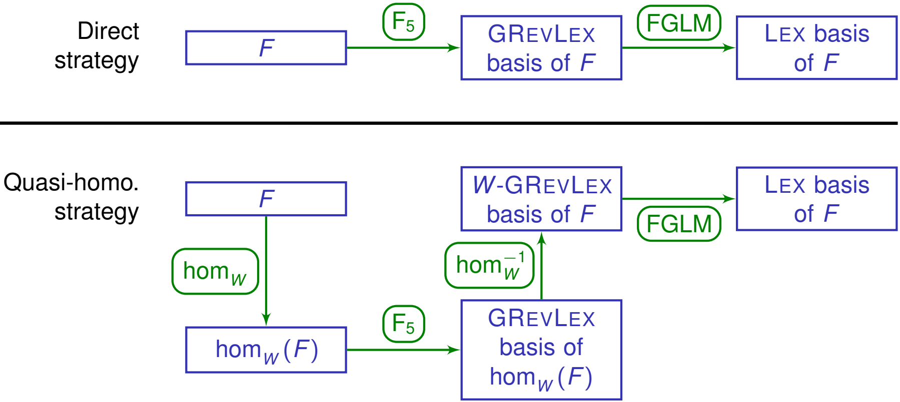


Benchmarks (1)

F : affine system with a quasi-homogeneous structure

$$f_i = \sum_{\alpha} c_\alpha m_\alpha \text{ with } \deg_W(m_\alpha) \leq d_i$$

Assumption: the highest W-degree components are regular (e.g. if F is generic)



Benchmarks (2)

n	$\deg(I)$	t_{F_5}(qh)	Speed-up for F_5	t_{FGLM}(qh)	Speed-up for FGLM
10	4096	7.5 s	5.4	2.4 s	2.6
11	8192	33.3 s	6.4	17.5 s	2.4
12	16 384	167.9 s	6.8	115.8 s	2.1
13	32 768	796.7 s	8.4	782.7 s	2.1
14	65 536	5040.1 s	∞	5602.3 s	

Benchmarks obtained with FGb on generic affine systems
with W-degree (4) for $W = (2, \dots, 2, 1, 1)$

n	$\deg(I)$	t_{F_5}(qh)	Speed-up for F_5	t_{FGLM}(qh)	Speed-up for FGLM
4	512	0.1 s	1	0.1 s	1
5	65 536	935.4 s	6.9	2164.4 s	3.2

Benchmarks obtained with real systems
(DLP on Edwards curves : Faugère, Gaudry, Huot, Renault 2013):
W-degree (4) w.r.t $W = (2, \dots, 2, 1)$

Conclusion

What we have done

- Theoretical results for quasi-homogeneous systems under generic hypotheses
- Computational strategy for quasi-homogeneous systems
- Complexity results for F_5 and FGLM for this strategy
  - Bound on the maximal degree reached by the F_5 algorithm
  - Complexity overall divided by $(\prod w_i)^\omega$
  - Polynomial in the number of solutions

Perspectives

- Overdetermined systems: adapt the definitions and the results
- Affine systems: find the most appropriate system of weights

Conclusion

What we have done

- Theoretical results for quasi-homogeneous systems under generic hypotheses
- Computational strategy for quasi-homogeneous systems
- Complexity results for F_5 and FGLM for this strategy
  - Bound on the maximal degree reached by the F_5 algorithm
  - Complexity overall divided by $(\prod w_i)^{\omega}$
  - Polynomial in the number of solutions

Perspectives

- Overdetermined systems: adapt the definitions and the results
- Affine systems: find the most appropriate system of weights

One last word

Thank you for your attention!