On The Complexity Of Computing Gröbner Bases For Quasi-Homogeneous Systems

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, France

June 29, 2013

Motivation

Discrete Logarithm Problem (Faugère, Gaudry, Huot, Renault 2013)

$$0 = \begin{bmatrix} 7871 \\ 18574 \\ 14294 \\ 32775 \\ 20289 \end{bmatrix} e_5^{16} + \begin{bmatrix} 53362 \\ 50900 \\ 36407 \\ 58813 \\ 20802 \end{bmatrix} \tilde{e}_1^8 + \begin{bmatrix} 26257 \\ 128 \\ 3037 \\ 38424 \\ 41456 \end{bmatrix} \tilde{e}_1^7 \tilde{e}_2 + \begin{bmatrix} 25203 \\ 23117 \\ 28918 \\ 29298 \\ 56353 \end{bmatrix} \tilde{e}_1^6 \tilde{e}_2^2 + \begin{bmatrix} 19817 \\ 29737 \\ 52187 \\ 36574 \\ 46683 \end{bmatrix} \tilde{e}_1^5 \tilde{e}_2^3 + \begin{bmatrix} 9843 \\ 3752 \\ 27006 \\ 64195 \\ 63059 \end{bmatrix} \tilde{e}_1^4 \tilde{e}_2^4 + \begin{bmatrix} 11204 \\ 25459 \\ 58263 \\ 17964 \\ 57146 \end{bmatrix} \tilde{e}_1^3 \tilde{e}_2^5$$

$$+ \begin{bmatrix} 46217 \\ 5478 \\ 45631 \\ 13171 \\ 42548 \end{bmatrix} \tilde{e}_1^2 \tilde{e}_2^6 + \begin{bmatrix} 63811 \\ 50777 \\ 48809 \\ 1858 \\ 55751 \end{bmatrix} \tilde{e}_1 \tilde{e}_2^7 + \begin{bmatrix} 40524 \\ 6881 \\ 1238 \\ 8056 \\ 54831 \end{bmatrix} \tilde{e}_2^8 + \begin{bmatrix} 4522 \\ 1728 \\ 18652 \\ 54885 \\ 8241 \end{bmatrix} \tilde{e}_1^7 \tilde{e}_3 + \begin{bmatrix} 27518 \\ 32176 \\ 31159 \\ 28424 \\ 5276 \end{bmatrix} \tilde{e}_1^6 \tilde{e}_2 \tilde{e}_3 + \text{2067 smaller monomials}$$

Motivation

Discrete Logarithm Problem (Faugère, Gaudry, Huot, Renault 2013)

$$0 = \begin{bmatrix}7871\\18574\\14294\\32775\\20289\end{bmatrix} e_5^{16} + \begin{bmatrix}53362\\50900\\36407\\58813\\20802\end{bmatrix} \tilde{e}_1^{8} + \begin{bmatrix}26257\\128\\3037\\38424\\41456\end{bmatrix} \tilde{e}_1^{7}\tilde{e}_2 + \begin{bmatrix}25203\\23117\\28918\\29298\\56353\end{bmatrix} \tilde{e}_1^{6}\tilde{e}_2^{2} + \begin{bmatrix}19817\\29737\\52187\\36574\\46683\end{bmatrix} \tilde{e}_1^{5}\tilde{e}_2^{3} + \begin{bmatrix}9843\\3752\\27006\\64195\\63059\end{bmatrix} \tilde{e}_1^{4}\tilde{e}_2^{4} + \begin{bmatrix}11204\\25459\\58263\\17964\\57146\end{bmatrix} \tilde{e}_1^{3}\tilde{e}_2^{5}$$

$$+ \begin{bmatrix}46217\\5478\\45631\\13171\\42548\end{bmatrix} \tilde{e}_1^{2}\tilde{e}_2^{6} + \begin{bmatrix}63811\\50777\\48809\\1858\\55751\end{bmatrix} \tilde{e}_1\tilde{e}_2^{7} + \begin{bmatrix}40524\\6881\\1238\\8056\\54831\end{bmatrix} \tilde{e}_2^{8} + \begin{bmatrix}4522\\1728\\18652\\54885\\8241\end{bmatrix} \tilde{e}_1^{7}\tilde{e}_3 + \begin{bmatrix}27518\\32176\\31159\\28424\\5276\end{bmatrix} \tilde{e}_1^{6}\tilde{e}_2\tilde{e}_3 + \text{2067 smaller monomials}$$

Description of the system

- Ideal invariant under the group $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n$, rewritten with the invariants:
$$\begin{cases} \tilde{e}_i := e_i(x_1^2, \ldots, x_n^2) \;\; (1 \le i \le n-1) \\ e_n(x_1, \ldots, x_n) \end{cases}$$
- n equations of degree 2^{n-1} in $\mathbb{F}_q[\tilde{e}_1, \ldots, \tilde{e}_{n-1}, e_n]$
- 1 DLP = thousands of such systems

Goal: compute a Gröbner basis

- Total degree grading
  $\to$ difficult (intractable with Magma)
  $\to$ non regular
- Weighted degree grading
  $\mathrm{Weight}(\tilde{e}_i) = 2 \cdot \mathrm{Weight}(e_i)$
  $\to$ easier
  $\to$ regular
- Two questions:
  - Algorithms for this structure?
  - Complexity estimates?

Motivation

Discrete Logarithm Problem (Faugère, Gaudry, Huot, Renault 2013)

$$0 = \begin{bmatrix} 7871 \\ 18574 \\ 14294 \\ 32775 \\ 20289 \end{bmatrix} e_5^{16} + \begin{bmatrix} 53362 \\ 50900 \\ 36407 \\ 58813 \\ 20802 \end{bmatrix} \tilde{e}_1^8 + \begin{bmatrix} 26257 \\ 128 \\ 3037 \\ 38424 \\ 41456 \end{bmatrix} \tilde{e}_1^7 \tilde{e}_2 + \begin{bmatrix} 25203 \\ 23117 \\ 28918 \\ 29298 \\ 56353 \end{bmatrix} \tilde{e}_1^6 \tilde{e}_2^2 + \begin{bmatrix} 19817 \\ 29737 \\ 52187 \\ 36574 \\ 46683 \end{bmatrix} \tilde{e}_1^5 \tilde{e}_2^3 + \begin{bmatrix} 9843 \\ 3752 \\ 27006 \\ 64195 \\ 63059 \end{bmatrix} \tilde{e}_1^4 \tilde{e}_2^4 + \begin{bmatrix} 11204 \\ 25459 \\ 58263 \\ 17964 \\ 57146 \end{bmatrix} \tilde{e}_1^3 \tilde{e}_2^5$$

$$+ \begin{bmatrix} 46217 \\ 5478 \\ 45631 \\ 13171 \\ 42548 \end{bmatrix} \tilde{e}_1^2 \tilde{e}_2^6 + \begin{bmatrix} 63811 \\ 50777 \\ 48809 \\ 1858 \\ 55751 \end{bmatrix} \tilde{e}_1 \tilde{e}_2^7 + \begin{bmatrix} 40524 \\ 6881 \\ 1238 \\ 8056 \\ 54831 \end{bmatrix} \tilde{e}_2^8 + \begin{bmatrix} 4522 \\ 1728 \\ 18652 \\ 54885 \\ 8241 \end{bmatrix} \tilde{e}_1^7 \tilde{e}_3 + \begin{bmatrix} 27518 \\ 32176 \\ 31159 \\ 28424 \\ 5276 \end{bmatrix} \tilde{e}_1^6 \tilde{e}_2 \tilde{e}_3 + \text{2067 smaller monomials}$$

Description of the system

- Ideal invariant under the group $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n$,
  rewritten with the invariants:
  $$\begin{cases} \tilde{e}_i := e_i(x_1^2, \ldots, x_n^2) \quad (1 \leq i \leq n-1) \\ e_n(x_1, \ldots, x_n) \end{cases}$$
- n equations of degree 2^{n-1} in $\mathbb{F}_q[\tilde{e}_1, \ldots, \tilde{e}_{n-1}, e_n]$
- 1 DLP $=$ thousands of such systems

Goal: compute a Gröbner basis

- Total degree grading
  $\to$ difficult (intractable with Magma)
  $\to$ non regular
- Weighted degree grading
  $\text{Weight}(\tilde{e}_i) = 2 \cdot \text{Weight}(e_i)$
  $\to$ easier
  $\to$ regular
- Two questions:
  - Algorithms for this structure?
  - Complexity estimates?

Motivation

Discrete Logarithm Problem (Faugère, Gaudry, Huot, Renault 2013)

$$0 = \begin{bmatrix}7871\\18574\\14294\\32775\\20289\end{bmatrix} e_5^{16} + \begin{bmatrix}53362\\50900\\36407\\58813\\20802\end{bmatrix} \tilde{e}_1^{8} + \begin{bmatrix}26257\\128\\3037\\38424\\41456\end{bmatrix} \tilde{e}_1^{7}\tilde{e}_2 + \begin{bmatrix}25203\\23117\\28918\\29298\\56353\end{bmatrix} \tilde{e}_1^{6}\tilde{e}_2^{2} + \begin{bmatrix}19817\\29737\\52187\\36574\\46683\end{bmatrix} \tilde{e}_1^{5}\tilde{e}_2^{3} + \begin{bmatrix}9843\\3752\\27006\\64195\\63059\end{bmatrix} \tilde{e}_1^{4}\tilde{e}_2^{4} + \begin{bmatrix}11204\\25459\\58263\\17964\\57146\end{bmatrix} \tilde{e}_1^{3}\tilde{e}_2^{5}$$

$$+ \begin{bmatrix}46217\\5478\\45631\\13171\\42548\end{bmatrix} \tilde{e}_1^{2}\tilde{e}_2^{6} + \begin{bmatrix}63811\\50777\\48809\\1858\\55751\end{bmatrix} \tilde{e}_1\tilde{e}_2^{7} + \begin{bmatrix}40524\\6881\\1238\\8056\\54831\end{bmatrix} \tilde{e}_2^{8} + \begin{bmatrix}4522\\1728\\18652\\54885\\8241\end{bmatrix} \tilde{e}_1^{7}\tilde{e}_3 + \begin{bmatrix}27518\\32176\\31159\\28424\\5276\end{bmatrix} \tilde{e}_1^{6}\tilde{e}_2\tilde{e}_3 + \text{2067 smaller monomials}$$

Description of the system

- Ideal invariant under the group $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n$, rewritten with the invariants:
$$\begin{cases} \tilde{e}_i := e_i(x_1^2, \ldots, x_n^2) & (1 \le i \le n-1) \\ e_n(x_1, \ldots, x_n) \end{cases}$$
- n equations of degree 2^{n-1} in $\mathbb{F}_q[\tilde{e}_1, \ldots, \tilde{e}_{n-1}, e_n]$
- 1 DLP $=$ thousands of such systems

Goal: compute a Gröbner basis

- Total degree grading
  $\to$ difficult (intractable with Magma)
  $\to$ non regular
- Weighted degree grading
  $\text{Weight}(\tilde{e}_i) = 2 \cdot \text{Weight}(e_i)$
  $\to$ easier
  $\to$ regular
- Two questions:
  - Algorithms for this structure?
  - Complexity estimates?

Gröbner bases and structured systems

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
→ Can we exploit it?

Successfully studied structures

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

Quasi-homogeneous systems: définitions

Definition (e.g. [Robbiano 1986], [Becker and Weispfenning 1993])

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

Weighted degree (or W-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

$\rightarrow$ Example: physical systems: Volume $=$ Area $\times$ Height

Weight 3 Weight 2 Weight 1

Given a general (non-quasi-homogeneous) system and a system of weights

Computational strategy: quasi-homogenize it as in the homogeneous case

Complexity estimates: consider the highest-W-degree components of the system

- Enough to study quasi-homogeneous systems

Quasi-homogeneous systems: définitions

Definition (e.g. [Robbiano 1986], [Becker and Weispfenning 1993])

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

Weighted degree (or W-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

→ Example: physical systems: Volume = Area × Height

Weight 3 (Volume), Weight 2 (Area), Weight 1 (Height)

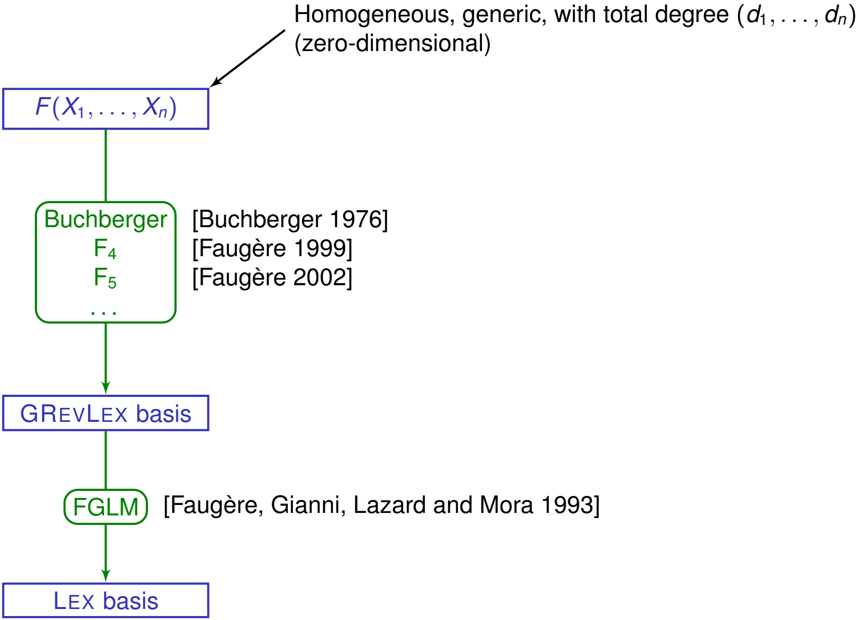
Given a general (non-quasi-homogeneous) system and a system of weights

Computational strategy: quasi-homogenize it as in the homogeneous case

Complexity estimates: consider the highest-W-degree components of the system

- Enough to study quasi-homogeneous systems

Complexity for generic homogeneous systems



Complexity for generic homogeneous systems

Homogeneous, generic, with total degree $(d_1, \ldots, d_n)$ (zero-dimensional)

$F(X_1, \ldots, X_n)$

↓

F_5 ⟵ Highest degree $d_{\max} \leq \sum_{i=1}^{n}(d_i - 1) + 1$; Size of a 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

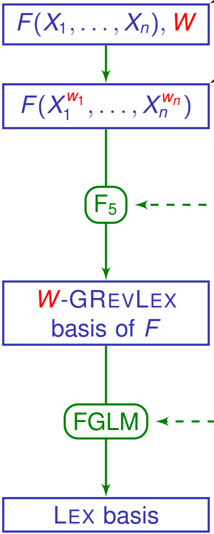
$$O\left(\binom{n+d_{\max}-1}{d_{\max}}^3 + n\left(\prod_{i=1}^{n} d_i\right)^3\right)$$

Main results: strategy and complexity results

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

W-Homogeneous, generic, with W-degree $(d_1, \ldots, d_n)$ (zero-dimensional)

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



Highest W-degree

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

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

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

$$O\left(\left(\frac{1}{\prod_{i=1}^{n} w_i}\right)^3 \left[\binom{n + d_{W,\max} - 1}{d_{W,\max}}^3 + n\left(\prod_{i=1}^{n} d_i\right)^3\right]\right)$$

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:

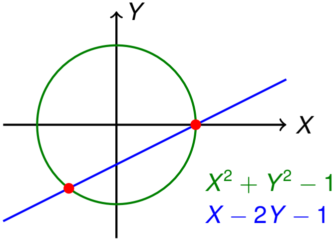
1. Find a generic property which rules out all reductions to zero
   - Regular sequences
2. Design new algorithms to take advantage of this structure
   - Adapt algorithms for the homogeneous case to the quasi-homogeneous case
3. Obtain complexity results

Regular sequences

Definition (e.g. [Eisenbud 1995])

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

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

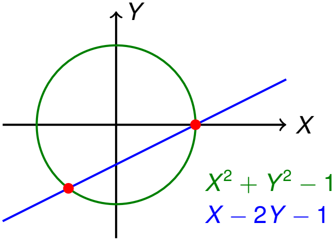


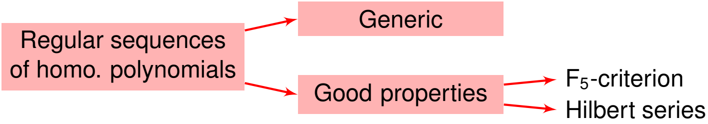
Regular sequences

Definition (e.g. [Eisenbud 1995])

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

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



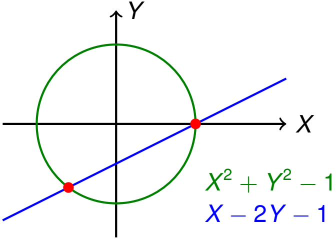


Regular sequences

Definition (e.g. [Eisenbud 1995])

$F = (f_1, \ldots, f_m)$ 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

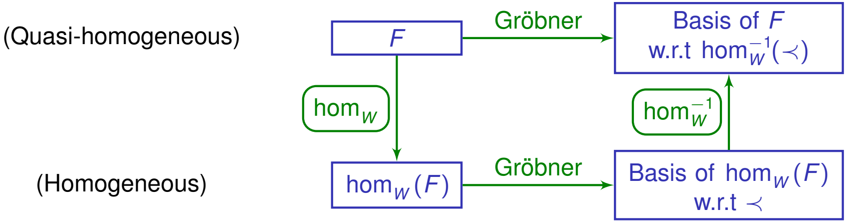
From quasi-homogeneous to homogeneous

Transformation morphism

$$\begin{array}{rccc} \hom_W : & (\mathbb{K}[\mathbf{X}], W\text{-deg}) & \to & (\mathbb{K}[\mathbf{X}], \deg) \\ & f & \mapsto & f(X_1^{w_1}, \ldots, X_n^{w_n}) \end{array}$$

- Graded injective morphism
- Sends regular sequences on regular sequences
- $\text{S-Pol}(\hom_W(f), \hom_W(g)) = \hom_W(\text{S-Pol}(f, g))$

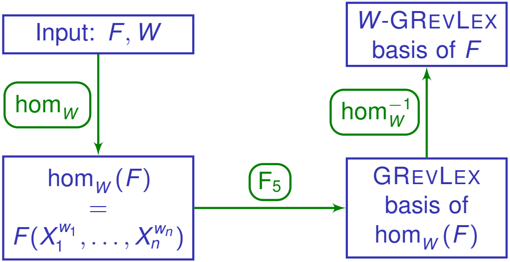
$\longrightarrow$ Good behavior w.r.t Gröbner bases



Adapting the algorithms

Detailed strategy

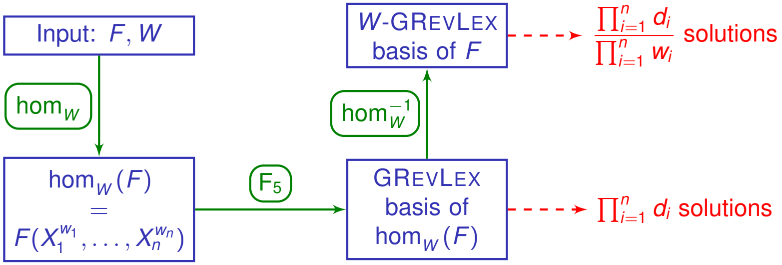
- F_5 algorithm on the homogenized system
- FGLM algorithm on the quasi-homogeneous system



Adapting the algorithms

Detailed strategy

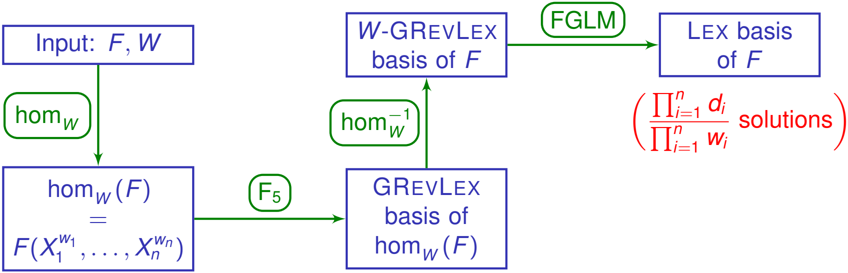
- F_5 algorithm on the homogenized system
- FGLM algorithm on the quasi-homogeneous system



Adapting the algorithms

Detailed strategy

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

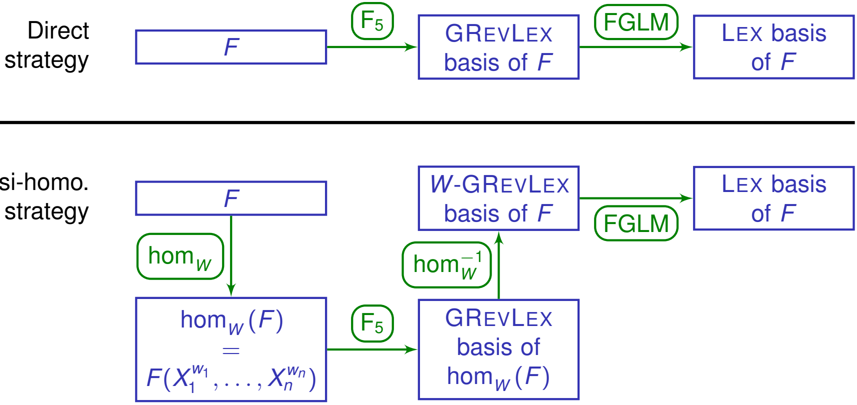


Benchmarking

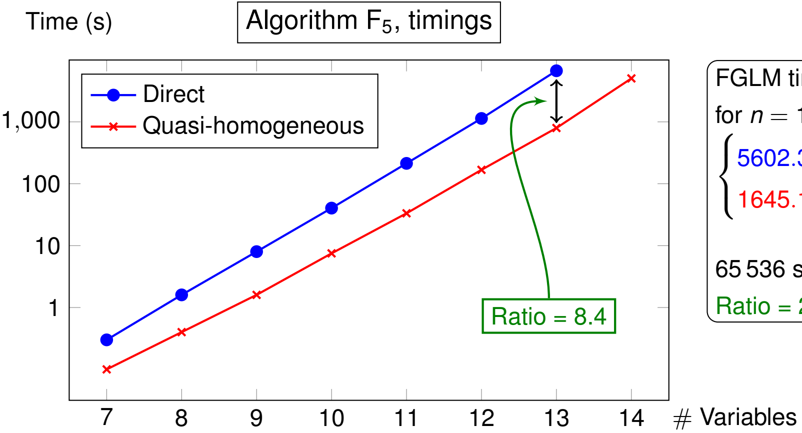
F : affine system with a quasi-homogeneous structure

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

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



Benchmarks for generic systems



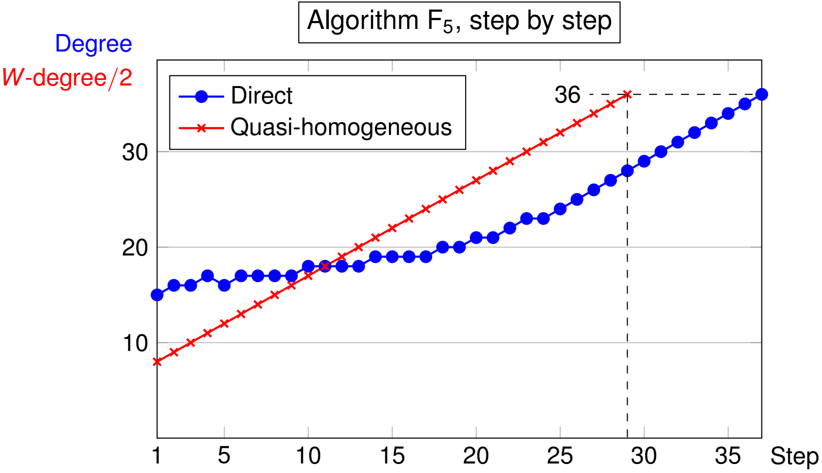
FGLM timing for $n = 13$:
$\begin{cases} 5602.3\,\text{s} \\ 1645.1\,\text{s} \end{cases}$

65 536 solutions

Ratio = 2.1

- Generic systems in n variables with $\begin{cases} \text{weights } W = (2, \ldots, 2, 1, 1) \\ W\text{-degree } D = (4, \ldots, 4) \end{cases}$
- Number of solutions: 2^{n+2}
- Benchmarks obtained with FGb : $\begin{cases} F_5 \text{ [Faugère 2002]} \\ \text{SPARSEFGLM [Faugère and Mou 2013]} \end{cases}$

A closer look at F_5 (the DLP example)



- 5 equations of W-degree $(16, \ldots, 16)$ in 5 variables with $W = (2, \ldots, 2, 1)$
- 65 536 solutions
- Timings:

Magma (F_4)	> 12 h	6044 s	Speed-up: 9.3
FGb (F_5)	12 297 s	567 s	Speed-up: 21.7

Conclusion

What we have done

- Theoretical results for quasi-homogeneous systems under generic assumptions
- 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 $(\prod w_i)^3$

Consequences

- Successfully applied to a cryptographical problem
- Wide range of potential applications

Perspectives

- Overdetermined systems: adapt the definitions and the results
- Affine systems: find the most appropriate system of weights
  (e.g for the DLP, how to choose the weights of the e_i's?)

Conclusion

What we have done

- Theoretical results for quasi-homogeneous systems under generic assumptions
- 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 $(\prod w_i)^3$

Consequences

- Successfully applied to a cryptographical problem
- Wide range of potential applications

Perspectives

- Overdetermined systems: adapt the definitions and the results
- Affine systems: find the most appropriate system of weights (e.g for the DLP, how to choose the weights of the e_i's?)

Thank you for your attention!