On The Complexity Of Computing Gröbner Bases For Weighted Homogeneous Systems

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

Thibaut Verron[1]

[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

Journées Nationales de Calcul Formel, 6 novembre 2014

Context

Polynomial System Solving

- Input: polynomial system $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$
- Output: exact solution

Important and difficult

- Many applications
  - Cryptography, mechanics...
- Difficult problem
  - Decision problem is NP-hard
- Many tools
  - Triangular sets [Aubry, Lazard and Moreno Maza 1999]
  - Resultants [Cattani and Dickenstein 2005]
  - Geometric resolution [Giusti, Lecerf and Salvy 2001]
  - Gröbner bases [Buchberger 1965]

Context

Polynomial System Solving

- Input: polynomial system $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$
- Output: exact solution

Computing Gröbner bases

(Buchberger, F_4, F_5...)

1. Select a set of pairs of polynomials from a queue
2. Reduce these polynomials
3. Add the new polynomials to the basis, add new pairs to the queue
4. Repeat 1-3 until the queue is empty

Context

Polynomial System Solving

- Input: polynomial system $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$
- Output: exact solution

Computing Gröbner bases

(Buchberger, F_4, F_5...)

1. Select a set of pairs of polynomials from a queue
2. Reduce these polynomials
3. Add the new polynomials to the basis, add new pairs to the queue
4. Repeat 1-3 until the queue is empty

Importance of structure

- Systems from applications are not generic!
- Design dedicated strategies
- Complexity studies with generic properties

Examples of structures

- Homogeneous systems
- Multi-homogeneous systems (Dickenstein, Emiris, Faugère/Safey/Spaenlehauer...)
- Systems with group symmetries (Colin, Gattermann, Faugère/Rahmany, Faugère/Svartz...)
- Weighted homogeneous systems
- Sparse systems (Sturmfels, Faugère/Spaenlehauer/Svartz...)

Problem statement: an example (1)

Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)

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

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

Description of the system

- Ideal invariant under the group $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n$, rewritten with the invariants:
  $$\begin{cases} \tilde{e}_i := e_i(x_1^2, \ldots, x_n^2) \quad (1 \le i \le n-1) \\ e_n(x_1, \ldots, x_n) \end{cases}$$
- 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

- Normal strategy (total degree)
  $\to$ difficult
  $\to$ non regular
- Weighted degree strategy
  $\text{Weight}(\tilde{e}_i) = 2 \cdot \text{Weight}(e_i)$
  $\to$ easier
  $\to$ regular

Problem statement: an example (1)

Discrete Logarithm Problem on Edwards elliptic curves (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

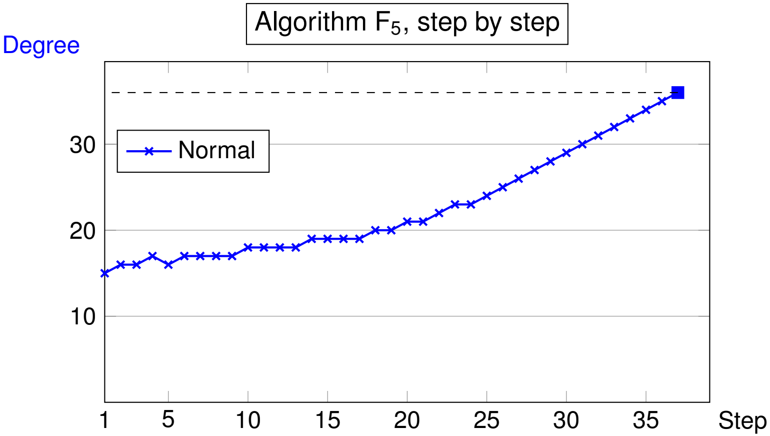
- Ideal invariant under the group $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n$,
  rewritten with the invariants:
  $$\begin{cases}\tilde{e}_i := e_i(x_1^2, \ldots, x_n^2) & (1 \le i \le n-1)\\ e_n(x_1, \ldots, x_n)\end{cases}$$
- n equations of degree 2^{n-1}
  in $\mathbb{F}_q[\tilde{e}_1,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

Goal: compute a Gröbner basis

- Normal strategy (total degree)
  $\rightarrow$ difficult
  $\rightarrow$ non regular
- Weighted degree strategy
  $\text{Weight}(\tilde{e}_i) = 2 \cdot \text{Weight}(e_i)$
  $\rightarrow$ easier
  $\rightarrow$ regular

Problem statement: an example (2)

Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)



- 5 equations of degree $(16, \ldots, 16)$ in 5 variables with $W = (2, \ldots, 2, 1)$
- 65 536 solutions
- Without weights: 2 h (37 steps)
- With weights: 15 min (29 steps)

Problem statement: an example (3)

Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)

$$
\begin{aligned}
0 = {} & \begin{bmatrix}7871\\18574\\14294\\32775\\20289\end{bmatrix} e_5^{16} + \begin{bmatrix}53362\\50900\\36407\\58813\\20802\end{bmatrix} \tilde{e}_1^{8} + \begin{bmatrix}26257\\128\\3037\\38424\\41456\end{bmatrix} \tilde{e}_1^{7}\tilde{e}_2 + \begin{bmatrix}25203\\23117\\28918\\29298\\56353\end{bmatrix} \tilde{e}_1^{6}\tilde{e}_2^{2} + \begin{bmatrix}19817\\29737\\52187\\36574\\46683\end{bmatrix} \tilde{e}_1^{5}\tilde{e}_2^{3} + \begin{bmatrix}9843\\3752\\27006\\64195\\63059\end{bmatrix} \tilde{e}_1^{4}\tilde{e}_2^{4} + \begin{bmatrix}11204\\25459\\58263\\17964\\57146\end{bmatrix} \tilde{e}_1^{3}\tilde{e}_2^{5} \\
& + \begin{bmatrix}46217\\5478\\45631\\13171\\42548\end{bmatrix} \tilde{e}_1^{2}\tilde{e}_2^{6} + \begin{bmatrix}63811\\50777\\48809\\1858\\55751\end{bmatrix} \tilde{e}_1\tilde{e}_2^{7} + \begin{bmatrix}40524\\6881\\1238\\8056\\54831\end{bmatrix} \tilde{e}_2^{8} + \begin{bmatrix}4522\\1728\\18652\\54885\\8241\end{bmatrix} \tilde{e}_1^{7}\tilde{e}_3 + \begin{bmatrix}27518\\32176\\31159\\28424\\5276\end{bmatrix} \tilde{e}_1^{6}\tilde{e}_2\tilde{e}_3 + \text{2067 smaller monomials}
\end{aligned}
$$

Description of the system

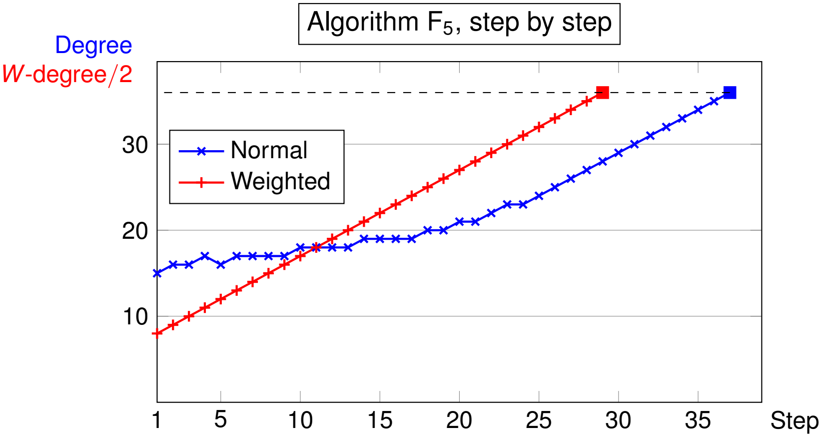
- Ideal invariant under the group $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n$, rewritten with the invariants:
  $$\begin{cases} \tilde{e}_i := e_i(x_1^2, \ldots, x_n^2) \quad (1 \leq i \leq n-1) \\ e_n(x_1, \ldots, x_n) \end{cases}$$
- n equations of degree 2^{n-1} in $\mathbb{F}_q[\tilde{e}_1,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

Goal: compute a Gröbner basis

- Normal strategy (total degree)
  $\rightarrow$ difficult
  $\rightarrow$ non regular
- Weighted degree strategy
  $\mathrm{Weight}(\tilde{e}_i) = 2 \cdot \mathrm{Weight}(e_i)$
  $\rightarrow$ easier
  $\rightarrow$ regular

Problem statement: an example (4)

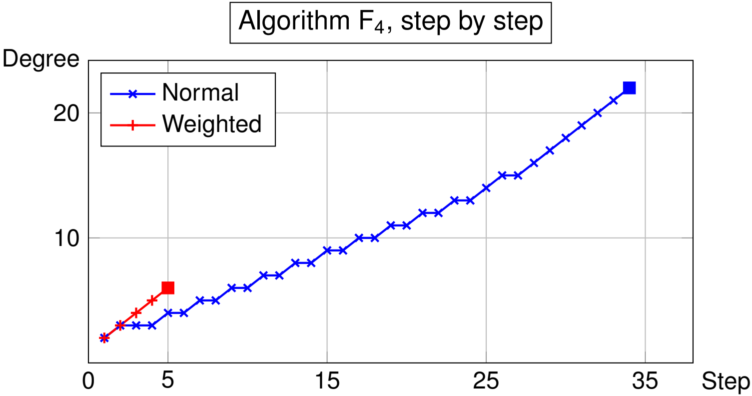
Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)



- 5 equations of degree $(16, \ldots, 16)$ in 5 variables with $W = (2, \ldots, 2, 1)$
- 65 536 solutions
- Without weights: 2 h (37 steps)
- With weights: 15 min (29 steps)

Problem statement: another example

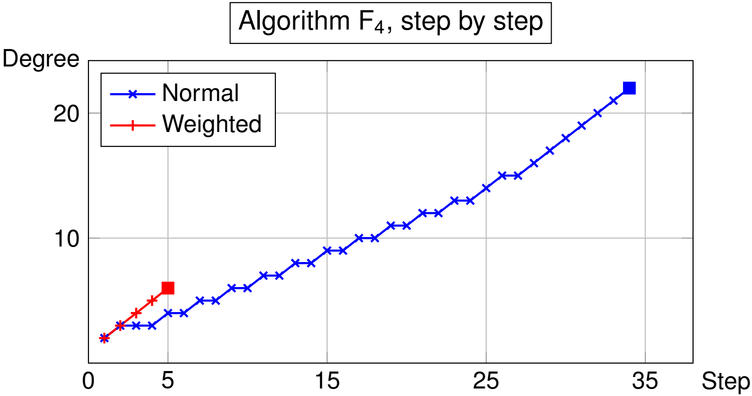
Ideal of relations between 50 monomials of degree 2 in 25 variables



- 50 equations of degree 2 in 75 variables
- GREVLEX ordering (e.g. for a 2-step strategy)
- Without weights: 3.9 h (34 steps reaching degree 22)
- With weights: 0.1 s (5 steps reaching degree 6)

Problem statement: another example

Ideal of relations between 50 monomials of degree 2 in 25 variables



Problem

- Strategy for this structure?
- Complexity bounds? Relevant generic properties?

Weighted homogeneous systems

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

Weighted homogeneous polynomial: poly. with monomials of same W-degree

Given a general (not weighted homogeneous) system and a system of weights

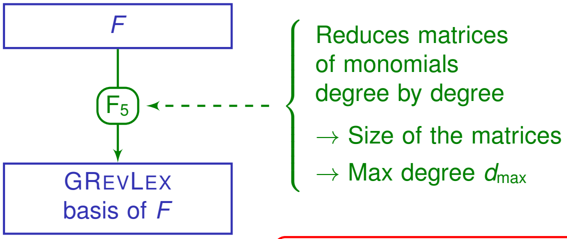
Computational strategy: weighted-homogenize it as in the homogeneous case

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

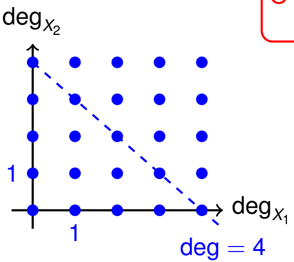
- Enough to study weighted homogeneous systems
- Notations: $(f_1, \dots, f_m)$, W-homo. with W-degree $(d_1, \dots, d_m)$

Strategy in the homogeneous case

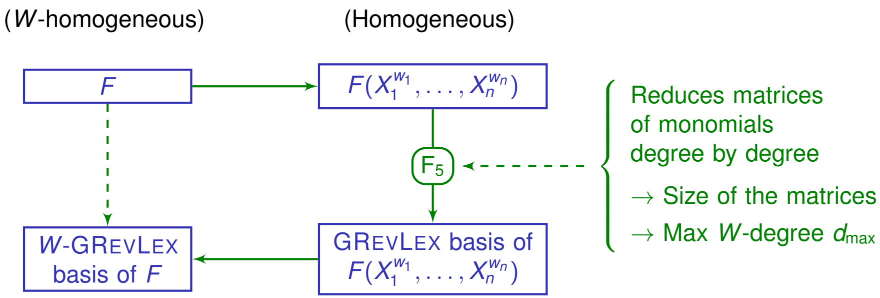
(Homogeneous)

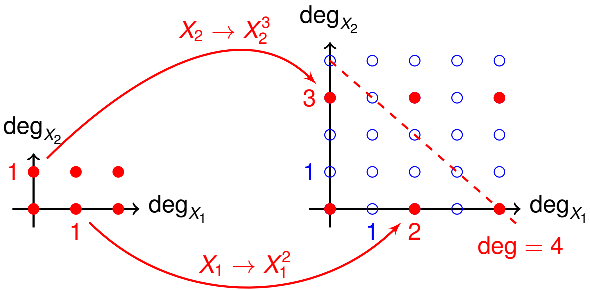


$$O\left(d_{max}\binom{n+d_{max}-1}{d_{max}}^{\omega}\right)$$

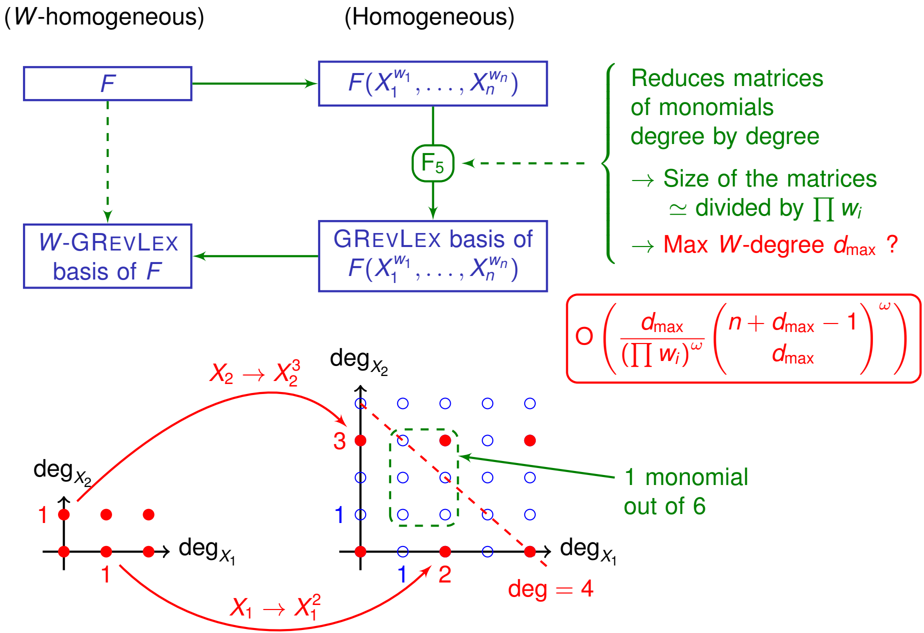


Strategy in the W-homogeneous case

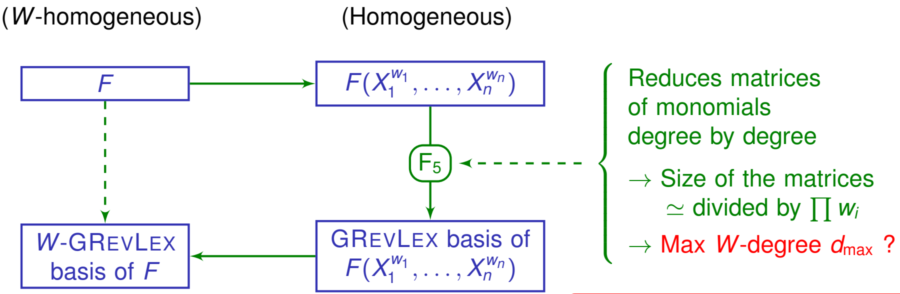




Strategy in the W-homogeneous case



Strategy in the W-homogeneous case



$$O\left(\frac{d_{\max}}{\left(\prod w_i\right)^{\omega}} \binom{n + d_{\max} - 1}{d_{\max}}^{\omega}\right)$$

Results from the homogeneous case ($m \leq n$) [Faugère, Safey, V. 2013]

- Generic properties: regular sequences ($m = n$), Noether position ($m < n$)
- Weighted Macaulay's bound: $d_{\max} \leq \sum_{i=1}^{m} d_i - \sum_{i=1}^{m} w_i + \max_{1 \leq j \leq m} \{w_j\}$

Main results

- The previous bound: $d_{\max} \leq \sum_{i=1}^{m} d_i - \sum_{i=1}^{m} w_i + \max_{1 \leq j \leq m} \{w_j\}$

The order of the variables matters: simultaneous Noether position ($m \leq n$)

- Better bound on $d_{\max}$: $d_{\max} \leq \sum_{i=1}^{m} d_i - \sum_{i=1}^{m} w_i + w_m$
- Algorithmic improvement: order the variables so that $w_m \leq w_j \quad \forall j$

The overdetermined case: semi-regular sequences

- Tricky definition in the weighted case
- With hypotheses, same characterization as in the homogeneous case
- Practical and theoretical gains

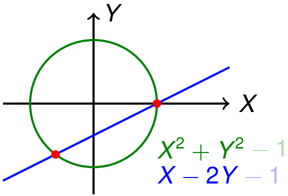
Regular sequences ($m \leq n$)

Definition

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

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

$(I_i := \langle f_1, \ldots, f_i \rangle)$



Properties

- Generic if not empty (for large classes of W-degrees and weights)
- Algorithmic benefit: F_5 criterion
- Hilbert Series:

$$\begin{aligned} \text{HS} &= \text{ generating series of the rank defects of the } F_5 \text{ matrices per } W\text{-deg} \\ &= \frac{\prod_{i=1}^{m}(1 - T^{d_i})}{\prod_{i=1}^{n}(1 - T^{w_i})} \end{aligned}$$

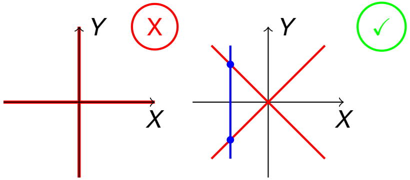
- Macaulay bound (if $m = n$): $d_{\max} \leq \sum_{i=1}^{n} d_i - \sum_{i=1}^{n} w_i + \max_{1 \leq j \leq n} \{w_j\}$

Noether position ($m < n$)

Definition

$F = (f_1, \ldots, f_m) \in \mathbb{K}[X_1, \ldots, X_n]$
is in Noether position iff
$(F, X_{m+1}, \ldots, X_n)$ is regular

"Regularity + selected variables"



Properties

- Generic if not empty
- True up to a generic change of coordinates if non-trivial changes exist
  (Ex: if $1 = w_n \mid w_{n-1} \mid \ldots \mid w_1$)
- Macaulay bound on $d_{\max}$: $d_{\max} \leq \sum_{i=1}^{m} d_i - \sum_{i=1}^{m} w_i + \max_{1 \leq j \leq m} \{w_j\}$
  (only the first m weights matter)

Simultaneous Noether position ($m \leq n$)

Noether position = information on what variables are important
$\Rightarrow$ Good property for W-homogeneous systems in general

Definition

$F = (f_1, \ldots, f_m) \in \mathbb{K}[X_1, \ldots, X_n]$
is in simultaneous Noether position iff
$(f_1, \ldots, f_j)$ is in Noether pos. for all j's

Properties

- $d_{\max} \leq \sum_{i=1}^{m} (d_i - w_i) + w_m$
- Better to have $w_m \leq w_j$ ($j \neq m$)

Simultaneous Noether position ($m \leq n$)

Noether position = information on what variables are important
$\Rightarrow$ Good property for W-homogeneous systems in general

Definition

$F = (f_1, \ldots, f_m) \in \mathbb{K}[X_1, \ldots, X_n]$
is in simultaneous Noether position iff
$(f_1, \ldots, f_j)$ is in Noether pos. for all j's

Properties

- $d_{\max} \leq \sum_{i=1}^{m} (d_i - w_i) + w_m$
- Better to have $w_m \leq w_j$ ($j \neq m$)

Order of the variables	w_m	$d_{\max}$	Macaulay's bound	New bound	F_5 time (s)
$X_1 > X_2 > X_3 > X_4$	1	210	229	210	101.9
$X_4 > X_3 > X_2 > X_1$	20	220	229	229	255.5

Generic W-homo. system, W-degree $(60, 60, 60, 60)$ w.r.t $W = (20, 5, 5, 1)$

Overdetermined case ($m > n$)

Equivalent definitions in the homogeneous case

$F = (f_1, \dots, f_m) \in \mathbb{K}[X_1, \dots, X_n]$ homogeneous is semi-regular

$\iff \forall\, k \in \{1, \dots, m\}, \forall\, d \in \mathbb{N}, (\,\cdot f_k) : (A/I_{k-1})_d \to (A/I_{k-1})_{d+d_k}$ is full-rank

$\iff \forall\, k \in \{1, \dots, m\}, \mathrm{HS}_{A/I_k} = \left\lfloor \frac{\prod_{i=1}^{k}(1 - T^{d_i})}{(1-T)^n} \right\rfloor_+$ (truncated at the first coef. ≤ 0)

But in the weighted case...

Ex: $n = 3$, $W = (3, 2, 1)$, $m = 8$, $D = (6, \dots, 6)$:

$$\left\lfloor \frac{\prod_{i=1}^{m}(1 - T^{d_i})}{\prod_{i=1}^{n}(1 - T^{w_i})} \right\rfloor_+ = 1 + T + 2T^2 + 3T^3 + 4T^4 + 5T^5 - T^6 + 0T^7 - 6T^8 + \cdots$$

$$\mathrm{HS}_{A/I} = 1 + T + 2T^2 + 3T^3 + 4T^4 + 5T^5 + 0T^6 + T^7$$

Overdetermined case ($m > n$)

Equivalent definitions in the weighted homogeneous case

Assume that $1 = w_n \mid w_{n-1} \mid \dots \mid w_1$.

$F = (f_1, \dots, f_m) \in \mathbb{K}[X_1, \dots, X_n]$ W-homogeneous is semi-regular

$\iff \forall\, k \in \{1, \dots, m\}, \forall\, d \in \mathbb{N}, (\,\cdot\, f_k) : (A/I_{k-1})_d \to (A/I_{k-1})_{d+d_k}$ is full-rank

$\iff \forall\, k \in \{1, \dots, m\}, \mathrm{HS}_{A/I_k} = \left\lfloor \frac{\prod_{i=1}^{k}(1 - T^{d_i})}{\prod_{i=1}^{n}(1 - T^{w_i})} \right\rfloor_+$ (truncated at the first coef. ≤ 0)

Properties

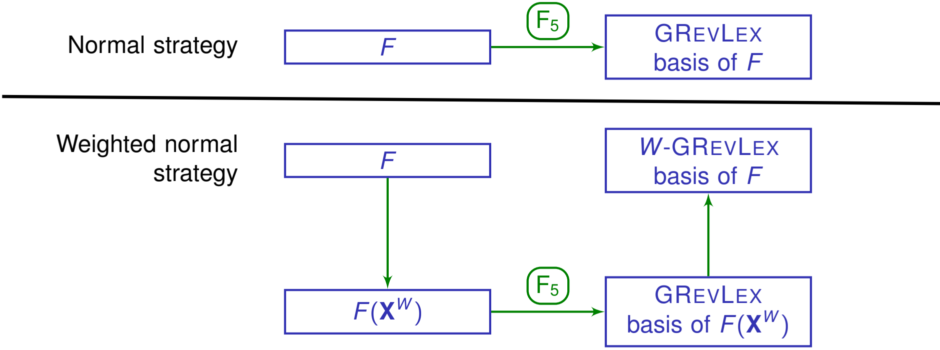
- Conjectured to be generic
  - Proved in some cases (ex: $m = n + 1$)
- Practical and theoretical gains
  - Asymptotic studies of $d_{\max}$

Experimental data

F : affine system with a weighted 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 generic



$$O\left(\frac{d_{\max}}{(\prod w_i)^{\omega}} \binom{n + d_{\max} - 1}{d_{\max}}^{\omega} \right)$$

Experimental results

System	Normal (s)	Weighted (s)	Speed-up
DLP Edwards $n = 5$, GREVLEX order (F_5, FGb)	6461.2	935.4	6.9
DLP Edwards $n = 5$, GREVLEX order (F_4, Magma)	56 195.0	6044.0	9.3
Invariant rels. Cyclic $n = 5$, GREVLEX order (F_4, Magma)	$> 75\,000$	392.7	> 191
Invariant rels. Cyclic $n = 5$, elimination order (F_4, Magma)	NA	382.5	NA
Monomial rels., $n = 26$, $m = 52$, GREVLEX order (F_4, Magma)	14 630.6	0.2	73 153
Monomial rels., $n = 26$, $m = 52$, elimination order (F_4, Magma)	17 599.5	8054.2	2.2

Conclusion and perspectives

What has been done

- Theoretical results for W-homogeneous systems under generic properties
- Complexity bounds for F_5 for a W-GREVLEX basis
  - Size of the matrices divided by $(\prod w_i)$
  - Bounds on the maximal degree reached by the F_5 algorithm
  - Bounds for 0-dim., positive-dim. and overdetermined systems
  - Indication on the best order for the variables
- Consequences:
  - Zero-dim: already successfully used on systems from the DLP
  - Positive-dim: applicable to polynomial inversion problems
  - Overdetermined: applicable to many problems (ex: cryptography)

Perspectives

- Some timings still not completely understood
- Affine systems: algorithm to find a good system of weights
- Additional structure: W-homo. for several systems of weights, weights $\leq 0\dots$

Conclusion and perspectives

What has been done

- Theoretical results for W-homogeneous systems under generic properties
- Complexity bounds for F_5 for a W-GREVLEX basis
  - Size of the matrices divided by $(\prod w_i)$
  - Bounds on the maximal degree reached by the F_5 algorithm
  - Bounds for 0-dim., positive-dim. and overdetermined systems
  - Indication on the best order for the variables
- Consequences:
  - Zero-dim: already successfully used on systems from the DLP
  - Positive-dim: applicable to polynomial inversion problems
  - Overdetermined: applicable to many problems (ex: cryptography)

Perspectives

- Some timings still not completely understood
- Affine systems: algorithm to find a good system of weights
- Additional structure: W-homo. for several systems of weights, weights $\leq 0\ldots$

One last word

Thank you for your attention!