On The Complexity Of Computing Gröbner Bases For Weighted Homogeneous Systems

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

Thibaut Verron[2]

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

[2] Toulouse Universités, INP-ENSEEIHT-IRIT, CNRS, Équipe APO

Séminaire *Géométrie et Algèbre Effectives*,
2 juin 2017

Polynomial system solving

Applications:
- Cryptography
- Physics, industry
- Mathematics...

Polynomial equations

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

Solutions,
e.g. find all the solutions
if finite (dimension 0)

- Numerical: give approximations of the solutions
  - Newton's method
  - Homotopy continuation method
- Symbolic: give exact solutions
  - Gröbner bases
  - Resultant method
  - Triangular sets
  - Geometric resolution

Computing Gröbner bases for generic systems: the normal strategy

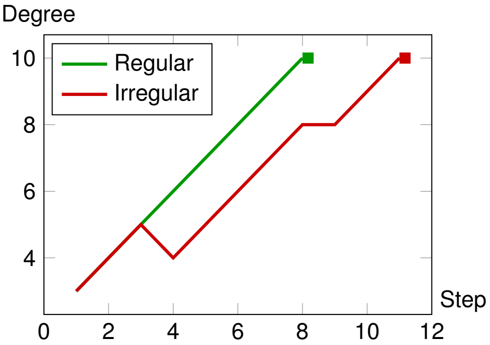
Gröbner basis algorithms (e.g. F_5)

- Compute a basis by iteratively building and reducing matrices of polynomials of same degree
- Normal strategy: perform lowest-degree reductions first
- Degree = indicator of progress

Computing Gröbner bases for generic systems: the normal strategy

Gröbner basis algorithms (e.g. F_5)

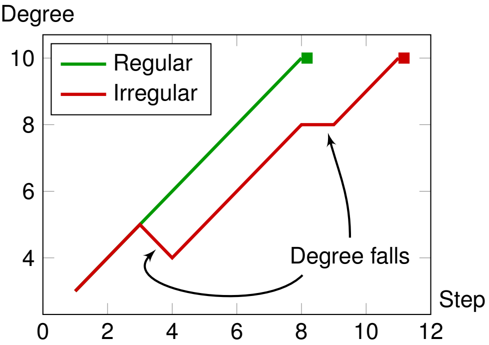
- Compute a basis by iteratively building and reducing matrices of polynomials of same degree
- Normal strategy: perform lowest-degree reductions first
- Degree = indicator of progress



Computing Gröbner bases for generic systems: the normal strategy

Gröbner basis algorithms (e.g. F_5)

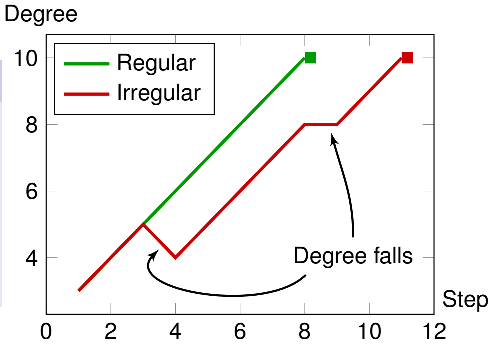
- Compute a basis by iteratively building and reducing matrices of polynomials of same degree
- Normal strategy: perform lowest-degree reductions first
- Degree = indicator of progress



Degree fall?

- Definition: reduction resulting in a lower degree polynomial
- Example: $X \cdot (Y-1) - Y \cdot (X-1) = XY - YX + Y - X$
- Consequence: "next d" $< d+1$

Computing Gröbner bases for generic systems: the normal strategy



Gröbner basis algorithms (e.g. F_5)

- Compute a basis by iteratively building and reducing matrices of polynomials of same degree
- Normal strategy: perform lowest-degree reductions first
- Degree = indicator of progress

Regular sequences $\implies$ algorithmic regularity!

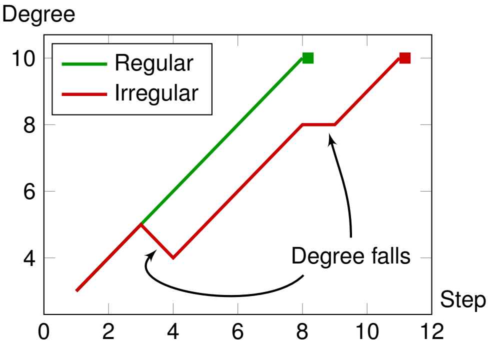
- F_5-criterion: no reduction to zero in F_5 ($\iff$ all matrices have full-rank) for regular sequences
- Degree falls $\iff$ Reduction to zero of the highest degree components

$\rightsquigarrow$ Regularity in the affine sense = regularity of the highest degree components

Computing Gröbner bases for generic systems: the normal strategy

Gröbner basis algorithms (e.g. F_5)

- Compute a basis by iteratively building and reducing matrices of polynomials of same degree
- Normal strategy: perform lowest-degree reductions first
- Degree = indicator of progress



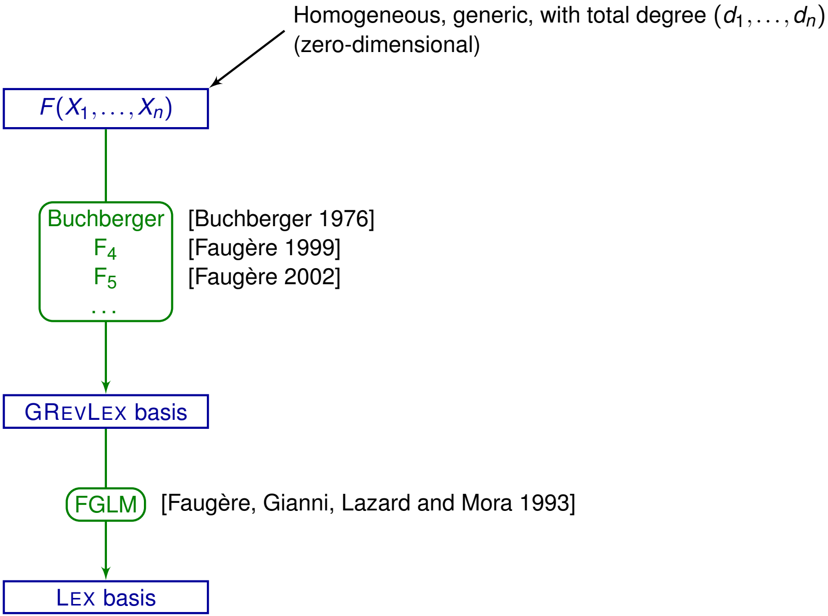
Regular sequences $\Longrightarrow$ algorithmic regularity!

- F_5-criterion: no reduction to zero in F_5 ($\Longleftrightarrow$ all matrices have full-rank) for regular sequences
- Degree falls $\Longleftrightarrow$ Reduction to zero of the highest degree components

$\rightsquigarrow$ Regularity in the affine sense = regularity of the highest degree components

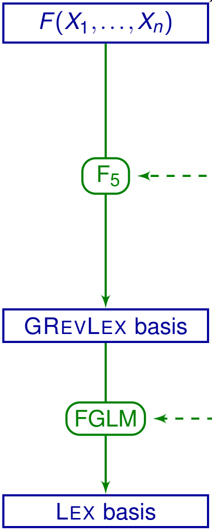
This notion depends on the homogeneous structure!

Strategy and complexity for generic homogeneous systems



Strategy and complexity for generic homogeneous systems

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



Highest degree $\sim$ # of reduction steps

$$= d_{\text{reg}} \leq \sum_{i=1}^{n} (d_i - 1) + 1$$

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

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

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

The weighted homogeneous structure: an example (1)

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

$$0 = \begin{bmatrix}41518\\33900\\8840\\22855\\29081\end{bmatrix} X_5^{16} + \begin{bmatrix}49874\\32136\\34252\\24932\\11782\end{bmatrix} X_1^{8} + \begin{bmatrix}45709\\10698\\45336\\26076\\55993\end{bmatrix} X_1^{7}X_2 + \begin{bmatrix}46659\\59796\\38267\\39647\\27683\end{bmatrix} X_1^{6}X_2^{2} + \begin{bmatrix}32367\\23164\\64111\\63692\\29095\end{bmatrix} X_1^{5}X_2^{3} + \begin{bmatrix}37627\\25182\\59951\\60422\\11080\end{bmatrix} X_1^{4}X_2^{4} +$$

$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^{3}X_2^{5} + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^{2}X_2^{6} + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1X_2^{7} + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^{8} + \begin{bmatrix}17060\\60912\\64907\\61073\\37208\end{bmatrix} X_1^{7}X_3 + \begin{bmatrix}55016\\15550\\19633\\28147\\25442\end{bmatrix} X_1^{6}X_2X_3 +$$

$$\begin{bmatrix}31264\\26817\\35757\\43106\\44133\end{bmatrix} X_1^{5}X_2^{2}X_3 + \begin{bmatrix}38258\\44188\\46688\\55434\\64632\end{bmatrix} X_1^{4}X_2^{3}X_3 + \begin{bmatrix}19475\\52270\\9282\\51171\\17150\end{bmatrix} X_1^{3}X_2^{4}X_3 + \begin{bmatrix}4467\\31828\\34222\\30753\\37662\end{bmatrix} X_1^{2}X_2^{5}X_3 + \text{2063 smaller monomials}$$

The weighted homogeneous structure: an example (1)

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

$$0 = \begin{bmatrix}41518\\33900\\8840\\22855\\29081\end{bmatrix} X_5^{16} + \begin{bmatrix}49874\\32136\\34252\\24932\\11782\end{bmatrix} X_1^8 + \begin{bmatrix}45709\\10698\\45336\\26076\\55993\end{bmatrix} X_1^7 X_2 + \begin{bmatrix}46659\\59796\\38267\\39647\\27683\end{bmatrix} X_1^6 X_2^2 + \begin{bmatrix}32367\\23164\\64111\\63692\\29095\end{bmatrix} X_1^5 X_2^3 + \begin{bmatrix}37627\\25182\\59951\\60422\\11080\end{bmatrix} X_1^4 X_2^4 +$$

$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^3 X_2^5 + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^2 X_2^6 + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1 X_2^7 + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^8 + \begin{bmatrix}17060\\60912\\64907\\61073\\37208\end{bmatrix} X_1^7 X_3 + \begin{bmatrix}55016\\15550\\19633\\28147\\25442\end{bmatrix} X_1^6 X_2 X_3 +$$

$$\begin{bmatrix}31264\\26817\\35757\\43106\\44133\end{bmatrix} X_1^5 X_2^2 X_3 + \begin{bmatrix}38258\\44188\\46688\\55434\\64632\end{bmatrix} X_1^4 X_2^3 X_3 + \begin{bmatrix}19475\\52270\\9282\\51171\\17150\end{bmatrix} X_1^3 X_2^4 X_3 + \begin{bmatrix}4467\\31828\\34222\\30753\\37662\end{bmatrix} X_1^2 X_2^5 X_3 + \text{2063 smaller monomials}$$

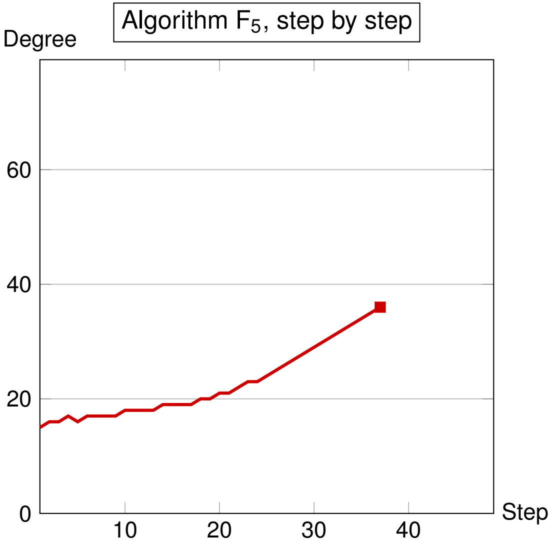
Goal: compute a Gröbner basis

Normal strategy (total degree):

- Non generic
- Non regular in the affine sense
- Non regular computation

The weighted homogeneous structure: an example (2)

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



- Without weights:
  2 h (37 steps, $d_{reg} = 36$)
- With $W = (2, 2, 1, 1, 1)$:
  2 h (46 steps, $d_{reg} = 38$)
- With $W = (2, 2, 2, 2, 1)$:
  15 min (29 steps, $d_{reg} = 72$)

The weighted homogeneous structure: an example (3)

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

$$0 = \begin{bmatrix}41518\\33900\\8840\\22855\\29081\end{bmatrix} X_5^{16} + \begin{bmatrix}49874\\32136\\34252\\24932\\11782\end{bmatrix} X_1^8 + \begin{bmatrix}45709\\10698\\45336\\26076\\55993\end{bmatrix} X_1^7 X_2 + \begin{bmatrix}46659\\59796\\38267\\39647\\27683\end{bmatrix} X_1^6 X_2^2 + \begin{bmatrix}32367\\23164\\64111\\63692\\29095\end{bmatrix} X_1^5 X_2^3 + \begin{bmatrix}37627\\25182\\59951\\60422\\11080\end{bmatrix} X_1^4 X_2^4 +$$

$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^3 X_2^5 + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^2 X_2^6 + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1 X_2^7 + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^8 + \begin{bmatrix}17060\\60912\\64907\\61073\\37208\end{bmatrix} X_1^7 X_3 + \begin{bmatrix}55016\\15550\\19633\\28147\\25442\end{bmatrix} X_1^6 X_2 X_3 +$$

$$\begin{bmatrix}31264\\26817\\35757\\43106\\44133\end{bmatrix} X_1^5 X_2^2 X_3 + \begin{bmatrix}38258\\44188\\46688\\55434\\64632\end{bmatrix} X_1^4 X_2^3 X_3 + \begin{bmatrix}19475\\52270\\9282\\51171\\17150\end{bmatrix} X_1^3 X_2^4 X_3 + \begin{bmatrix}4467\\31828\\34222\\30753\\37662\end{bmatrix} X_1^2 X_2^5 X_3 + \text{2063 smaller monomials}$$

Goal: compute a Gröbner basis

Normal strategy (total degree):

- Non generic
- Non regular in the affine sense
- Non regular computation

Alt. strategy: use weights

$=$ substitute $X_i \leftarrow X_i^{w_i}$ for $W = (w_1, \ldots, w_5)$

What weights?

- $W = (1,1,1,1,1)$: nothing changed
- $W = (2,2,1,1,1)$: better...
- $W = (2,2,2,2,1)$: regular!

The weighted homogeneous structure: an example (3)

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

$$0 = \begin{bmatrix}41518\\33900\\8840\\22855\\29081\end{bmatrix} X_5^{16} + \begin{bmatrix}49874\\32136\\34252\\24932\\11782\end{bmatrix} X_1^{8} + \begin{bmatrix}45709\\10698\\45336\\26076\\55993\end{bmatrix} X_1^{7}X_2 + \begin{bmatrix}46659\\59796\\38267\\39647\\27683\end{bmatrix} X_1^{6}X_2^{2} + \begin{bmatrix}32367\\23164\\64111\\63692\\29095\end{bmatrix} X_1^{5}X_2^{3} + \begin{bmatrix}37627\\25182\\59951\\60422\\11080\end{bmatrix} X_1^{4}X_2^{4} +$$

$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^{3}X_2^{5} + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^{2}X_2^{6} + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1X_2^{7} + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^{8} + \begin{bmatrix}17060\\60912\\64907\\61073\\37208\end{bmatrix} X_1^{7}X_3 + \begin{bmatrix}55016\\15550\\19633\\28147\\25442\end{bmatrix} X_1^{6}X_2X_3 +$$

$$\begin{bmatrix}31264\\26817\\35757\\43106\\44133\end{bmatrix} X_1^{5}X_2^{2}X_3 + \begin{bmatrix}38258\\44188\\46688\\55434\\64632\end{bmatrix} X_1^{4}X_2^{3}X_3 + \begin{bmatrix}19475\\52270\\9282\\51171\\17150\end{bmatrix} X_1^{3}X_2^{4}X_3 + \begin{bmatrix}4467\\31828\\34222\\30753\\37662\end{bmatrix} X_1^{2}X_2^{5}X_3 + \text{2063 smaller monomials}$$

Goal: compute a Gröbner basis

Normal strategy (total degree):

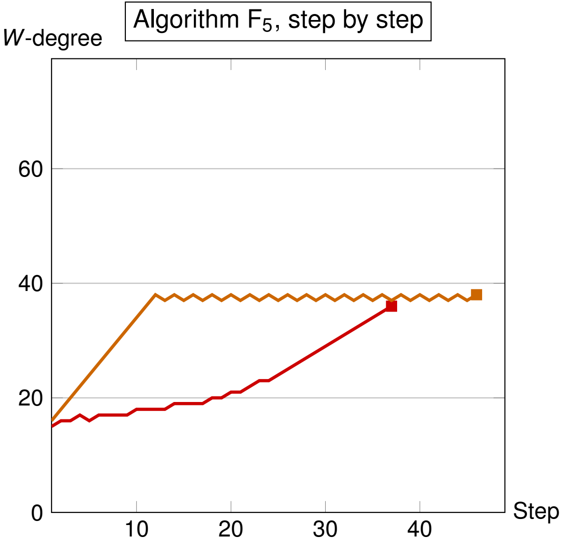
- Non generic
- Non regular in the affine sense
- Non regular computation

Alt. strategy: use weights

$=$ substitute $X_i \leftarrow X_i^{w_i}$ for $W = (w_1, \ldots, w_5)$

What weights?

- $W = (1,1,1,1,1)$: nothing changed
- $W = (2,2,1,1,1)$: better...
- $W = (2,2,2,2,1)$: regular!



- With $W = (1,1,1,1,1)$: 2 h (37 steps, $d_{reg} = 36$)
- With $W = (2,2,1,1,1)$: 2 h (46 steps, $d_{reg} = 38$)
- With $W = (2,2,2,2,1)$: 15 min (29 steps, $d_{reg} = 72$)

The weighted homogeneous structure: an example (5)

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

$$0 = \begin{bmatrix}41518\\33900\\8840\\22855\\29081\end{bmatrix} X_5^{16} + \begin{bmatrix}49874\\32136\\34252\\24932\\11782\end{bmatrix} X_1^{8} + \begin{bmatrix}45709\\10698\\45336\\26076\\55993\end{bmatrix} X_1^{7}X_2 + \begin{bmatrix}46659\\59796\\38267\\39647\\27683\end{bmatrix} X_1^{6}X_2^{2} + \begin{bmatrix}32367\\23164\\64111\\63692\\29095\end{bmatrix} X_1^{5}X_2^{3} + \begin{bmatrix}37627\\25182\\59951\\60422\\11080\end{bmatrix} X_1^{4}X_2^{4} +$$

$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^{3}X_2^{5} + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^{2}X_2^{6} + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1X_2^{7} + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^{8} + \begin{bmatrix}17060\\60912\\64907\\61073\\37208\end{bmatrix} X_1^{7}X_3 + \begin{bmatrix}55016\\15550\\19633\\28147\\25442\end{bmatrix} X_1^{6}X_2X_3 +$$

$$\begin{bmatrix}31264\\26817\\35757\\43106\\44133\end{bmatrix} X_1^{5}X_2^{2}X_3 + \begin{bmatrix}38258\\44188\\46688\\55434\\64632\end{bmatrix} X_1^{4}X_2^{3}X_3 + \begin{bmatrix}19475\\52270\\9282\\51171\\17150\end{bmatrix} X_1^{3}X_2^{4}X_3 + \begin{bmatrix}4467\\31828\\34222\\30753\\37662\end{bmatrix} X_1^{2}X_2^{5}X_3 + \text{2063 smaller monomials}$$

Goal: compute a Gröbner basis

Normal strategy (total degree):

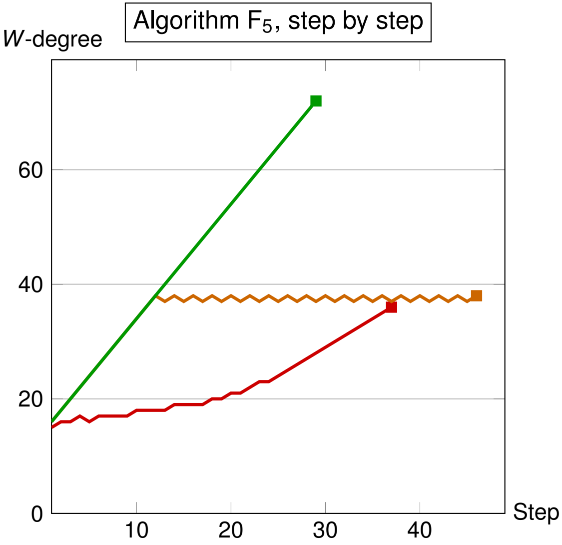
- Non generic
- Non regular in the affine sense
- Non regular computation

Alt. strategy: use weights

$=$ substitute $X_i \leftarrow X_i^{w_i}$ for $W = (w_1, \ldots, w_5)$

What weights?

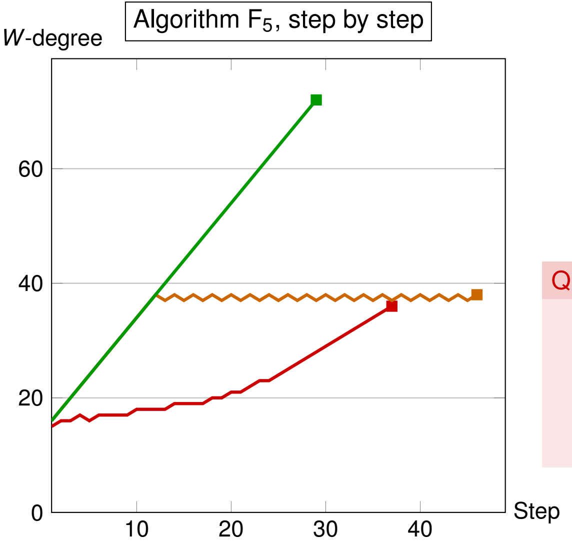
- $W = (1,1,1,1,1)$: nothing changed
- $W = (2,2,1,1,1)$: better...
- $W = (2,2,2,2,1)$: regular!



- With $W = (1,1,1,1,1)$: 2 h (37 steps, $d_{\text{reg}} = 36$)
- With $W = (2,2,1,1,1)$: 2 h (46 steps, $d_{\text{reg}} = 38$)
- With $W = (2,2,2,2,1)$: 15 min (29 steps, $d_{\text{reg}} = 72$)

The weighted homogeneous structure: an example (6)

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



- With $W = (1,1,1,1,1)$:
  2 h (37 steps, $d_{\text{reg}} = 36$)
- With $W = (2,2,1,1,1)$:
  2 h (46 steps, $d_{\text{reg}} = 38$)
- With $W = (2,2,2,2,1)$:
  15 min (29 steps, $d_{\text{reg}} = 72$)

Questions

- Explain the regularity?
- Complexity bounds?
- Why does FGLM become a bottleneck?

Weighted homogeneous systems: definitions

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

Weighted 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-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

Weighted homogeneous systems: definitions

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. containing only monomials of same W-degree

→ Example: physical systems: Volume = Area × Height

Weight 3 Weight 2 Weight 1

Given a general (non-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

Main results: strategy and complexity results

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

$F(X_1, \ldots, X_n), W$ ← W-Homogeneous, generic, with W-degree $(d_1, \ldots, d_n)$ (zero-dimensional)

↓

$F(X_1^{w_1}, \ldots, X_n^{w_n})$ ← Homogeneous, with total degree $(d_1, \ldots, d_n)$

↓

F$_5$ ← Highest W-degree

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

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

↓

W-GRevLex basis of F

↓

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

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

↓

Lex basis

Roadmap

Input

- $W = (w_1, \dots, w_n)$ system of weights
- $F = (f_1, \dots, f_m)$ generic sequence of W-homogeneous polynomials with W-degree $(d_1, \dots, d_m)$

General roadmap:

1. Find a generic property with "good" algorithmic and algebraic consequences
   - Regular sequences (dimension 0, $m = n$)
   - Noether position (positive dimension, $m \leq n$)
   - ...Semi-regular sequences (dimension 0, $m > n$)
2. Design new algorithms to take advantage of this structure
   - Adapt algorithms for the homogeneous case to the weighted homogeneous case
3. Obtain complexity results for these algorithms

Roadmap

Input

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

General roadmap:

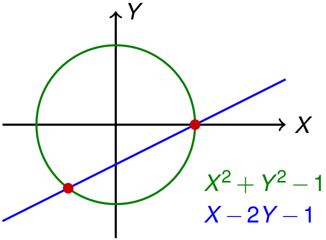
1. Find a generic property with "good" algorithmic and algebraic consequences
   - Regular sequences (dimension 0, $m = n$)
   - Noether position (positive dimension, $m \leq n$)
   - ...Semi-regular sequences (dimension 0, $m > n$)
2. Design new algorithms to take advantage of this structure
   - Adapt algorithms for the homogeneous case to the weighted homogeneous case
3. Obtain complexity results for these algorithms

Regular sequences

Definition

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

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

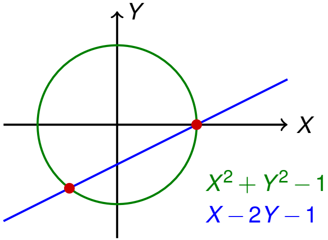


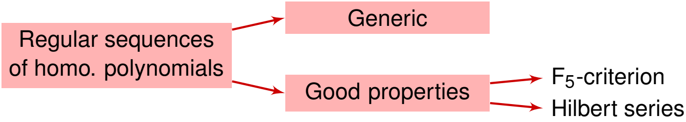
Regular sequences

Definition

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

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

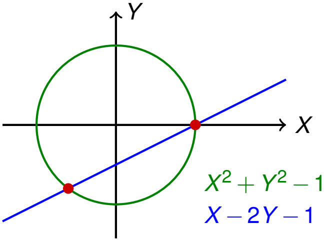




Definition

$F = (f_1, \ldots, f_m)$ weighted 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 W-homo. polynomials → Generic if $\neq \varnothing$

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

Properties of regular sequences

Hilbert series

$$\mathrm{HS}_{A/I}(T) = \sum_{d=0}^{\infty} (\text{rank defect of the } \mathrm{F}_5 \text{ matrix at degree } d) \cdot T^d$$

Properties

For regular sequences of homogeneous polynomials of degree d_i:

$$\mathrm{HS}_{A/I}(T) = \frac{(1-T^{d_1})\cdots(1-T^{d_m})}{(1-T)^n}$$

In zero dimension ($m = n$):

- Bézout bound on the degree: $D = \prod_{i=1}^{n} d_i$
- Macaulay bound on the degree of regularity: $d_{\mathrm{reg}} \leq \sum_{i=1}^{n} (d_i - 1) + 1$

Properties of regular sequences

Hilbert series

$$\mathrm{HS}_{A/I}(T) = \sum_{d=0}^{\infty} (\text{rank defect of the } \mathrm{F}_5 \text{ matrix at } W\text{-degree } d) \cdot T^d$$

Properties

For regular sequences of W-homogeneous polynomials of W-degree d_i:

$$\mathrm{HS}_{A/I}(T) = \frac{(1-T^{d_1})\cdots(1-T^{d_m})}{(1-T^{w_1})\cdots(1-T^{w_n})}$$

In zero dimension ($m = n$):

- Bézout bound on the degree: $D = \frac{\prod_{i=1}^{n} d_i}{\prod_{i=1}^{n} w_i}$
- Macaulay bound on the degree of regularity: $d_{\mathrm{reg}} \leq \sum_{i=1}^{n} (d_i - w_i) + \max\{w_j\}$

Limitations

Limitations of the regularity

- $m < n$ (positive dimension): no real information
- $m = n$ (zero dimension, complete intersection)
  - exact formula for d_{reg}?
  - d_{reg} depends on the order of the variables
  - Hilbert series: independent from that order
- $m > n$ (e.g. cryptography): no regular sequence

$\Longrightarrow$ Additional properties

- $m < n$: Noether position
- $m = n$: simultaneous Noether position
- $m > n$: semi-regular sequences

Noether position ($m < n$)

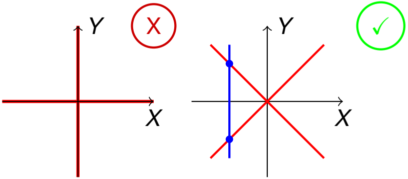
Definition

$F = (f_1, \ldots, f_m) \in \mathbb{K}[X_1, \ldots, X_n]$

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

  (E.g. if $1 = w_n \mid w_{n-1} \mid \ldots \mid w_1$)
- Macaulay bound on d_{reg}: $d_{\mathrm{reg}} \leq \sum_{i=1}^{m} d_i - \sum_{i=1}^{m} w_i + \max_{1 \leq j \leq m} \{w_j\}$

  (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

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

Properties

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

Order of the variables	w_m	d_{reg}	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)

Properties

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

Overdetermined case ($m > n$)

Equivalent definitions in the weighted homogeneous case?

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

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

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

Properties

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

No equivalence without hypotheses on the weights

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

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

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

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 (Fröberg)
- Proved in some cases (ex: $m = n+1$)
- Practical and theoretical gains
- Asymptotic studies of d_{reg}

No equivalence without hypotheses on the weights

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

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

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

Roadmap

Input

- $W = (w_1, \dots, w_n)$ system of weights
- $F = (f_1, \dots, f_m)$ generic sequence of W-homogeneous polynomials with W-degree $(d_1, \dots, d_m)$

General roadmap:

1. Find a generic property with “good” algorithmic and algebraic consequences
   - Regular sequences (dimension 0, $m = n$)
   - Noether position (positive dimension, $m \leq n$)
   - ... Semi-regular sequences (dimension 0, $m > n$)
2. Design new algorithms to take advantage of this structure
   - Adapt algorithms for the homogeneous case to the weighted homogeneous case
3. Obtain complexity results for these algorithms

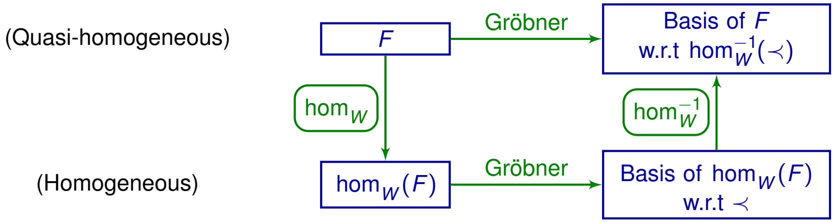
Algorithms: from weighted homogeneous to homogeneous

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
- $\text{S-Pol}(\hom_W(f), \hom_W(g)) = \hom_W(\text{S-Pol}(f, g))$

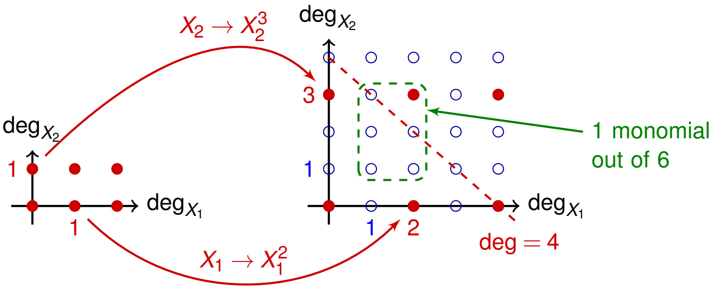
$\longrightarrow$ Good behavior w.r.t Gröbner bases



Size of the Macaulay matrices

Counting the monomials

- $\hom_W(F)$ lies in an algebra with a lot of useless monomials
- Count them: combinatorial object named Sylvester denumerants
- Result[1]: asymptotically $N_d \sim \dfrac{\#\text{Monomials of total degree } d}{\prod_{i=1}^n w_i}$

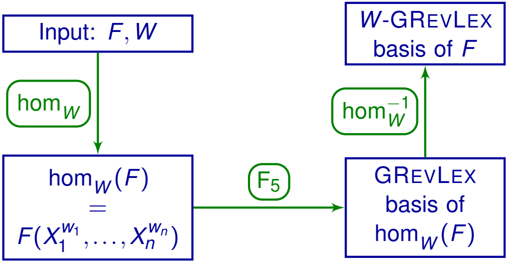


[1] Geir Agnarsson (2002). 'On the Sylvester denumerants for general restricted partitions'

Adapting the algorithms

Detailed strategy

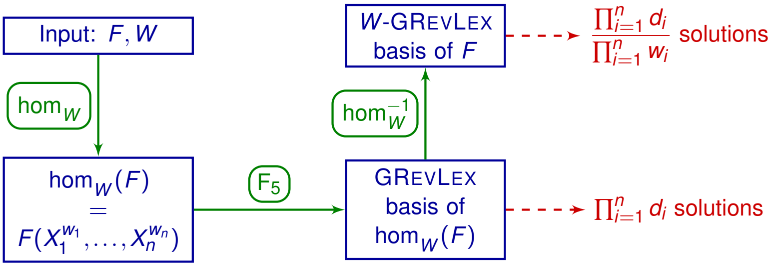
- F_5 algorithm on the homogenized system
- FGLM algorithm on the weighted homogeneous system



Adapting the algorithms

Detailed strategy

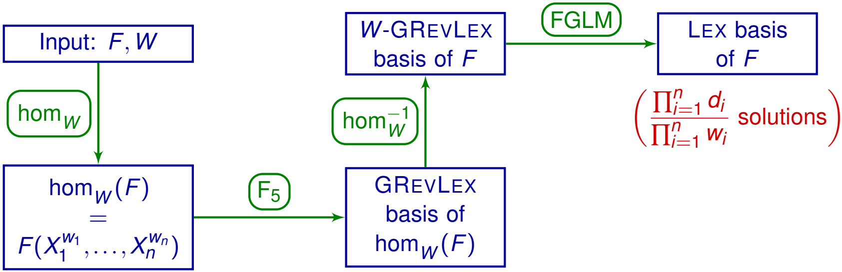
- F_5 algorithm on the homogenized system
- FGLM algorithm on the weighted homogeneous system



Adapting the algorithms

Detailed strategy

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



Roadmap

Input

- $W = (w_1, \dots, w_n)$ system of weights
- $F = (f_1, \dots, f_m)$ generic sequence of W-homogeneous polynomials with W-degree $(d_1, \dots, d_m)$

General roadmap:

1. Find a generic property with "good" algorithmic and algebraic consequences
   - Regular sequences (dimension 0, $m = n$)
   - Noether position (positive dimension, $m \leq n$)
   - ...Semi-regular sequences (dimension 0, $m > n$)
2. Design new algorithms to take advantage of this structure
   - Adapt algorithms for the homogeneous case to the weighted homogeneous case
3. Obtain complexity results for these algorithms

Complexity

Input

- $W = (w_1, \dots, w_n)$
- $F = (f_1, \dots, f_n) \in \mathbb{K}[X_1, \dots, X_n]$ generic W-homogeneous

Complexity of F_5

$$\left(\frac{1}{\prod_{i=1}^n w_i}\right)^3 \binom{n + d_{\mathrm{reg}} - 1}{d_{\mathrm{reg}}}^3$$

- Asymptotic gain from the size of the matrices
- Practical gain from the weighted Macaulay bound (d_{reg})

Complexity of FGLM

$$\left(\frac{1}{\prod_{i=1}^n w_i}\right)^3 n \left(\prod_{i=1}^n d_i\right)^3$$

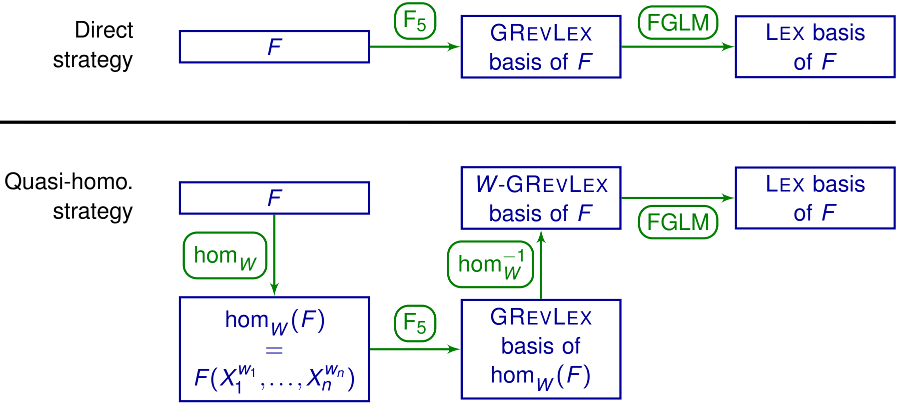
- Asymptotic gain from the weighted Bézout bound (number of solutions)

Benchmarking

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 regular (e.g. if F is generic)

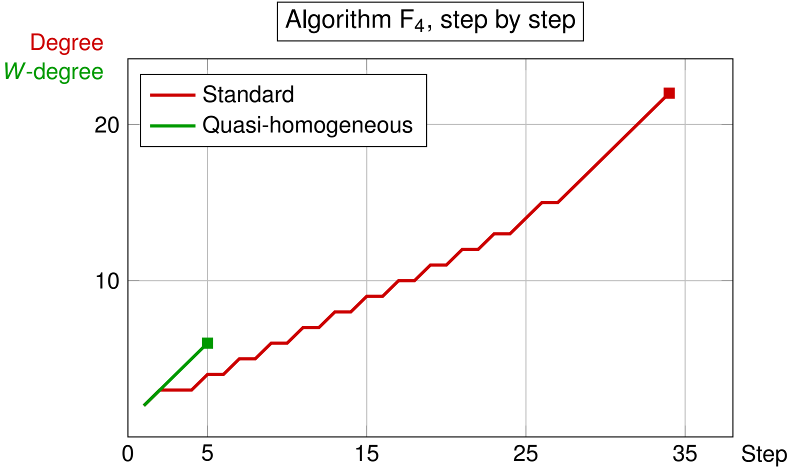


Experimental results

System	Normal (s)	Weighted (s)	Speed-up
DLP Edwards $n=5$, GREVLEX (F_5, FGb)	6461.2	935.4	6.9
DLP Edwards $n=5$, GREVLEX (F_4, Magma)	56195.0	6044.0	9.3
Invariant relations, Cyclic $n=5$, GREVLEX (F_4, Magma)	>75000	392.7	>191
Monomial relations, $n=26$, $m=52$, GREVLEX (F_4, Magma)	14630.6	0.2	73153
DLP Edwards $n=5$, LEX (Sparse-FGLM, FGb)	6835.6	2164.4	3.2
Invariant relations, Cyclic $n=5$, ELIM (F_4, Magma)	NA	382.5	NA
Monomial relations, $n=26$, $m=52$, ELIM (F_4, Magma)	17599.5	8054.2	2.2

A run of F_4 on an inversion example

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



- 50 equations of (W-)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 W-degree 6)

Conclusion

What we have done

- Theoretical results for weighted homogeneous systems under generic assumptions
- Computational strategy for weighted 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

- Affine systems: find the most appropriate system of weights
- Additional structure: weighted homo. for several systems of weights, weights ≤ 0...

Conclusion

What we have done

- Theoretical results for weighted homogeneous systems under generic assumptions
- Computational strategy for weighted 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

- Affine systems: find the most appropriate system of weights
- Additional structure: weighted homo. for several systems of weights, weights ≤ 0...

Thank you for your attention!