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

March 22, 2013

Motivations

Polynomial system

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

→ Gröbner basis →

Parametrization of the solutions

$$\mathbf{q}(\mathbf{T}) = 0$$
$$\mathbf{X} = \mathbf{p}(\mathbf{T})$$

Applications:

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

Difficult problem

- NP-hard in finite field
- Exponential number of solutions

Problem:
Exploit the structures of the system

Examples of successfully studied structures:

- Homogeneous
- Bihomogeneous: [**FSS10b**]
- Group symmetries: e.g [**FS12**]
- Quasi-homogeneous

Motivations

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

Gröbner basis

Parametrization of the solutions
$$\mathbf{q}(\mathbf{T}) = 0$$
$$\mathbf{X} = \mathbf{p}(\mathbf{T})$$

Row-echelon form of the Macaulay matrix

$$\begin{pmatrix} \vdots \\ m_i F_j \\ \vdots \end{pmatrix}$$

Applications:

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

Difficult problem

- NP-hard in finite field
- Exponential number of solutions

Problem:
Exploit the structures of the system

Examples of successfully studied structures:

- Homogeneous
- Bihomogeneous: [**FSS10b**]
- Group symmetries: e.g [**FS12**]
- Quasi-homogeneous

Motivations

Polynomial system

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

Gröbner basis

Parametrization of the solutions

$$\mathbf{q}(\mathbf{T}) = 0$$
$$\mathbf{X} = \mathbf{p}(\mathbf{T})$$

Row-echelon form of the Macaulay matrix

$$\begin{pmatrix} \vdots \\ m_i F_j \\ \vdots \end{pmatrix}$$

Applications:

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

Difficult problem

- NP-hard in finite field
- Exponential number of solutions

Problem:
Exploit the structures of the system

Examples of successfully studied structures:

- Homogeneous
- Bihomogeneous: [**FSS10b**]
- Group symmetries: e.g [**FS12**]
- Quasi-homogeneous

Polynomial system

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

Gröbner basis

Parametrization of the solutions

$$\mathbf{q}(\mathbf{T}) = 0$$
$$\mathbf{X} = \mathbf{p}(\mathbf{T})$$

Applications:

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

Row-echelon form of the Macaulay matrix

$$\begin{pmatrix} \vdots \\ m_i F_j \\ \vdots \end{pmatrix}$$

Difficult problem

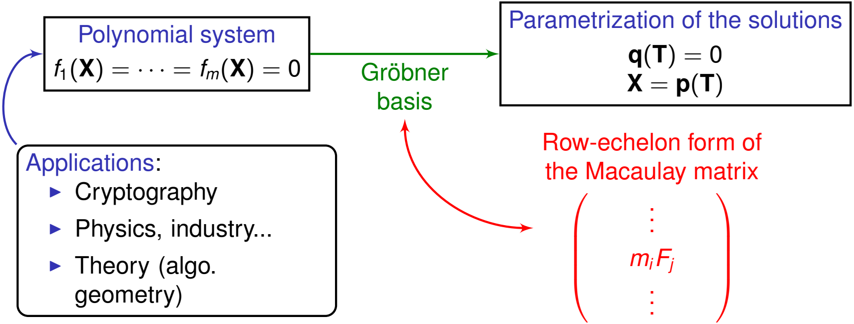
- NP-hard in finite field
- Exponential number of solutions

Problem:
Exploit the structures of the system

Examples of successfully studied structures:

- Homogeneous
- Bihomogeneous: [**FSS10b**]
- Group symmetries: e.g [**FS12**]
- Quasi-homogeneous

Motivations



Difficult problem

- NP-hard in finite field
- Exponential number of solutions

Problem:
Exploit the structures of the system

Examples of successfully studied structures:

- Homogeneous
- Bihomogeneous: [**FSS10b**]
- Group symmetries: e.g [**FS12**]
- Quasi-homogeneous

Definitions of 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 (Volume), Weight 2 (Area), Weight 1 (Height)

Polynomial inversion

$$\begin{cases} X = T^2 + U^2 & \text{Weight 2} \\ Y = T^3 - TU^2 & \text{Weight 3} \\ Z = T + 2U & \text{Weight 1} \end{cases} \longrightarrow P(X, Y, Z) = 0$$

Definitions of 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

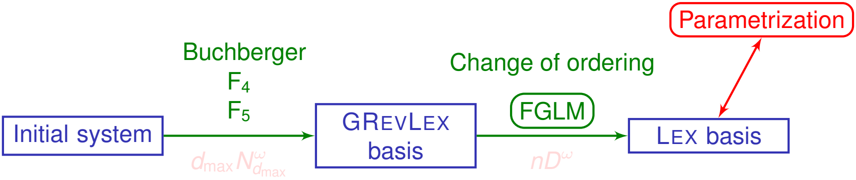
Weight 3 (Volume), Weight 2 (Area), Weight 1 (Height)

Polynomial inversion

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

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

Usual two-steps strategy in the zero-dimensional case



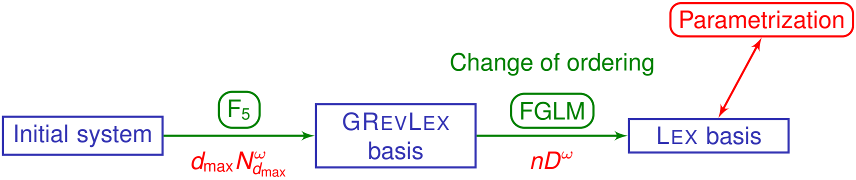
Relevant complexity parameters

- $d_{\max}$ = highest degree reached by F_5
  Less than the degree of regularity d_{reg}.
  For generic homo. systems:
  $$d_{\text{reg}} = \sum_{i=1}^{n}(d_i - 1) + 1 \text{ [**Lazard83**]}$$
- D = degree of the ideal
  $$= \text{number of solutions in dim. } 0$$
  $$= \prod_{i=1}^{n} d_i \text{ (homo. generic case)}$$
- N_d (Macaulay matrix at degree d) → N_d

For an homogeneous system:

$$N_d = \binom{n+d-1}{d}$$

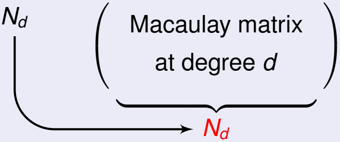
Usual two-steps strategy in the zero-dimensional case



Relevant complexity parameters

- d_{max} = highest degree reached by F5
  Less than the degree of regularity d_{reg}.
  For generic homo. systems:
  $$d_{reg} = \sum_{i=1}^{n}(d_i - 1) + 1 \text{ [\textbf{Lazard83}]}$$
- D = degree of the ideal
  $= $ number of solutions in dim. 0
  $= \prod_{i=1}^{n} d_i$ (homo. generic case)

- N_d



For an homogeneous system:

$$N_d = \binom{n+d-1}{d}$$

Main results

Adaptation of the usual strategy, so that we still have the complexity:

- $C_{F_5} = O\left(d_{\text{reg}} N_{d_{\text{reg}}}^{\omega}\right)$
- $C_{\text{FGLM}} = O\left(nD^{\omega}\right)$

with estimations of the parameters for generic quasi-homogeneous systems:

- $D = \dfrac{\prod_{i=1}^{n} d_i}{\prod_{i=1}^{n} w_i}$
- $d_{\text{reg}} = \displaystyle\sum_{i=1}^{n}(d_i - w_i) + \max\{w_j\}$
- $N_d \simeq \dfrac{1}{\prod_{i=1}^{n} w_i}\dbinom{n+d-1}{d}$

Main results

Adaptation of the usual strategy, so that we still have the complexity:

- $C_{F_5} = O\left(d_{\text{reg}} N_{d_{\text{reg}}}^{\omega}\right)$
- $C_{\text{FGLM}} = O\left(nD^{\omega}\right)$

with estimations of the parameters for generic quasi-homogeneous systems:

- $D = \prod_{i=1}^{n} d_i$
- $d_{\text{reg}} = \sum_{i=1}^{n} (d_i - 1) + 1$
- $N_d = \binom{n+d-1}{d}$

Remark

If we set the weights to $(1, \ldots, 1)$,
we recover the usual values for homogeneous systems.

Setting a road-map

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 road-map:

1. Find a generic property which rules out all reductions to zero
2. Design new algorithms to take advantage of this structure
3. Obtain complexity results

Setting a road-map

Input

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

General road-map:

1. Find a generic property which rules out all reductions to zero
   - Does the F_5-criterion still work for quasi-homo. regular sequences?
   - Are quasi-homo. regular sequences still generic?
2. Design new algorithms to take advantage of this structure
3. Obtain complexity results

Setting a road-map

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 road-map:

1. Find a generic property which rules out all reductions to zero
   - Does the F_5-criterion still work for quasi-homo. regular sequences?
   - Are quasi-homo. regular sequences still generic?
2. Design new algorithms to take advantage of this structure
   - Adapt the matrix-F_5 algorithm to reduce the size of the computed matrices
3. Obtain complexity results

Setting a road-map

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 road-map:

1. Find a generic property which rules out all reductions to zero
   - Does the F_5-criterion still work for quasi-homo. regular sequences?
   - Are quasi-homo. regular sequences still generic?
2. Design new algorithms to take advantage of this structure
   - Adapt the matrix-F_5 algorithm to reduce the size of the computed matrices
3. Obtain complexity results
   - What is the overall complexity?

Setting a road-map

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 road-map:

1. Find a generic property which rules out all reductions to zero
    - Does the F_5-criterion still work for quasi-homo. regular sequences?
    - Are quasi-homo. regular sequences still generic?
2. Design new algorithms to take advantage of this structure
3. Obtain complexity results

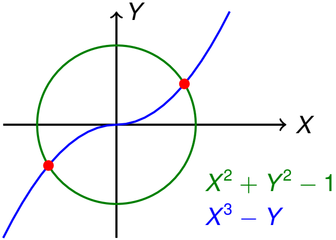
Regular sequences

Definition

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

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

For affine systems: defined w.r.t the highest weighted-degree components.



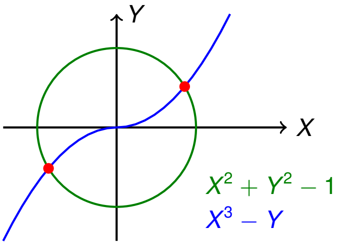
Regular sequences

Definition

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

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

For affine systems: defined w.r.t the highest weighted-degree components.



Generic sequences of homo. polynomials → Generic

Generic sequences of homo. polynomials → Good properties → F_5-criterion; Complexity results

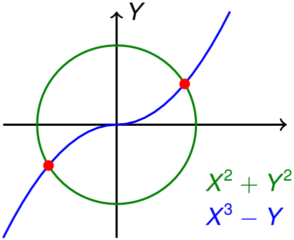
Regular sequences

Definition

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

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

For affine systems: defined w.r.t the highest weighted-degree components.



Result (Faugère, Safey, V.)

Regular seq. are generic amongst systems of quasi-homo. poly. of given W-degree, **assuming there exists at least one regular sequence for that W-degree**.

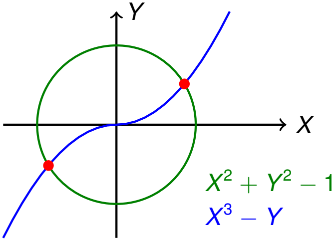
Regular sequences

Definition

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

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

For affine systems: defined w.r.t the highest weighted-degree components.



Result (Faugère, Safey, V.)

Regular seq. are generic amongst systems of quasi-homo. poly. of given W-degree, **assuming there exists at least one regular sequence for that W-degree**.

Why this condition?

- $W = (2, 3),\ d_1 = 4,\ d_2 = 4$: no regular sequence
- $W = (2, 3),\ d_1 = 6,\ d_2 = 6$: (X_1^3, X_2^2) is regular, regular sequences are generic

Hilbert series, degree and degree of regularity

Hilbert series of an ideal

The Hilbert series of a (quasi-)homogeneous ideal is defined as the generating series of the rank defects in the Macaulay matrices of successive degrees.

$$\mathrm{HS}_I(t) = \sum_{d=0}^{\infty} \dim_{K-ev} \left(K[\mathbf{X}]/I\right)_d t^d$$

Expression for a zero-dimensional regular sequence:

$$\mathrm{HS}_I(t) = \frac{(1-t^{d_1})\cdots(1-t^{d_n})}{(1-t)\cdots(1-t)} = (1+\cdots+t^{d_1-1})\cdots(1+\cdots+t^{d_n-1})$$

Bézout and Macaulay bounds

- Bézout bound: $D = \mathrm{HS}_I(t := 1) = \prod_{i=1}^{n} d_i$
- Macaulay bound: $d_{\mathrm{reg}} = \deg(\mathrm{HS}_I) + 1 = \sum_{i=1}^{n}(d_i - 1) + 1$

Hilbert series, degree and degree of regularity

Hilbert series of an ideal

The Hilbert series of a (quasi-)homogeneous ideal is defined as the generating series of the rank defects in the Macaulay matrices of successive degrees.

$$\mathrm{HS}_I(t) = \sum_{d=0}^{\infty} \dim_{K-ev} (K[\mathbf{X}]/I)_d \, t^d$$

Expression for a zero-dimensional regular sequence:

$$\mathrm{HS}_I(t) = \frac{(1-t^{d_1})\cdots(1-t^{d_n})}{(1-t)\cdots(1-t)} = (1+\cdots+t^{d_1-1})\cdots(1+\cdots+t^{d_n-1})$$

Bézout and Macaulay bounds

- Bézout bound: $D = \mathrm{HS}_I(t := 1) = \prod_{i=1}^{n} d_i$
- Macaulay bound: $d_{\mathrm{reg}} = \deg(\mathrm{HS}_I) + 1 = \sum_{i=1}^{n} (d_i - 1) + 1$

Hilbert series, degree and degree of regularity

Hilbert series of an ideal

The Hilbert series of a (quasi-)homogeneous ideal is defined as the generating series of the rank defects in the Macaulay matrices of successive degrees.

$$\mathrm{HS}_I(t) = \sum_{d=0}^{\infty} \dim_{K-ev} \left(K[\mathbf{X}]/I\right)_d t^d$$

Expression for a zero-dimensional regular sequence:

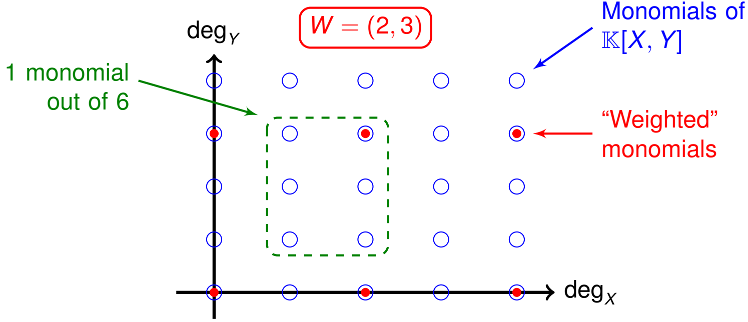
$$\mathrm{HS}_I(t) = \frac{(1-t^{d_1})\cdots(1-t^{d_n})}{(1-t^{w_1})\cdots(1-t^{w_n})} = \frac{(1+\cdots+t^{d_1-1})\cdots(1+\cdots+t^{d_n-1})}{(1+\cdots+t^{w_1-1})\cdots(1+\cdots+t^{w_n-1})}$$

Bézout and Macaulay bounds

- Bézout bound: $D = \mathrm{HS}_I(t := 1) = \dfrac{\prod_{i=1}^{n} d_i}{\prod_{i=1}^{n} w_i}$
- Macaulay bound: $d_{\mathrm{reg}} = \deg(\mathrm{HS}_I) + \max\{w_j\} = \sum_{i=1}^{n}(d_i - w_i) + \max\{w_j\}$

Size of the Macaulay matrices

- Need to count the monomials with a given W-degree
- Combinatorial object named Sylvester denumerants
- Result[1]: asymptotically $N_d \sim \frac{\#\text{Monomials of total degree } d}{\prod_{i=1}^{n} w_i}$



[1] **Geir02**.

Setting a road-map

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 $(d_1, \ldots, d_n)$.

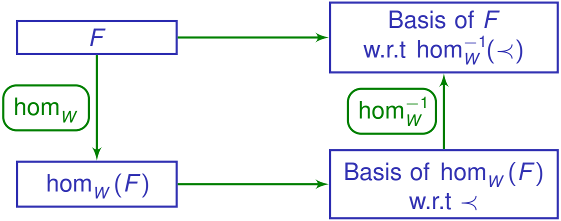
General road-map:

1. Find a generic property which rules out all reductions to zero
2. Design new algorithms to take advantage of this structure
   - Adapt the matrix-F_5 algorithm to reduce the size of the computed matrices
3. Obtain complexity results

Homogenization 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 onto regular sequences
- Good behavior w.r.t Gröbner bases



The W-GRevLex ordering

Analogous to the GRevLex ordering, except monomials are selected according to their W-degree instead of total degree.

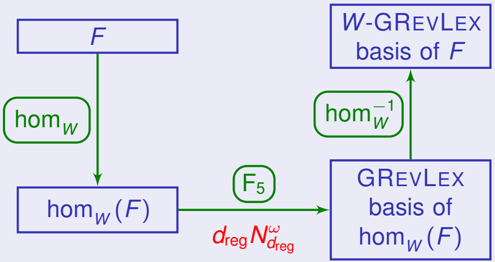
Detailed strategy

Adapting the algorithms

The W-GREVLEX ordering

Analogous to the GREVLEX ordering, except monomials are selected according to their W-degree instead of total degree.

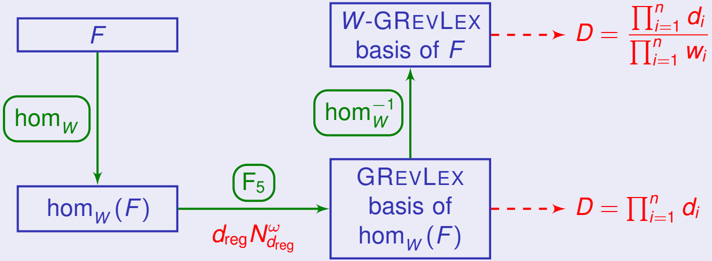
Detailed strategy



The W-GREVLEX ordering

Analogous to the GREVLEX ordering, except monomials are selected according to their W-degree instead of total degree.

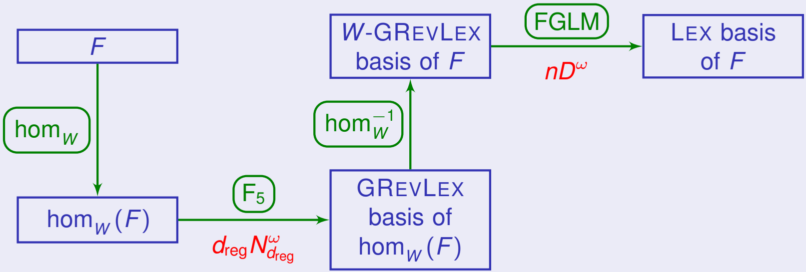
Detailed strategy



The W-GRevLex ordering

Analogous to the GRevLex ordering, except monomials are selected according to their W-degree instead of total degree.

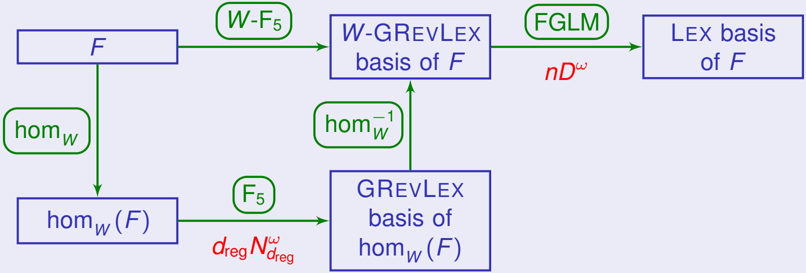
Detailed strategy



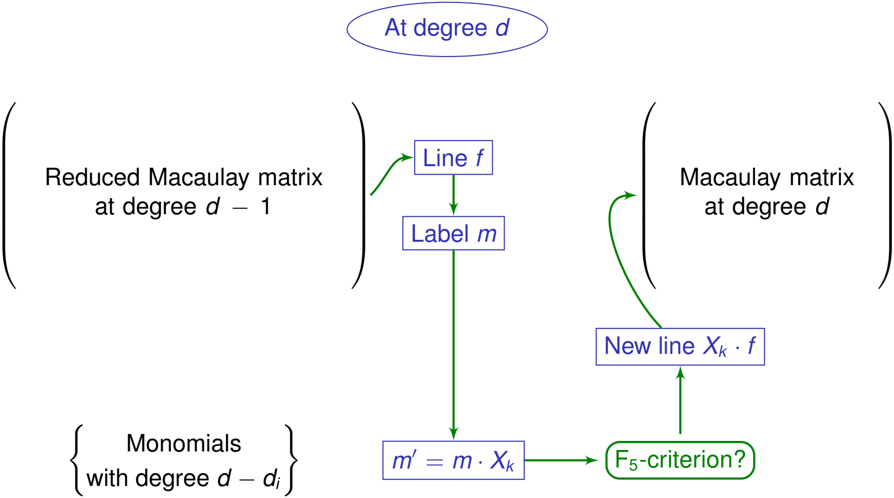
The W-GREVLEX ordering

Analogous to the GREVLEX ordering, except monomials are selected according to their W-degree instead of total degree.

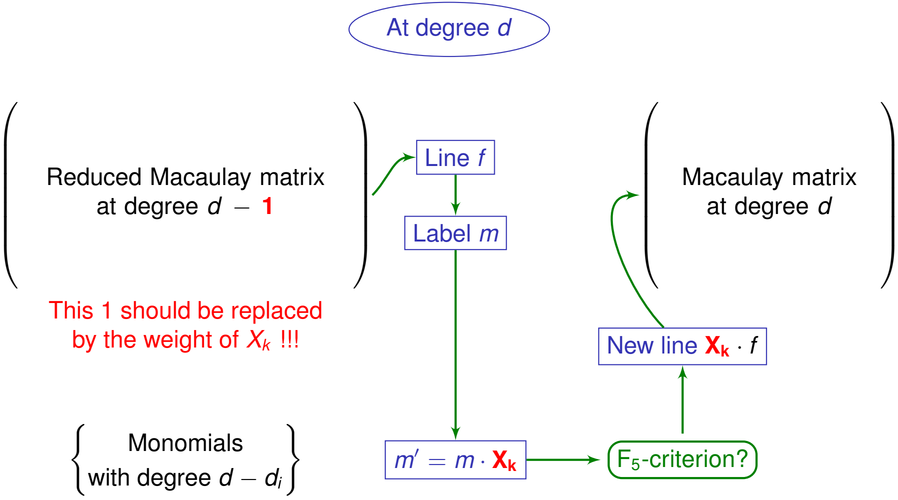
Detailed strategy



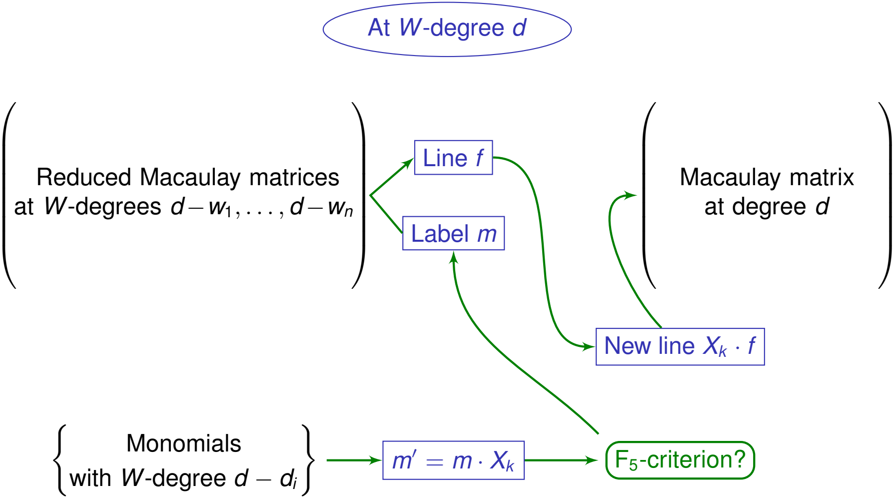
How to adapt the matrix-F_5 algorithm?



How to adapt the matrix-F_5 algorithm?



How to adapt the matrix-F_5 algorithm?



Setting a road-map

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 road-map:

1. Find a generic property which rules out all reductions to zero
2. Design new algorithms to take advantage of this structure
3. Obtain complexity results
   - What is the overall complexity?

Main results

Adaptation of the usual strategy, so that we still have the complexity:

- $C_{F_5} = O\left(d_{\text{reg}} N_{d_{\text{reg}}}^{\omega}\right)$
- $C_{\text{FGLM}} = O\left(nD^{\omega}\right)$

with estimations of the parameters for generic quasi-homogeneous systems:

- $D = \dfrac{\prod_{i=1}^{n} d_i}{\prod_{i=1}^{n} w_i}$
- $d_{\text{reg}} = \sum_{i=1}^{n} (d_i - w_i) + \max\{w_j\}$
- $N_d \simeq \dfrac{1}{\prod_{i=1}^{n} w_i} \binom{n+d-1}{d}$

Overall, the complexity is divided by $\left(\prod w_i\right)^{\omega}$
when compared to a homogeneous system of the same degree.

And what about higher dimension?

For homogeneous systems in positive dimension ($m \leq n$):

- Bézout bound: $D = \prod_{i=1}^{m} d_i$
- Macaulay bound: $d_{\text{reg}} \leq \sum_{i=1}^{m}(d_i - 1) + 1$

Definition

The sequence $f_1, \ldots, f_m$ is in Noether position iff the sequence $f_1, \ldots, f_m, X_{m+1}, \ldots, X_n$ is regular.

Properties

- Information about which variables really matter to the system.
- Not necessary for homogeneous systems in "big enough" fields, because that property is always satisfied up to a linear change of variables.

And what about higher dimension?

For W-homogeneous systems in positive dimension ($m \leq n$):

- Bézout bound: $D = \dfrac{\prod_{i=1}^{n} d_i}{???}$
- Macaulay bound: $d_{\mathrm{reg}} \leq \sum_{i=1}^{m} (d_i - ???) + ???$

Which of the weights to use in the formulas?

Definition

The sequence $f_1, \ldots, f_m$ is in Noether position iff the sequence $f_1, \ldots, f_m, X_{m+1}, \ldots, X_n$ is regular.

Properties

- Information about which variables really matter to the system.
- Not necessary for homogeneous systems in "big enough" fields, because that property is always satisfied up to a linear change of variables.

And what about higher dimension?

For W-homogeneous systems in positive dimension ($m \leq n$):

- Bézout bound: $D = \dfrac{\prod_{i=1}^{n} d_i}{???}$
- Macaulay bound: $d_{\text{reg}} \leq \sum_{i=1}^{m} (d_i - ???) + ???$

Which of the weights to use in the formulas?

Definition

The sequence $f_1, \ldots, f_m$ is in Noether position
iff the sequence $f_1, \ldots, f_m, X_{m+1}, \ldots, X_n$ is regular.

Properties

- Information about which variables really matter to the system.
- Not necessary for homogeneous systems in “big enough” fields, because that property is always satisfied up to a linear change of variables.

Results for a positive-dimensional ideal in Noether position

Result (Faugère, Safey, V.)

Sequences in Noether pos. are generic amongst W-homo. seq. of given W-degree, assuming there exists some sequence in Noether position with that W-degree.

- Bézout bound:

$$D = \frac{\prod_{i=1}^{m} d_i}{\prod_{i=1}^{m} w_i}$$

- Macaulay bound:

$$d_{\text{reg}} = \sum_{i=1}^{m} (d_i - w_i) + \max\{w_j : j \leq m\}$$

- Algorithm matrix-F_5 still runs in complexity polynomial in the Bézout bound.
- Algorithm FGLM only works for zero-dimensional systems.
- These results are nonetheless helpful when we study affine systems (through homogenization).

Results for a positive-dimensional ideal in Noether position

Result (Faugère, Safey, V.)

Sequences in Noether pos. are generic amongst W-homo. seq. of given W-degree, assuming there exists some sequence in Noether position with that W-degree.

- Bézout bound:

$$D = \frac{\prod_{i=1}^{m} d_i}{\prod_{i=1}^{m} w_i}$$

- Macaulay bound:

$$d_{\mathrm{reg}} = \sum_{i=1}^{m}(d_i - w_i) + \max\{w_j : j \leq m\}$$

- Algorithm matrix-F_5 still runs in complexity polynomial in the Bézout bound.
- Algorithm FGLM only works for zero-dimensional systems.
- These results are nonetheless helpful when we study affine systems (through homogenization).

Benchmarks with generic systems

n	$\deg(I)$	t_{F_5}(qh)	Ratio for F_5	t_{FGLM}(qh)	Ratio for FGLM
7	512	0.09s	3.2	0.06s	1.7
8	1024	0.39s	4.2	0.17s	1.9
9	2048	1.63s	4.9	0.59s	2.0
10	4096	7.54s	5.4	2.36s	2.6
11	8192	33.3s	6.4	17.5s	2.4
12	16384	167.9s	6.8	115.8s	
13	32768	796.7s	8.4	782.74s	
14	65536	5040.1s	∞	5602.27s	

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

n	$\deg(I)$	t_{F_5}(qh)	Ratio for F_5	t_{FGLM}(qh)	Ratio for FGLM
3	16	0.00s		0.00s	
4	512	0.03s	3.7	0.07s	
5	65536	935.39s	6.9	2164.38s	3.2

Benchmarks obtained with systems arising in the DLP on Edwards curves, with W-degree (4) for $W = (2, \ldots, 2, 1)$

(Faugère, Gaudry, Huot, Renault 2013)

Conclusion

What we have done

- Theoretical results for quasi-homogeneous systems under generic hypotheses
- Variant of the usual strategy for these systems (variant of F_5 + weighted order)
- Complexity results for F_5 and FGLM for this strategy
  - 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
- Variant of the usual strategy for these systems (variant of F_5 + weighted order)
- Complexity results for F_5 and FGLM for this strategy
  - 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

Thanks for listening!