On The Complexity Of Computing Gröbner Bases For Weighted Homogeneous Systems

Jean-Charles Faugère\textsuperscript{1} \quad Mohab Safey El Din\textsuperscript{1,2} \\

\textbf{Thibaut Verron}\textsuperscript{1}

\textsuperscript{1}Université Pierre et Marie Curie, Paris 6, France \quad
INRIA Paris-Rocquencourt, Équipe POLSYS \quad
Laboratoire d'Informatique de Paris 6, UMR CNRS 7606

\textsuperscript{2}Institut Universitaire de France

12 september 2014
An example
Finding the relations between 50 monomials of degree 2 in 25 variables

\[
\begin{align*}
X_{15}X_{25} - T_1 & \quad X_{21}X_{22} - T_{11} & \quad X_{12}X_{14} - T_{21} & \quad X_3X_{21} - T_{31} & \quad X_1X_{12} - T_{41} \\
X_2X_4 - T_2 & \quad X_4X_{12} - T_{12} & \quad X_4X_{16} - T_{22} & \quad X_6X_{24} - T_{32} & \quad X_5X_{12} - T_{42} \\
X_8X_{15} - T_3 & \quad X_1^2 - T_{13} & \quad X_6X_8 - T_{23} & \quad X_6X_8 - T_{23} & \quad X_1X_{19} - T_{43} \\
X_6X_8 - T_4 & \quad X_1X_2 - T_{14} & \quad X_{14}^2 - T_{24} & \quad X_{13}X_{20} - T_{34} & \quad X_{12}X_{18} - T_{44} \\
X_5X_{12} - T_5 & \quad X_2^2 - T_{15} & \quad X_8X_{21} - T_{25} & \quad X_6X_{19} - T_{35} & \quad X_7X_{11} - T_{45} \\
X_6X_{12} - T_6 & \quad X_5X_{10} - T_{16} & \quad X_{16}X_{23} - T_{26} & \quad X_9X_{15} - T_{36} & \quad X_9X_{20} - T_{46} \\
X_9X_{19} - T_7 & \quad X_1X_{10} - T_{17} & \quad X_3X_{13} - T_{27} & \quad X_2X_{13} - T_{37} & \quad X_4X_{21} - T_{47} \\
X_6X_{10} - T_8 & \quad X_{20}X_{23} - T_{18} & \quad X_{11}X_{20} - T_{28} & \quad X_{10}X_{23} - T_{38} & \quad X_7X_{23} - T_{48} \\
X_8X_{18} - T_9 & \quad X_2X_{23} - T_{19} & \quad X_{14}X_{22} - T_{29} & \quad X_3X_7 - T_{39} & \quad X_{14}X_{22} - T_{49} \\
X_5X_8 - T_{10} & \quad X_3X_{14} - T_{20} & \quad X_{16}X_{23} - T_{30} & \quad X_{10}X_{19} - T_{40} & \quad X_5X_7 - T_{50}
\end{align*}
\]
**An example**

Finding the relations between 50 monomials of degree 2 in 25 variables

| $X_{15}X_{25} - T_1$ | $X_{21}X_{22} - T_{11}$ | $X_{12}X_{14} - T_{21}$ | $X_{3}X_{21} - T_{31}$ | $X_{1}X_{12} - T_{41}$ |
| $X_2X_4 - T_2$       | $X_{4}X_{12} - T_{12}$ | $X_{4}X_{16} - T_{22}$ | $X_{6}X_{24} - T_{32}$ | $X_{5}X_{12} - T_{42}$ |
| $X_8X_{15} - T_3$    | $X_{2}^2 - T_{13}$    | $X_{2}^2 - T_{24}$    | $X_{13}X_{20} - T_{34}$ | $X_{16}X_{19} - T_{43}$ |
| $X_6X_8 - T_4$      | $X_1X_2 - T_{14}$     | $X_8X_{21} - T_{25}$  | $X_6X_{19} - T_{35}$  | $X_{12}X_{18} - T_{44}$ |
| $X_5X_{12} - T_5$   | $X_{25} - T_{15}$     | $X_8X_{23} - T_{26}$  | $X_9X_{15} - T_{36}$  | $X_7X_{11} - T_{45}$  |
| $X_6X_{12} - T_6$   | $X_5X_{10} - T_{16}$  | $X_{16}X_{23} - T_{26}$ | $X_9X_{20} - T_{46}$ | $X_9X_{20} - T_{46}$ |
| $X_9X_{19} - T_7$   | $X_1X_{10} - T_{17}$  | $X_{3}X_{13} - T_{27}$ | $X_{2}X_{13} - T_{37}$ | $X_4X_{21} - T_{47}$ |
| $X_6X_{10} - T_8$   | $X_{20}X_{23} - T_{18}$ | $X_{11}X_{20} - T_{28}$ | $X_{10}X_{23} - T_{38}$ | $X_7X_{23} - T_{48}$ |
| $X_8X_{18} - T_9$   | $X_2X_{23} - T_{19}$  | $X_{14}X_{22} - T_{29}$ | $X_{3}X_{7} - T_{39}$ | $X_{14}X_{22} - T_{49}$ |
| $X_5X_8 - T_{10}$   | $X_{3}X_{14} - T_{20}$ | $X_{16}X_{23} - T_{30}$ | $X_{10}X_{19} - T_{40}$ | | $X_5X_{7} - T_{50}$ |

**Description of the system**

- 50 equations, 75 variables
- Polynomials $m_i - T_i$ with $m_i$ degree 2 monomial
- **Goal**: find all relations between the $m_i$ \iff find all polynomials $P(T_j)$ in the ideal

**Tool**: Gröbner bases

**Total degree grading**

- difficult (~8h with Magma, intermediate basis in 4h)
- irregular behavior
  (highest deg. components not indep.)

**Weighted degree grading**

- Weight($T_i$) = Degree($m_i$) = 2
- easier (~4h with Magma, intermediate basis in 0.1s)
- regular behavior
An example
Finding the relations between 50 monomials of degree 2 in 25 variables

\[ X_{15}X_{25} - T_1 \]
\[ X_{24}X_4 - T_2 \]
\[ X_{8}X_{15} - T_3 \]
\[ X_{6}X_{8} - T_4 \]
\[ X_{5}X_{12} - T_5 \]
\[ X_{6}X_{12} - T_6 \]
\[ X_{9}X_{19} - T_7 \]
\[ X_{6}X_{10} - T_8 \]
\[ X_{8}X_{18} - T_9 \]
\[ X_{5}X_{8} - T_{10} \]
\[ X_{21}X_{22} - T_{11} \]
\[ X_{4}X_{12} - T_{12} \]
\[ X_{1}X_{2} - T_{14} \]
\[ X_{25}^2 - T_{15} \]
\[ X_{5}X_{10} - T_{16} \]
\[ X_{1}X_{10} - T_{17} \]
\[ X_{20}X_{23} - T_{18} \]
\[ X_{3}X_{14} - T_{20} \]
\[ X_{12}X_{14} - T_{21} \]
\[ X_{4}X_{16} - T_{22} \]
\[ X_{4}^2 - T_{24} \]
\[ X_{8}X_{21} - T_{25} \]
\[ X_{5}X_{19} - T_{35} \]
\[ X_{6}X_{19} - T_{35} \]
\[ X_{2}X_{23} - T_{19} \]
\[ X_{2}X_{10} - T_{26} \]
\[ X_{3}X_{13} - T_{27} \]
\[ X_{11}X_{20} - T_{28} \]
\[ X_{4}X_{22} - T_{29} \]
\[ X_{3}X_{7} - T_{39} \]
\[ X_{16}X_{23} - T_{30} \]
\[ X_{10}X_{19} - T_{40} \]
\[ X_{5}X_{7} - T_{50} \]

Description of the system
- 50 equations, 75 variables
- Polynomials \( m_i - T_i \) with \( m_i \) degree 2 monomial
- Goal: find all relations between the \( m_i \) \iff find all polynomials \( P(T_j) \) in the ideal

Tool: Gröbner bases

Total degree grading
- difficult (~8h with Magma, intermediate basis in 4h)
- irregular behavior (highest deg. components not indep.)

Weighted degree grading
- \( \text{Weight}(T_i) = \text{Degree}(m_i) = 2 \)
- easier (~4h with Magma, intermediate basis in 0.1s)
- regular behavior
An example
Finding the relations between 50 monomials of degree 2 in 25 variables

\[
\begin{align*}
X_{15}X_{25} - T_1 & \quad X_{21}X_{22} - T_{11} & \quad X_{12}X_{14} - T_{21} & \quad X_3X_{21} - T_{31} & \quad X_1X_{12} - T_{41} \\
X_2X_4 - T_2 & \quad X_4X_{12} - T_{12} & \quad X_4X_{16} - T_{22} & \quad X_6X_{24} - T_{32} & \quad X_5X_{12} - T_{42} \\
X_8X_{15} - T_3 & \quad X_{12} - T_{13} & \quad X_6X_8 - T_{23} & \quad X_{15}X_{25} - T_{33} & \quad X_6X_{19} - T_{43} \\
X_6X_8 - T_4 & \quad X_1X_2 - T_{14} & \quad X^2_{14} - T_{24} & \quad X_{13}X_{20} - T_{34} & \quad X_7X_{11} - T_{44} \\
X_5X_{12} - T_5 & \quad X^2_{25} - T_{15} & \quad X_8X_{21} - T_{25} & \quad X_6X_{19} - T_{35} & \quad X_7X_{11} - T_{45} \\
X_6X_{12} - T_6 & \quad X_5X_{10} - T_{16} & \quad X_{16}X_{23} - T_{26} & \quad X_9X_{15} - T_{36} & \quad X_9X_{20} - T_{46} \\
X_9X_{19} - T_7 & \quad X_1X_{10} - T_{17} & \quad X_3X_{13} - T_{27} & \quad X_2X_{13} - T_{37} & \quad X_4X_{21} - T_{47} \\
X_6X_{10} - T_8 & \quad X_{20}X_{23} - T_{18} & \quad X_{11}X_{20} - T_{28} & \quad X_{10}X_{23} - T_{38} & \quad X_7X_{23} - T_{48} \\
X_8X_{18} - T_9 & \quad X_2X_{23} - T_{19} & \quad X_{14}X_{22} - T_{29} & \quad X_3X_7 - T_{39} & \quad X_{14}X_{22} - T_{49} \\
X_5X_8 - T_{10} & \quad X_3X_{14} - T_{20} & \quad X_{16}X_{23} - T_{30} & \quad X_{10}X_{19} - T_{40} & \quad X_5X_7 - T_{50}
\end{align*}
\]

Description of the system
- 50 equations, 75 variables
- Polynomials $m_i - T_i$ with $m_i$ degree 2 monomial
- **Goal**: find all relations between the $m_i$ $\iff$ find all polynomials $P(T_j)$ in the ideal

Tool: Gröbner bases

Total degree grading
- difficult (~8h with Magma, intermediate basis in 4h)
- irregular behavior (highest deg. components not indep.)

Weighted degree grading
- Weight($T_i$) = Degree($m_i$) = 2
- easier (~4h with Magma, intermediate basis in 0.1s)
- regular behavior
A run of $F_4$ on the example
Ideal of relations between 50 monomials of degree 2 in 25 variables

Algorithm $F_4$, step by step

- 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)
Gröbner bases and structured systems

Polynomial system

\[
\begin{align*}
    f : \quad X^2 + 2XY + Y^2 + X &= 0 \\
    g : \quad X^2 - XY + Y^2 + Y - 1 &= 0
\end{align*}
\]

Gröbner basis

\[
\begin{align*}
    Y^3 &+ Y^2 - \frac{4}{9}X - \frac{2}{9}Y - \frac{4}{9} \\
    X^2 &+ Y^2 + \frac{1}{3}X + \frac{2}{3}Y - \frac{2}{3} \\
    XY &+ \frac{1}{3}X - \frac{1}{3}Y + \frac{1}{3}
\end{align*}
\]

Problematic

Structured systems

→ Can we exploit it?

Successfully studied structures

- Bihomogeneous (Dickenstein, Emiris, Faugère, Safey, Spaenlehauer...)
- Group symmetries (Colin, Faugère, Gatermann, Rahmany, Svartz...)
- Weighted homo. / Quasi-homo. ([Traverso 1996], [FSV 2013]...)
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. with monomials of same \( W \)-degree

→ Example: physical systems: Volume = Area \( \times \) Height

\[ \text{Weight 3} \quad \text{Weight 2} \quad \text{Weight 1} \]

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
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): \( \text{deg}_W(X_1^{\alpha_1} \cdots X_n^{\alpha_n}) = \sum_{i=1}^{n} w_i \alpha_i \)

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

→ Example: physical systems: Volume = Area \( \times \) Height

\[\begin{array}{c}
\text{Weight 3} \\
\text{Weight 2} \\
\text{Weight 1}
\end{array}\]

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
Complexity for generic homogeneous systems

Homogeneous, generic, with total degree \((d_1, \ldots, d_m)\)

\[ F(X_1, \ldots, X_n) \]

Buchberger

- [Buchberger 1976]
- [Faugère 1999]
- [Faugère 2002]

\[ \text{GREVLEX basis} \]

if \(m \geq n\) (zero-dimensional case)

\[ \text{FGLM} \]  
[Faugère, Gianni, Lazard and Mora 1993]

\[ \text{LEX basis} \]
Complexity for generic homogeneous systems

Homogeneous, generic, with total degree \((d_1, \ldots, d_m)\)

- \(F(X_1, \ldots, X_n)\)
- \(F_5\)
- \(\text{GRevLex basis}\)
- \(\text{FGLM}\) if \(m \geq n\) (zero-dimensional case)
- \(\text{Lex basis}\)

- Highest degree \(d_{\text{reg}} \leq \sum_{i=1}^{m} (d_i - 1) + 1\)
- Size of the matrix at degree \(d = \binom{n + d - 1}{d}\)

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

\[O\left(\left(\frac{n + d_{\text{reg}} - 1}{d_{\text{reg}}}\right)^3 + n\left(\prod_{i=1}^{n} d_i\right)^3\right)\]
Computational strategy for weighted homogeneous systems

- $F(X_1, \ldots, X_n)$, $W$
  - $W$-Homogeneous, generic, with $W$-degree $(d_1, \ldots, d_m)$
  - (zero-dimensional: $m = n$)

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

- $W$-GREVLEX basis of $F$
- $\text{FGLM}$
  - $W$-GREVLEX basis of $F$
- $\text{LEX basis}$

$W = (w_1, \ldots, w_n)$
Algorithms: from weighted homogeneous to homogeneous

Transformation morphism

\[ \text{hom}_W : (\mathbb{K}[X], W\text{-deg}) \rightarrow (\mathbb{K}[X], \text{deg}) \]

\[ f \mapsto f(X_1^{w_1}, \ldots, X_n^{w_n}) \]

- Graded injective morphism
- Sends regular ("independent") sequences on regular sequences
- \( S\text{-Pol}(\text{hom}_W(f), \text{hom}_W(g)) = \text{hom}_W(S\text{-Pol}(f, g)) \)
  \[ \rightarrow \text{Good behavior w.r.t Gröbner bases} \]

(Weighted homogeneous)  

\[ F \]

Gröbner

Basis of \( F \) w.r.t \( \text{hom}_W^{-1}(\prec) \)

(Homogeneous)

\[ \text{hom}_W(F) \]

Gröbner

Basis of \( \text{hom}_W(F) \) w.r.t \( \prec \)
Size of the Macaulay matrices

Counting the monomials

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

\(^1\)Geir Agnarsson (2002). ‘On the Sylvester denumerants for general restricted partitions’
$F(X_1, \ldots, X_n), W$

$F(X_1^{w_1}, \ldots, X_n^{w_n})$

$F_5$

$W$-GRevLex basis of $F$

$W$-Homogeneous, generic, with $W$-degree $(d_1, \ldots, d_m)$
(zero-dimensional: $m = n$)

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

Highest $W$-degree

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

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

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

$O\left(\left(\frac{1}{\prod_{i=1}^{n} w_i}\right)^3 \left[\binom{n + d_{W,\text{reg}} - 1}{d_{W,\text{reg}}}^3 + n \left(\prod_{i=1}^{n} d_i\right)^3\right]\right)$
Main results: lifted hypotheses and sharper bound

\[ F(X_1, \ldots, X_n), W \]

\[ F(X_1^{w_1}, \ldots, X_n^{w_n}) \]

\[ W\text{-Homogeneous, generic, with } W\text{-degree } (d_1, \ldots, d_m) \]

\[ (m < n \text{ or } m = n \text{ or } m > n) \]

Homogeneous, with total degree \((d_1, \ldots, d_m)\)

\[ W = (w_1, \ldots, w_n) \]

\[ W\text{-Homogeneous, with total degree } (d_1, \ldots, d_m) \]

\[
\begin{align*}
\text{Highest } W\text{-degree (if } m \leq n) & \\
& d_{W, \text{reg}} \leq \sum_{i=1}^{m} (d_i - w_i) + w_m
\end{align*}
\]

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

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

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

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

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

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

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

Property [FSV 2013]

- Regular sequences of \( W\)-homo. polynomials
- Generic if \( \neq \emptyset \)
- Good properties
- \( F_5 \)-criterion
- Hilbert series
Properties of regular sequences

Hilbert series

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

Properties

For regular sequences of \( W \)-homogeneous polynomials of \( W \)-degree \( d_i \):

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

In dimension zero \((m = n)\):

- **Bézout bound on the degree:** \( D = \frac{\prod_{i=1}^{n} d_i}{\prod_{i=1}^{n} w_i} \)

- **Macaulay bound on \( d_{\text{reg}} \) [FSV 2013]:** \( d_{\text{reg}} \leq \sum_{i=1}^{n} (d_i - w_i) + \max\{w_j\} \)
Can we do better? Yes, but not with the regularity alone.

Positive dimension ($m < n$)

- Need to know what variables matter to the system
- Information not available from regularity
  → (Simultaneous) Noether position

Dimension 0 ($m = n$)

- Macaulay’s bound on $d_{\text{reg}}$ is not sharp
- $d_{\text{reg}}$ depends on the order of the variables:

<table>
<thead>
<tr>
<th>$W$</th>
<th>$W$-degree</th>
<th>Macaulay’s bound</th>
<th>$d_{\text{reg}}$</th>
<th>$F_4$ DRL time</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(20, 5, 5, 1)$</td>
<td>$(60, 60, 60, 60)$</td>
<td>229</td>
<td>210</td>
<td>471s</td>
</tr>
<tr>
<td>$(1, 5, 5, 20)$</td>
<td>$(60, 60, 60, 60)$</td>
<td>229</td>
<td>220</td>
<td>916s</td>
</tr>
</tbody>
</table>

→ Simultaneous Noether position

Overdetermined systems ($m > n$)

- No regular sequence → Semi-regularity
Noether position

\[ F = (f_1, \ldots, f_m) \in \mathbb{K}[X_1, \ldots, X_n], \; m \leq n \]

- **Noether position:**
  \((F, X_{m+1}, \ldots, X_n)\) regular

- **simultaneous Noether position:**
  \((f_1, \ldots, f_j)\) in NP for all \(j\)'s

Properties

- **Generic** if not empty
- **Valid under generic change of coordinates** for “nice” systems of weights
- **Relevant property for fine-grained complexity** (structure lemma [Bardet 2004])
- For a \(W\)-homogeneous sequence in simultaneous Noether position:

\[
d_{\text{reg}} \leq \sum_{i=1}^{m} (d_i - w_i) + w_m \quad \text{(sharp if \(w_m = 1\))}
\]
### Semi-regular sequences

- **If** \( m > n \), reductions to zero cannot be eliminated.
- **Semi-regular sequence**: all reductions to zero are at high degrees.
- **Hilbert series of a semi-regular homogeneous sequence**:
  \[
  HS_{A/I}(T) = \left( \frac{1 - T^{d_1}}{1 - T} \right) \cdots \left( \frac{1 - T^{d_m}}{1 - T} \right) (1 - T)^n
  \]
  (series truncated to the first coefficient \( \leq 0 \))

- For \( W \)-homogeneous systems, only true for “nice” systems of weights.
- **Main consequence**: asymptotic estimate of the degree of regularity [Bardet 2004]

### Fröberg’s conjecture

Semi-regular sequences are generic.

**Proved for:**
- \( n = 2 \)
- \( n = 3 \) for large fields
- \( m = n + 1 \) in characteristic 0.
Semi-regular sequences

- If $m > n$, reductions to zero cannot be eliminated.
- **Semi-regular sequence**: all reductions to zero are at high degrees
- Hilbert series of a semi-regular $W$-homogeneous sequence:
  \[
  \text{HS}_{A/I}(T) = \left[ \frac{(1 - T^{d_1}) \cdots (1 - T^{d_m})}{(1 - T^{w_1}) \cdots (1 - T^{w_n})} \right] \quad \text{(series truncated to the first coefficient } \leq 0)\]

- For $W$-homogeneous systems, only true for “nice” systems of weights
- Main consequence: asymptotic estimate of the degree of regularity [Bardet 2004]

Fröberg’s conjecture

Semi-regular sequences are generic.

Proved for:
- $n = 2$
- $n = 3$ for large fields
- $m = n + 1$ in characteristic 0
## Complexity

### Input

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

### Complexity of \( F_5 \)

\[
\left( \frac{1}{\prod_{i=1}^{n} w_i} \right)^3 \left( n + d_{\text{reg}} - 1 \right)^3
\]

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

### Complexity of FGLM (\( m = n \))

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

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

$F$ : 0-dim. affine system with a weighted homogeneous structure

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

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

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

Algorithm $F_5$, timings

- FGLM timing for $n = 13$:
  - 5602.3 s
  - 1645.1 s
- 65,536 solutions
- Ratio = 2.1

Ratio = 8.4 for $n = 10$
The story is not over...

Sometimes, “normally” faster...

- Generic complete intersection (\texttt{GREVLEX}): 13 min. vs. 1h45 (speed-up: 8)
- Relations between monomials (elim.): 4h vs 8h (speed-up: 2)
- Relations between 14 invariants of the cyclic-5 group (elim.): 40 min. vs 10h (speed-up: 16)

... sometimes, faster than that...

- Relations between monomials (\texttt{GREVLEX}): 0.1s vs 4h (speed-up: 144 000)

... and sometimes, same speed.

- Relations between monomials (elim. from \texttt{GREVLEX})
- Elimination on generic systems (elim.)
Conclusion and perspectives

What we have done

- **Theoretical results** for $W$-homogeneous systems under generic assumptions
- **Complexity results** for $F_5$ for positive-dim. systems and overdetermined systems
  - Bound on the maximal degree reached by the $F_5$ algorithm
  - Complexity overall divided by $(\prod w_i)^3$

Consequences

Wide range of potential applications:
- Polynomial inversion, implicitization (positive dimension)
- Cryptography (overdetermined)

Perspectives

- Timings still not completely understood
- Affine systems: find the most appropriate system of weights
- Additional structure: $W$-homo. for several systems of weights, weights $\leq 0$...
Conclusion and perspectives

What we have done

- **Theoretical results** for $W$-homogeneous systems under generic assumptions
- **Complexity results** for $F_5$ for positive-dim. systems and overdetermined systems
  - Bound on the maximal degree reached by the $F_5$ algorithm
  - Complexity overall divided by $(\prod w_i)^3$

Consequences

Wide range of potential applications:

- Polynomial inversion, implicitization (positive dimension)
- Cryptography (overdetermined)

Perspectives

- Timings still not completely understood
- **Affine systems**: find the most appropriate system of weights
- **Additional structure**: $W$-homo. for several systems of weights, weights $\leq 0$...
Thank you for your attention!