

Complexity of polynomial system solving and related invariants

Elisa Gorla

Institut de mathématiques, Université de Neuchâtel

Workshop on Algebraic Methods in Post-Quantum Cryptography,
Ohrid, August 11, 2026

THE UBIQUITY OF POLYNOMIAL SYSTEM SOLVING

Many problems in the sciences and engineering may be modelled via polynomials, e.g.:

- algebraic statistics,
- algebraic biology,
- chemical reaction networks,
- coding theory,
- computer vision,
- cryptography,
- networks modelling,
- neuroscience,
- robotics,
- string theory,
- topological data analysis via (multivariate) persistent homology.

MULTIVARIATE CRYPTOGRAPHY

The security of multivariate cryptographic primitives relies on the computational hardness of solving a system of polynomial equations over a finite field $\mathbb{F}_q$.

MULTIVARIATE CRYPTOGRAPHY

The security of multivariate cryptographic primitives relies on the computational hardness of solving a system of polynomial equations over a finite field $\mathbb{F}_q$.

We focus on systems which:

- have a finite number of solutions over the algebraic closure,
- are not homogeneous (but if they are, our analysis becomes easier!),
- contain the field equations $x_1^q - x_1, \dots, x_n^q - x_n$, if q is small.

MULTIVARIATE CRYPTOGRAPHY

The security of multivariate cryptographic primitives relies on the computational hardness of solving a system of polynomial equations over a finite field $\mathbb{F}_q$.

We focus on systems which:

- have a finite number of solutions over the algebraic closure,
- are not homogeneous (but if they are, our analysis becomes easier!),
- contain the field equations $x_1^q - x_1, \dots, x_n^q - x_n$, if q is small.

How to solve such a system?

- one can find the solutions by exhaustive search,
- using [Gröbner bases](#),
- by exploiting the specific structure of the system (structural attacks).

HOW TO COMPUTE A GRÖBNER BASIS

Linear algebra based algorithms are the most efficient. They include F_4/F_5 and XL and its variants.

HOW TO COMPUTE A GRÖBNER BASIS

Linear algebra based algorithms are the most efficient. They include F_4/F_5 and XL and its variants.

Definition

Given a system $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R = K[x_1, \dots, x_n]$,
for each degree d one has a **Macaulay matrix**:

- columns $\leftrightarrow$ monomials of degree $\leq d$
- rows $\leftrightarrow \mu f_i$, μ a monomial, $\deg(\mu f_i) \leq d$
- the entry (i, j) is the coefficient of the monomial corresponding to column j in the polynomial corresponding to row i

The matrix is brought in RREF.

For $d \gg 0$, the rows are a Gröbner basis of $\mathcal{F}$.

Standard algorithms simply compute the RREF of a Macaulay matrix in a given degree, while **mutant algorithms** add new rows to the matrix whenever a degree drop occurs, then compute the RREF again.

EXAMPLE

$f_1 = x_1x_2 + x_2$, $f_2 = x_2^2 - 1$, degrevlex order

	x_1^2	x_1x_2	x_2^2	x_1	x_2	1
f_1	0	1	0	0	1	0
f_2	0	0	1	0	0	-1

EXAMPLE

$f_1 = x_1x_2 + x_2$, $f_2 = x_2^2 - 1$, degrevlex order

	x_1^2	x_1x_2	x_2^2	x_1	x_2	1
f_1	0	1	0	0	1	0
f_2	0	0	1	0	0	-1

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	x_1^2	x_1x_2	x_2^2	x_1	x_2	1
x_1f_1	0	1	0	0	0	1	0	0	0	0
x_1f_2	0	0	1	0	0	0	0	-1	0	0
x_2f_1	0	0	1	0	0	0	1	0	0	0
x_2f_2	0	0	0	1	0	0	0	0	-1	0
f_1	0	0	0	0	0	1	0	0	1	0
f_2	0	0	0	0	0	0	1	0	0	-1

EXAMPLE

$f_1 = x_1x_2 + x_2$, $f_2 = x_2^2 - 1$, degrevlex order

	x_1^2	x_1x_2	x_2^2	x_1	x_2	1
f_1	0	1	0	0	1	0
f_2	0	0	1	0	0	-1

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	x_1^2	x_1x_2	x_2^2	x_1	x_2	1
	0	1	0	0	0	0	0	0	-1	0
	0	0	1	0	0	0	0	-1	0	0
	0	0	0	1	0	0	0	0	-1	0
	0	0	0	0	0	1	0	0	1	0
	0	0	0	0	0	0	1	0	0	-1
	0	0	0	0	0	0	0	1	0	1

$x_1 + 1$ and $x_2^2 - 1$ are a degrevlex Gröbner basis of (f_1, f_2) .

COMPLEXITY OF SOLVING A POLYNOMIAL SYSTEM

The solutions of a polynomial system can be obtained by:

- computing a Gröbner basis,
- a linear algebra step,
- computing the roots of a univariate polynomial.

COMPLEXITY OF SOLVING A POLYNOMIAL SYSTEM

The solutions of a polynomial system can be obtained by:

- computing a Gröbner basis,
- a linear algebra step,
- computing the roots of a univariate polynomial.

The complexity is dominated by the first step.

COMPLEXITY OF SOLVING A POLYNOMIAL SYSTEM

The solutions of a polynomial system can be obtained by:

- computing a Gröbner basis,
- a linear algebra step,
- computing the roots of a univariate polynomial.

The complexity is dominated by the first step.

The complexity of the first step is dominated by the cost of Gaussian elimination in the largest Macaulay matrix. This is bounded by the size of the matrix, hence by a binomial in the number of variables and the largest degree d in which we compute.

Definition

The **solving degree** of $\mathcal{F}$, denoted $\text{sol. deg}(\mathcal{F})$, is the least degree for which Gaussian elimination in the Macaulay matrix of degree d yields a Gröbner basis of $\mathcal{F} = \{f_1, \dots, f_m\}$. Write $\text{sol. deg}^s(\mathcal{F})$ for standard algorithms and $\text{sol. deg}^m(\mathcal{F})$ for mutant algorithms.

SOLVING DEGREE

Let $\mathcal{F} = \{f_1, \dots, f_m\}$, fix the **degrevlex order**.

Definition

The **solving degree** of $\mathcal{F}$ is the least degree for which Gaussian elimination in the Macaulay matrix of degree d yields a Gröbner basis of $\mathcal{F}$.

Write **solv. deg^s($\mathcal{F}$)** for standard and **solv. deg^m($\mathcal{F}$)** for mutant algorithms. **max. GB. deg($\mathcal{F}$)** is the largest degree of a polynomial in the Gröbner basis of $\mathcal{F}$.

SOLVING DEGREE

Let $\mathcal{F} = \{f_1, \dots, f_m\}$, fix the **degrevlex order**.

Definition

The **solving degree** of $\mathcal{F}$ is the least degree for which Gaussian elimination in the Macaulay matrix of degree d yields a Gröbner basis of $\mathcal{F}$.

Write **solv. deg^s($\mathcal{F}$)** for standard and **solv. deg^m($\mathcal{F}$)** for mutant algorithms. **max. GB. deg($\mathcal{F}$)** is the largest degree of a polynomial in the Gröbner basis of $\mathcal{F}$.

Remark

$$\text{solv. deg}^s(\mathcal{F}) \geq \text{solv. deg}^m(\mathcal{F}) \geq \text{max. GB. deg}(\mathcal{F})$$

$$\text{solv. deg}^s(\mathcal{F}) = \text{solv. deg}^m(\mathcal{F}) = \text{max. GB. deg}(\mathcal{F}) \text{ if } \mathcal{F} \text{ is homogeneous}$$

SOLVING DEGREE

Let $\mathcal{F} = \{f_1, \dots, f_m\}$, fix the **degrevlex order**.

Definition

The **solving degree** of $\mathcal{F}$ is the least degree for which Gaussian elimination in the Macaulay matrix of degree d yields a Gröbner basis of $\mathcal{F}$.

Write **solv. deg^s($\mathcal{F}$)** for standard and **solv. deg^m($\mathcal{F}$)** for mutant algorithms.
max. GB. deg($\mathcal{F}$) is the largest degree of a polynomial in the Gröbner basis of $\mathcal{F}$.

Remark

$$\text{solv. deg}^s(\mathcal{F}) \geq \text{solv. deg}^m(\mathcal{F}) \geq \text{max. GB. deg}(\mathcal{F})$$

$$\text{solv. deg}^s(\mathcal{F}) = \text{solv. deg}^m(\mathcal{F}) = \text{max. GB. deg}(\mathcal{F}) \text{ if } \mathcal{F} \text{ is homogeneous}$$

Example

The degrevlex Gröbner basis of $f_1 = x_1x_2 + x_2$, $f_2 = x_2^2 - 1$ is $x_1 + 1, x_2^2 - 1$, so $\text{max. GB. deg}(\mathcal{F}) = 2 < 3 = \text{solv. deg}^m(\mathcal{F}) = \text{solv. deg}^s(\mathcal{F})$.

BOUNDING THE SOLVING DEGREE

In order to bound the security of a multivariate cryptographic scheme, we estimate the solving degree of the corresponding polynomial system.

BOUNDING THE SOLVING DEGREE

In order to bound the security of a multivariate cryptographic scheme, we estimate the solving degree of the corresponding polynomial system.

As we cannot just compute the Gröbner basis and see in which degree the computation ends, we need a priori estimates for the solving degree.

BOUNDING THE SOLVING DEGREE

In order to bound the security of a multivariate cryptographic scheme, we estimate the solving degree of the corresponding polynomial system.

As we cannot just compute the Gröbner basis and see in which degree the computation ends, we need a priori estimates for the solving degree.

Several authors estimate the solving degree through a mix of heuristic arguments and computer experiments on small examples.

BOUNDING THE SOLVING DEGREE

In order to bound the security of a multivariate cryptographic scheme, we estimate the solving degree of the corresponding polynomial system.

As we cannot just compute the Gröbner basis and see in which degree the computation ends, we need a priori estimates for the solving degree.

Several authors estimate the solving degree through a mix of heuristic arguments and computer experiments on small examples.

One can produce rigorously proven estimates via invariants such as the degree of regularity, the first and last fall degree, and the Castelnuovo-Mumford regularity.

BOUNDING THE SOLVING DEGREE

In order to bound the security of a multivariate cryptographic scheme, we estimate the solving degree of the corresponding polynomial system.

As we cannot just compute the Gröbner basis and see in which degree the computation ends, we need a priori estimates for the solving degree.

Several authors estimate the solving degree through a mix of heuristic arguments and computer experiments on small examples.

One can produce rigorously proven estimates via invariants such as the degree of regularity, the first and last fall degree, and the Castelnuovo-Mumford regularity. Invariants may be hard to compute directly, but one can leverage a large commutative algebra literature to estimate them or even compute them via exact formulas.

DEGREE OF REGULARITY

For $f \in R$, f^{top} is the homogeneous component of largest degree of f , e.g.

$$f = x_1^2 x_3 + 2x_2^3 + x_1 x_3 - 2x_2 \rightsquigarrow f^{\text{top}} = x_1^2 x_3 + 2x_2^3.$$

To $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R$ we associate $\mathcal{F}^{\text{top}} = \{f_1^{\text{top}}, \dots, f_m^{\text{top}}\} \subseteq R$.

Definition (Bardet, Faugère, Salvy (2004))

The **degree of regularity** of $\mathcal{F}$ is

$$d_{\text{reg}}(\mathcal{F}) = \min\{\ell \in \mathbb{N} \mid (\mathcal{F}^{\text{top}})_{\ell} = R_{\ell}\},$$

where $R_{\ell} = \langle \text{monomials of deg } \ell \rangle$, $(\mathcal{F}^{\text{top}})_{\ell} = (\mathcal{F}^{\text{top}}) \cap R_{\ell}$, and $\min \emptyset = \infty$.

DEGREE OF REGULARITY

For $f \in R$, f^{top} is the homogeneous component of largest degree of f , e.g.

$$f = x_1^2 x_3 + 2x_2^3 + x_1 x_3 - 2x_2 \rightsquigarrow f^{\text{top}} = x_1^2 x_3 + 2x_2^3.$$

To $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R$ we associate $\mathcal{F}^{\text{top}} = \{f_1^{\text{top}}, \dots, f_m^{\text{top}}\} \subseteq R$.

Definition (Bardet, Faugère, Salvy (2004))

The **degree of regularity** of $\mathcal{F}$ is

$$d_{\text{reg}}(\mathcal{F}) = \min\{\ell \in \mathbb{N} \mid (\mathcal{F}^{\text{top}})_{\ell} = R_{\ell}\},$$

where $R_{\ell} = \langle \text{monomials of deg } \ell \rangle$, $(\mathcal{F}^{\text{top}})_{\ell} = (\mathcal{F}^{\text{top}}) \cap R_{\ell}$, and $\min \emptyset = \infty$.

Example

Let $\mathcal{F} = \{x_1 x_2 + x_2, x_2^2 - 1\} \subseteq K[x_1, x_2]$. Then $\mathcal{F}^{\text{top}} = \{x_1 x_2, x_2^2\}$ and $(x_1 x_2, x_2^2)_{\ell} = \langle x_1^{\ell-1} x_2, \dots, x_1 x_2^{\ell-1}, x_2^{\ell} \rangle \neq R_{\ell}$ for all $\ell \geq 2$, so $d_{\text{reg}}(\mathcal{F}) = \infty$.

EXAMPLE: EQUATIONS OF THE SAME DEGREE

Theorem (Gaggero, G. (to appear))

Assume that the LPP Conjecture holds. Let $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R$, with $f_1^{\text{top}}, \dots, f_m^{\text{top}}$ linearly independent of $\deg D$. If $m = n$, then let $k = 0$, $t = D - 1$. Else, let $1 \leq k \leq n - 1$ and $1 \leq t \leq D - 1$ be such that $m - n$ belongs to the interval $(\sigma_{k,t-1}, \sigma_{k,t}]$, where

$$\sigma_{k,t} = \sum_{i=1}^k \sum_{j=1}^{D-1} \binom{n-i-1+j}{j} - \sum_{j=t+1}^{D-1} \binom{n-k-1+j}{j} \quad \text{for } 0 \leq t \leq D-1.$$

If $d_{\text{reg}}(\mathcal{F}) < \infty$, then $d_{\text{reg}}(\mathcal{F}) \leq (D - t) + (n - k)(D - 1)$.

EXAMPLE: EQUATIONS OF THE SAME DEGREE

Theorem (Gaggero, G. (to appear))

Assume that the LPP Conjecture holds. Let $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R$, with $f_1^{\text{top}}, \dots, f_m^{\text{top}}$ linearly independent of $\deg D$. If $m = n$, then let $k = 0$, $t = D - 1$. Else, let $1 \leq k \leq n - 1$ and $1 \leq t \leq D - 1$ be such that $m - n$ belongs to the interval $(\sigma_{k,t-1}, \sigma_{k,t}]$, where

$$\sigma_{k,t} = \sum_{i=1}^k \sum_{j=1}^{D-1} \binom{n-i-1+j}{j} - \sum_{j=t+1}^{D-1} \binom{n-k-1+j}{j} \quad \text{for } 0 \leq t \leq D-1.$$

If $d_{\text{reg}}(\mathcal{F}) < \infty$, then $d_{\text{reg}}(\mathcal{F}) \leq (D - t) + (n - k)(D - 1)$.

Example

Let $n = 6$ and $D = 3$. If $m = 12$, then $d_{\text{reg}}(\mathcal{F}) \leq 11$.

If $m = 42$, then $d_{\text{reg}}(\mathcal{F}) \leq 8$. If $m = 54$, then $d_{\text{reg}}(\mathcal{F}) \leq 5$.

These bounds are tighter than the Macaulay Bound, if $m > n$.

EXAMPLE: EQUATIONS OF THE SAME DEGREE

Theorem (Gaggero, G. (to appear))

Assume that the LPP Conjecture holds. Let $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R$, with $f_1^{\text{top}}, \dots, f_m^{\text{top}}$ linearly independent of $\deg D$. If $m = n$, then let $k = 0$, $t = D - 1$. Else, let $1 \leq k \leq n - 1$ and $1 \leq t \leq D - 1$ be such that $m - n$ belongs to the interval $(\sigma_{k,t-1}, \sigma_{k,t}]$, where

$$\sigma_{k,t} = \sum_{i=1}^k \sum_{j=1}^{D-1} \binom{n-i-1+j}{j} - \sum_{j=t+1}^{D-1} \binom{n-k-1+j}{j} \quad \text{for } 0 \leq t \leq D-1.$$

If $d_{\text{reg}}(\mathcal{F}) < \infty$, then $d_{\text{reg}}(\mathcal{F}) \leq (D - t) + (n - k)(D - 1)$.

Example

Let $n = 6$ and $D = 3$. If $m = 12$, then $d_{\text{reg}}(\mathcal{F}) \leq 11$.

If $m = 42$, then $d_{\text{reg}}(\mathcal{F}) \leq 8$. If $m = 54$, then $d_{\text{reg}}(\mathcal{F}) \leq 5$.

These bounds are tighter than the Macaulay Bound, if $m > n$.

We produce a similar formula for $d_{\text{reg}}(\mathcal{F} \cup \{x_1^q - x_1, \dots, x_n^q - x_n\})$.

DEGREE OF REGULARITY AND SOLVING DEGREE

The degree of regularity has been used extensively as a proxy for the solving degree. However, until recently there was no proven connection between them.

Theorem (Semaev, Tenti (2021))

If $\mathcal{F} \supseteq \{x_1^q - x_1, \dots, x_n^q - x_n\}$ and $d_{\text{reg}}(\mathcal{F}) \geq \max\{\deg(f_1), \dots, \deg(f_m)\}$, then

$$\text{solv. deg}^s(\mathcal{F}) \leq 2d_{\text{reg}}(\mathcal{F}) - 2.$$

DEGREE OF REGULARITY AND SOLVING DEGREE

The degree of regularity has been used extensively as a proxy for the solving degree. However, until recently there was no proven connection between them.

Theorem (Semaev, Tenti (2021))

If $\mathcal{F} \supseteq \{x_1^q - x_1, \dots, x_n^q - x_n\}$ and $d_{\text{reg}}(\mathcal{F}) \geq \max\{\deg(f_1), \dots, \deg(f_m)\}$, then

$$\text{solv. deg}^s(\mathcal{F}) \leq 2d_{\text{reg}}(\mathcal{F}) - 2.$$

Theorem (Salizzoni (2025))

If $d_{\text{reg}}(\mathcal{F}) \geq \max\{\deg(f_1), \dots, \deg(f_m)\}$, then

$$\text{solv. deg}^m(\mathcal{F}) \leq d_{\text{reg}}(\mathcal{F}) + 1.$$

Both bounds are sharp.

DEGREE FALLS

$$\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R = \mathbb{F}_q[x_1, \dots, x_n], \deg(f_i) = d_i$$

Definition (Doubois, Gama (2010) – Ding, Yang (2011))

A **degree fall** occurs in **degree d** if there are $h_1, \dots, h_m \in R/(x_1^q, \dots, x_n^q)$ homogeneous of $\deg(h_i) = d - d_i$ s.t.

$$\sum_{i=1}^m h_i f_i^{\text{top}} = 0 \text{ modulo } (x_1^q, \dots, x_n^q).$$

A degree fall corresponds to a tuple $(h_1, \dots, h_m)$.

DEGREE FALLS

$$\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R = \mathbb{F}_q[x_1, \dots, x_n], \deg(f_i) = d_i$$

Definition (Doubois, Gama (2010) – Ding, Yang (2011))

A **degree fall** occurs in **degree** d if there are $h_1, \dots, h_m \in R/(x_1^q, \dots, x_n^q)$ homogeneous of $\deg(h_i) = d - d_i$ s.t.

$$\sum_{i=1}^m h_i f_i^{\text{top}} = 0 \text{ modulo } (x_1^q, \dots, x_n^q).$$

A degree fall corresponds to a tuple $(h_1, \dots, h_m)$.

This is called a degree fall since

$$\deg\left(\sum_{i=1}^m h_i f_i + \sum_{i=1}^n g_i(x_i^q - x_i)\right) < d = \deg(h_j f_j) = \deg(g_j(x_j^q - x_j))$$

for some $g_1, \dots, g_n \in R$.

TRIVIAL DEGREE FALLS AND FIRST FALL DEGREE

Trivial degree falls come from:

- $f_i^{\text{top}} f_j^{\text{top}} - f_j^{\text{top}} f_i^{\text{top}} = 0$
- $(f_i^{\text{top}})^q - f_i^{\text{top}}(x_1^q, \dots, x_n^q) = 0 \rightsquigarrow (f_i^{\text{top}})^q = 0 \text{ modulo } (x_1^q, \dots, x_n^q)$

Example

$\mathcal{F} = \{x_1 x_2 + x_2, x_2^2 - 1\} \subseteq \mathbb{F}_q[x_1, x_2]$, q odd, has $\mathcal{F}^{\text{top}} = \{x_1 x_2, x_2^2\}$.

The trivial degree falls come from $(x_2^2, -x_1 x_2)$, $((x_1 x_2)^{q-1}, 0)$, $(0, x_2^{2(q-1)})$, while $(x_2, -x_1)$, $(0, x_2^{q-2})$ give non-trivial degree falls.

TRIVIAL DEGREE FALLS AND FIRST FALL DEGREE

Trivial degree falls come from:

- $f_i^{\text{top}} f_j^{\text{top}} - f_j^{\text{top}} f_i^{\text{top}} = 0$
- $(f_i^{\text{top}})^q - f_i^{\text{top}}(x_1^q, \dots, x_n^q) = 0 \rightsquigarrow (f_i^{\text{top}})^q = 0 \text{ modulo } (x_1^q, \dots, x_n^q)$

Example

$\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1\} \subseteq \mathbb{F}_q[x_1, x_2]$, q odd, has $\mathcal{F}^{\text{top}} = \{x_1x_2, x_2^2\}$.

The trivial degree falls come from $(x_2^2, -x_1x_2)$, $((x_1x_2)^{q-1}, 0)$, $(0, x_2^{2(q-1)})$, while $(x_2, -x_1)$, $(0, x_2^{q-2})$ give non-trivial degree falls.

Definition (Doubois, Gama (2010) – Ding, Yang (2011))

The **first fall degree** of $\mathcal{F}$ is

$$d_{\text{ff}}(\mathcal{F}) = \min\{d \in \mathbb{N} \mid \text{a non-trivial degree fall occurs in } \deg d\}.$$

TRIVIAL DEGREE FALLS AND FIRST FALL DEGREE

Trivial degree falls come from:

- $f_i^{\text{top}} f_j^{\text{top}} - f_j^{\text{top}} f_i^{\text{top}} = 0$
- $(f_i^{\text{top}})^q - f_i^{\text{top}}(x_1^q, \dots, x_n^q) = 0 \rightsquigarrow (f_i^{\text{top}})^q = 0 \text{ modulo } (x_1^q, \dots, x_n^q)$

Example

$\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1\} \subseteq \mathbb{F}_q[x_1, x_2]$, q odd, has $\mathcal{F}^{\text{top}} = \{x_1x_2, x_2^2\}$.

The trivial degree falls come from $(x_2^2, -x_1x_2)$, $((x_1x_2)^{q-1}, 0)$, $(0, x_2^{2(q-1)})$, while $(x_2, -x_1)$, $(0, x_2^{q-2})$ give non-trivial degree falls. Hence $d_{\text{ff}}(\mathcal{F}) = 3$.

Definition (Doubois, Gama (2010) – Ding, Yang (2011))

The **first fall degree** of $\mathcal{F}$ is

$$d_{\text{ff}}(\mathcal{F}) = \min\{d \in \mathbb{N} \mid \text{a non-trivial degree fall occurs in } \deg d\}.$$

FIRST FALL DEGREE AND SOLVING DEGREE

- The first fall degree is heuristically used as a proxy for the solving degree.

FIRST FALL DEGREE AND SOLVING DEGREE

- The first fall degree is heuristically used as a proxy for the solving degree.
- It is often easier to compute than other invariants, as it suffices to exhibit a non-trivial degree fall to bound it from above.

FIRST FALL DEGREE AND SOLVING DEGREE

- The first fall degree is heuristically used as a proxy for the solving degree.
- It is often easier to compute than other invariants, as it suffices to exhibit a non-trivial degree fall to bound it from above.
- The first fall degree can be arbitrarily far from the solving degree.

Examples (Caminata, G. (2023))

- $\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1, x_3^{q-1} - 1, x_1^q - x_1\} \subseteq \mathbb{F}_q[x_1, x_2, x_3]$, $q \geq 4$
has $d_{\text{ff}}(\mathcal{F}) = 3 \leq q - 1 = \text{solv. deg}^m(\mathcal{F})$
- $\mathcal{F} = \{x_1^2 - 1, x_2^2 - 1\} \subseteq \mathbb{F}_q[x_1, x_2]$, q odd
has $d_{\text{ff}}(\mathcal{F}) = q \geq 2 = \text{solv. deg}^m(\mathcal{F})$

THE LAST FALL DEGREE

$$\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R = K[x_1, \dots, x_n], \quad R_{\leq d} = \langle \text{monomials of } \deg \leq d \rangle.$$

Definition (Huang, Kusters, Yang, Yeo (2015))

For $d \in \mathbb{Z}_{\geq 0}$, let $V_{\mathcal{F},d}$ be the smallest K -vector space s.t.:

- $\mathcal{F} \cap R_{\leq d} \subseteq V_{\mathcal{F},d}$,
- if $f \in V_{\mathcal{F},d}$ and $\deg(fg) \leq d$, then $fg \in V_{\mathcal{F},d}$.

THE LAST FALL DEGREE

$$\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R = K[x_1, \dots, x_n], \quad R_{\leq d} = \langle \text{monomials of } \deg \leq d \rangle.$$

Definition (Huang, Kosters, Yang, Yeo (2015))

For $d \in \mathbb{Z}_{\geq 0}$, let $V_{\mathcal{F},d}$ be the smallest K -vector space s.t.:

- $\mathcal{F} \cap R_{\leq d} \subseteq V_{\mathcal{F},d}$,
- if $f \in V_{\mathcal{F},d}$ and $\deg(fg) \leq d$, then $fg \in V_{\mathcal{F},d}$.

The last fall degree was introduced to measure the complexity of a specific algorithm to compute the solutions of a polynomial system.

Definition

The **last fall degree** of $\mathcal{F}$ is

$$d_{\text{lf}}(\mathcal{F}) = \min\{d \in \mathbb{N} \mid f \in V_{\mathcal{F}, \max\{d, \deg(f)\}} \text{ for all } f \in (\mathcal{F})\}.$$

HKYY prove that $d_{\text{lf}}(\mathcal{F}) < \infty$.

EXAMPLES

Example

$\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1\}$ has $V_{\mathcal{F},0} = V_{\mathcal{F},1} = 0$, $V_{\mathcal{F},2} = \langle x_1x_2 + x_2, x_2^2 - 1 \rangle$.

EXAMPLES

Example

$\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1\}$ has $V_{\mathcal{F},0} = V_{\mathcal{F},1} = 0$, $V_{\mathcal{F},2} = \langle x_1x_2 + x_2, x_2^2 - 1 \rangle$.

Since $x_1 + 1 = x_2(x_1x_2 + x_2) - (x_1 + 1)(x_2^2 - 1) \in V_{\mathcal{F},3}$,

then $(x_1 + 1)f \in V_{\mathcal{F},3}$ for all $f \in R_{\leq 2}$, hence

$$V_{\mathcal{F},3} = V_{\mathcal{F},2} + x_1 V_{\mathcal{F},2} + x_2 V_{\mathcal{F},2} + (x_1 + 1)R_{\leq 2}$$

and $d_{\text{lf}}(\mathcal{F}) = 3$.

EXAMPLES

Example

$\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1\}$ has $V_{\mathcal{F},0} = V_{\mathcal{F},1} = 0$, $V_{\mathcal{F},2} = \langle x_1x_2 + x_2, x_2^2 - 1 \rangle$.
Since $x_1 + 1 = x_2(x_1x_2 + x_2) - (x_1 + 1)(x_2^2 - 1) \in V_{\mathcal{F},3}$,
then $(x_1 + 1)f \in V_{\mathcal{F},3}$ for all $f \in R_{\leq 2}$, hence

$$V_{\mathcal{F},3} = V_{\mathcal{F},2} + x_1 V_{\mathcal{F},2} + x_2 V_{\mathcal{F},2} + (x_1 + 1)R_{\leq 2}$$

and $d_{\text{lf}}(\mathcal{F}) = 3$.

Example

If $\mathcal{F}$ is homogeneous, then $d_{\text{lf}}(\mathcal{F}) = 0$.

LAST FALL DEGREE, DEGREE OF REGULARITY, AND SOLVING DEGREE

Remark (G., Müller, Petit (2022)): $V_{\mathcal{F},d}$ is the rowspace of the Macaulay matrix of degree d after running a mutant algorithm.

LAST FALL DEGREE, DEGREE OF REGULARITY, AND SOLVING DEGREE

Remark (G., Müller, Petit (2022)): $V_{\mathcal{F},d}$ is the rowspace of the Macaulay matrix of degree d after running a mutant algorithm.

Theorem (G., Müller, Petit (2022) – Caminata, G. (2023))

$$\text{solv. deg}^m(\mathcal{F}) = \max\{d_{\text{lf}}(\mathcal{F}), \text{max. GB. deg}(\mathcal{F})\}$$

LAST FALL DEGREE, DEGREE OF REGULARITY, AND SOLVING DEGREE

Remark (G., Müller, Petit (2022)): $V_{\mathcal{F},d}$ is the rowspace of the Macaulay matrix of degree d after running a mutant algorithm.

Theorem (G., Müller, Petit (2022) – Caminata, G. (2023))

$$\text{solv. deg}^m(\mathcal{F}) = \max\{d_{\text{lf}}(\mathcal{F}), \max. \text{GB. deg}(\mathcal{F})\}$$

Corollary (GMP (2022), CG (2023), S (2025))

$$d_{\text{lf}}(\mathcal{F}) \leq d_{\text{reg}}(\mathcal{F}) + 1$$

The last fall degree is often the hardest invariant to compute.

THE LAST FALL DEGREE OF HFE

Hidden Fields Equations (HFE) was proposed by Patarin (1996)

$$Q(x) \in \mathbb{F}_{q^n}[x] \longleftrightarrow \mathcal{Q} = \{q_1, \dots, q_n\} \subseteq \mathbb{F}_q[x_1, \dots, x_n]$$

Theorem (G., Müller, Petit (2022))

The last fall degree of an HFE system $\mathcal{Q}$ over $\mathbb{F}_q$ with $\deg(Q) \leq D$ is

$$d_{\text{lf}}(\mathcal{Q}) \leq (q-1)(\lceil \log_q D \rceil + 1) + 1.$$

If in addition $\mathcal{Q}$ has at most $(q-1)(\lceil \log_q D \rceil + 1) + 1$ solutions, then

$$\text{solv. deg}^m(\mathcal{Q}) \leq (q-1)(\lceil \log_q D \rceil + 1) + 1.$$

This theorem yields the tightest proven estimate on the last fall degree and solving degree of HFE. It matches the experimental result by Faugere and Joux (2003) and the heuristic result by Ding and Hodges (2011) up to a factor two.

CONCLUSIONS

- The solving degree allows us to bound from above the complexity of computing Gröbner bases, hence of solving polynomial systems.

CONCLUSIONS

- The solving degree allows us to bound from above the complexity of computing Gröbner bases, hence of solving polynomial systems.
- Algebraic invariants provide a priori estimates on the solving degree.

CONCLUSIONS

- The solving degree allows us to bound from above the complexity of computing Gröbner bases, hence of solving polynomial systems.
- Algebraic invariants provide a priori estimates on the solving degree.
- The first fall degree is often the easiest to compute, but it only provides a heuristic estimate (which can be arbitrarily far from the solving degree).

CONCLUSIONS

- The solving degree allows us to bound from above the complexity of computing Gröbner bases, hence of solving polynomial systems.
- Algebraic invariants provide a priori estimates on the solving degree.
- The first fall degree is often the easiest to compute, but it only provides a heuristic estimate (which can be arbitrarily far from the solving degree).
- The degree of regularity and the last fall degree are often harder to compute, but they produce proven estimates.

CONCLUSIONS

- The solving degree allows us to bound from above the complexity of computing Gröbner bases, hence of solving polynomial systems.
- Algebraic invariants provide a priori estimates on the solving degree.
- The first fall degree is often the easiest to compute, but it only provides a heuristic estimate (which can be arbitrarily far from the solving degree).
- The degree of regularity and the last fall degree are often harder to compute, but they produce proven estimates.

Thank you for your attention!