Complexity of Gröbner bases computations and applications to cryptography

Elisa Gorla

Institut de mathématiques, Université de Neuchâtel

Journées nationales de calcul formel
March 2, 2021

Solving degree

$\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R = K[x_1, \ldots, x_n]$, degree reverse lexicographic order

Definition

The solving degree of $\mathcal{F}$, denoted $\mathrm{solv.deg}(\mathcal{F})$, is the least degree for which Gaussian elimination in the drl Macaulay matrix of degree d yields a Gröbner basis of $(\mathcal{F}) = (f_1, \ldots, f_m)$.
$\mathrm{max.GB.deg}(\mathcal{F})$ denotes the largest degree of a polynomial in a reduced drl Gröbner basis of $(\mathcal{F})$.

Solving degree

$\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R = K[x_1, \ldots, x_n]$, degree reverse lexicographic order

Definition

The solving degree of $\mathcal{F}$, denoted $\mathrm{solv.deg}(\mathcal{F})$, is the least degree for which Gaussian elimination in the drl Macaulay matrix of degree d yields a Gröbner basis of $(\mathcal{F}) = (f_1, \ldots, f_m)$.
$\mathrm{max.GB.deg}(\mathcal{F})$ denotes the largest degree of a polynomial in a reduced drl Gröbner basis of $(\mathcal{F})$.

Theorem (Caminata, G.)

Suppose that $(\mathcal{F}^h)$ is in generic coordinates, then

$$\mathrm{reg}(\mathcal{F}^h) \geq \mathrm{solv.deg}(\mathcal{F}) \geq \mathrm{max.GB.deg}(\mathcal{F})$$

where $\mathrm{reg}(\mathcal{F}^h)$ is the Castelnuovo-Mumford regularity of $(\mathcal{F}^h)$.

The Castelnuovo-Mumford regularity

$J = (F_1, \ldots, F_m)$, $F_i \in S = K[x_0, \ldots, x_n]$ homogeneous of $\deg(F_i) = d_i$

$$0 \to \bigoplus_{i=1}^{\ell_p} S(-b_{p,i}) \to \cdots \to \bigoplus_{i=1}^{\ell_1} S(-b_{1,i}) \to \bigoplus_{i=1}^{m} S(-d_i) \xrightarrow{(F_1,\ldots,F_m)} J \to 0$$

Definition

The Castelnuovo-Mumford regularity of J is $\mathrm{reg}(J) = \max\{b_{j,i} - j, d_i\}$.

The Castelnuovo-Mumford regularity

$J = (F_1, \dots, F_m)$, $F_i \in S = K[x_0, \dots, x_n]$ homogeneous of $\deg(F_i) = d_i$

$$0 \to \bigoplus_{i=1}^{\ell_p} S(-b_{p,i}) \to \cdots \to \bigoplus_{i=1}^{\ell_1} S(-b_{1,i}) \to \bigoplus_{i=1}^{m} S(-d_i) \xrightarrow{(F_1,\dots,F_m)} J \to 0$$

Definition

The Castelnuovo-Mumford regularity of J is $\mathrm{reg}(J) = \max\{b_{j,i} - j, d_i\}$.

Example

$J = (x_1^2, x_1x_2, x_2^3) \subseteq K[x_0, x_1, x_2]$ has minimal free resolution

$$0 \to S(-4) \oplus S(-3) \to S(-3) \oplus S(-2)^2 \to J \to 0$$

and $\mathrm{reg}(J) = \max\{2, 3, 3-1, 4-1\} = 3$.

A bound for the complexity of MinRank

MinRank Problem

Given $M_1, \ldots, M_n, N \in \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ and $r < \min\{k, m\}$, find $x_1, \ldots, x_n \in \mathbb{F}_q$ s.t.

$$\mathrm{rank}\left(N - \sum_{i=1}^{n} x_i M_i\right) \leq r.$$

A bound for the complexity of MinRank

Generalized MinRank Problem

Given $M \in \mathrm{Mat}_{k\times m}(K[x_1,\ldots,x_n])$ and $r < \min\{k,m\}$, find $x_1,\ldots,x_n \in K$ s.t.

$$\mathrm{rank}\,(M) \leq r.$$

A bound for the complexity of MinRank

Generalized MinRank Problem

Given $M \in \mathrm{Mat}_{k\times m}(K[x_1,\dots,x_n])$ and $r < \min\{k,m\}$, find $x_1,\dots,x_n \in K$ s.t.

$$\mathrm{rank}\,(M) \leq r.$$

The next result was shown by Faugère, Safey El Din, and Spaenlehauer for $d_{ij} = d \geq 1$.

Theorem (Caminata, G.)

Let $M \in \mathrm{Mat}_{k\times m}(R)$, let $r < k \leq m$ and $n \geq (m-r)(k-r)$.
Assume that the entries of M are generic of degree d_{ij} with $d_{ij} > 0$ and $d_{ij} + d_{h\ell} = d_{i\ell} + d_{hj}$ for all i, j, h, ℓ.
Let $\mathcal{F}$ be the homogeneous polynomial system of the minors of size $r+1$ of M.
Then

$$\mathrm{solv.deg}(\mathcal{F}) \leq (m-r)\sum_{i=1}^{r} d_{i,i} + \sum_{i=r+1}^{k}\sum_{j=r+1}^{m} d_{ij} - (m-r)(k-r) + 1.$$

Algebra and geometry

K field, $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R = K[x_1, \ldots, x_n]$, $I = (\mathcal{F})$

Definition

The affine variety associated to I is

$$V(I) = \{P = (x_1, \ldots, x_n) \in K^n \mid f_1(P) = \ldots = f_m(P) = 0\} \subseteq K^n.$$

Algebra and geometry

K field, $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R = K[x_1, \ldots, x_n]$, $I = (\mathcal{F})$

Definition

The affine variety associated to I is

$$V(I) = \{P = (x_1, \ldots, x_n) \in K^n \mid f_1(P) = \ldots = f_m(P) = 0\} \subseteq K^n.$$

Theorem (Hilbert's Nullstellensatz)

If $K = \overline{K}$, then we have a one-to-one correspondence between radical ideals and affine varieties.

Algebra and geometry

K field, $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R = K[x_1, \ldots, x_n]$, $I = (\mathcal{F})$

Definition

The affine variety associated to I is

$$V(I) = \{P = (x_1, \ldots, x_n) \in K^n \mid f_1(P) = \ldots = f_m(P) = 0\} \subseteq K^n.$$

Theorem (Hilbert's Nullstellensatz)

If $K = \overline{K}$, then we have a one-to-one correspondence between radical ideals and affine varieties.

Affine varieties in K^n are the closed sets of the Zarisky topology on K^n.

If $K = \mathbb{F}_q$, then the Zarisky topology is the discrete topology.

If K is infinite, then any $\emptyset \neq U \subseteq K^n$ open is dense, i.e. $\overline{U} = K^n$.

Genericity

Definition

A property is generic if it holds on a nonempty Zarisky-open set.
A polynomials of degree d in n variables is generic if it belong to a given Zarisky-open set of $K^{\binom{n+d}{d}}$.
A sequence of polynomials is generic if each polynomial is generic.

Genericity

Definition

A property is generic if it holds on a nonempty Zarisky-open set.
A polynomials of degree d in n variables is generic if it belong to a given Zarisky-open set of $K^{\binom{n+d}{d}}$.
A sequence of polynomials is generic if each polynomial is generic.

Over a finite field this is meaningless, but over an infinite field this means that the property holds "almost everywhere".

Genericity

Definition

A property is generic if it holds on a nonempty Zarisky-open set.
A polynomials of degree d in n variables is generic if it belong to a given Zarisky-open set of $K^{\binom{n+d}{d}}$.
A sequence of polynomials is generic if each polynomial is generic.

Over a finite field this is meaningless, but over an infinite field this means that the property holds "almost everywhere". However, when one can describe the open set via the equations of its complement, then one can check whether any given point belongs to the open set.

Example

Genericity conditions for the statement on the complexity of MinRank:

- the homogenization of the minors of M are the minors of the matrix obtained from M by homogenizing its entries,
- the zero locus of the minors has codimension $(m-r)(k-r)$.

Ideals in generic coordinates

K infinite, $S = K[x_0, \dots, x_n]$, fix the drl order, $J \subseteq S$ homogeneous
$G = \mathrm{GL}_{n+1}(K)$ acts on S as changes of coordinates

Theorem (Galligo)

There is a nonempty open $U \subseteq G \subseteq K^{(n+1)^2}$ *s.t.* $\mathrm{in}(gJ) = \mathrm{in}(hJ)$ *for* $g, h \in U$*.*

Definition

$\mathrm{gin}(J) := \mathrm{in}(gJ)$ for $g \in U$ is the (drl) generic initial ideal of J.

Ideals in generic coordinates

K infinite, $S = K[x_0, \ldots, x_n]$, fix the drl order, $J \subseteq S$ homogeneous
$G = \mathrm{GL}_{n+1}(K)$ acts on S as changes of coordinates

Theorem (Galligo)

There is a nonempty open $U \subseteq G \subseteq K^{(n+1)^2}$ s.t. $\mathrm{in}(gJ) = \mathrm{in}(hJ)$ for $g, h \in U$.

Definition

$\mathrm{gin}(J) := \mathrm{in}(gJ)$ for $g \in U$ is the (drl) generic initial ideal of J.

Theorem (Bayer, Stillman)

One has

$$\mathrm{reg}(J) = \mathrm{reg}(\mathrm{gin}(J)).$$

Hence, if J is in generic coordinates, then

$$\mathrm{reg}(J) = \mathrm{reg}(\mathrm{in}(J)).$$

Are we in generic coordinates?

One can decide if J is in generic coordinates by computing a Gröbner basis.

Are we in generic coordinates?

One can decide if J is in generic coordinates by computing a Gröbner basis.

Theorem (Caminata, G.)

$\mathcal{F} \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$. Assume that

$$x_1^q - x_1, \ldots, x_n^q - x_n \in \mathcal{F} \quad \text{or} \quad x_1^q - x_2, \ldots, x_{n-1}^q - x_n, x_n^q - x_1 \in \mathcal{F}.$$

Then $(\mathcal{F}^h)$ is in generic coordinates.

Corollary (Macaulay Bound)

$\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R = \mathbb{F}_q[x_1, \ldots, x_n]$, $\deg(f_i) = d_i$, $d_1 \geq \ldots \geq d_m$, $m \geq n+1$. *Assume that $(\mathcal{F}^h)$ is in generic coordinates, or that $\mathcal{F}$ contains the field equations, or their fake Weil descent. Then*

$$\operatorname{solv.deg}(\mathcal{F}) \leq d_1 + \ldots + d_{n+1} - n.$$

Invariants related to the solving degree

In addition to the Castelnuovo-Mumford regularity, other invariants of systems of polynomial equations may help estimating the solving degree:

- the degree of regularity d_{reg},
- the first fall degree d_{ff},
- the last fall degree d_{lf},
- the witness degree d_{wit}.

Homogeneous systems associated to $\mathcal{F}$

$\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R \rightsquigarrow \mathcal{F}^h = \{f_1^h, \ldots, f_m^h\} \subseteq S = R[x_0]$ and $\mathcal{F}^{\text{top}} = \{f_1^{\text{top}}, \ldots, f_m^{\text{top}}\} \subseteq R$ homogeneous.

Definition

The top degree part of $f = \sum_{a \in \mathbb{N}^n} \alpha_a x^a \in K[x_1, \ldots, x_n]$ is

$$f^{\text{top}} = \sum_{|a| = \deg(f)} \alpha_a x^a,$$

where $|a| = a_1 + \ldots + a_n = \deg(x^a)$.

Example

Let $\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1\} \subseteq K[x_1, x_2]$. Then

$\mathcal{F}^{\text{top}} = \{x_1x_2, x_2^2\} \subseteq K[x_1, x_2], \mathcal{F}^h = \{x_1x_2 + x_0x_2, x_2^2 - x_0^2\} \subseteq K[x_0, x_1, x_2]$.

Homogeneous systems associated to $\mathcal{F}$

$\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R \quad \rightsquigarrow \quad \mathcal{F}^h = \{f_1^h, \ldots, f_m^h\} \subseteq S = R[x_0]$ and $\mathcal{F}^{\text{top}} = \{f_1^{\text{top}}, \ldots, f_m^{\text{top}}\} \subseteq R$ homogeneous.

Definition

The top degree part of $f = \sum_{a \in \mathbb{N}^n} \alpha_a x^a \in K[x_1, \ldots, x_n]$ is

$$f^{\text{top}} = \sum_{|a| = \deg(f)} \alpha_a x^a,$$

where $|a| = a_1 + \ldots + a_n = \deg(x^a)$.

Example

Let $\mathcal{F} = \{x_1 x_2 + x_2, x_2^2 - 1\} \subseteq K[x_1, x_2]$. Then

$\mathcal{F}^{\text{top}} = \{x_1 x_2, x_2^2\} \subseteq K[x_1, x_2], \mathcal{F}^h = \{x_1 x_2 + x_0 x_2, x_2^2 - x_0^2\} \subseteq K[x_0, x_1, x_2]$.

If $f_1, \ldots, f_m$ are homogeneous, then $\mathcal{F} = \mathcal{F}^h = \mathcal{F}^{\text{top}}$.

Degree of regularity and solving degree

Definition (Bardet, Faugère, Salvy)

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

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

Since $\mathrm{in}(\mathcal{F})_\ell \supseteq \mathrm{in}(\mathcal{F}^{\mathrm{top}})_\ell = R_\ell$ for $\ell \geq d_{\mathrm{reg}}(\mathcal{F})$, then

$$d_{\mathrm{reg}}(\mathcal{F}) \geq \max.\mathrm{GB}.\deg(\mathcal{F}).$$

Degree of regularity and solving degree

Definition (Bardet, Faugère, Salvy)

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

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

Since $\mathrm{in}(\mathcal{F})_\ell \supseteq \mathrm{in}(\mathcal{F}^{\mathrm{top}})_\ell = R_\ell$ for $\ell \geq d_{\mathrm{reg}}(\mathcal{F})$, then

$$d_{\mathrm{reg}}(\mathcal{F}) \geq \max.\mathrm{GB}.\deg(\mathcal{F}).$$

Example

Let $\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1\} \subseteq K[x_1, x_2]$. Then $\mathcal{F}^{\mathrm{top}} = \{x_1x_2, x_2^2\}$ and $(x_1x_2, x_2^2)_\ell = \langle x_1^{\ell-1}x_2, \ldots, x_1x_2^{\ell-1}, x_2^\ell\rangle \neq R_\ell$ for all $\ell \geq 2$, so $d_{\mathrm{reg}}(\mathcal{F}) = \infty$.

Degree of regularity and solving degree

Definition (Bardet, Faugère, Salvy)

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

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

Since $\mathrm{in}(\mathcal{F})_\ell \supseteq \mathrm{in}(\mathcal{F}^{\mathrm{top}})_\ell = R_\ell$ for $\ell \geq d_{\mathrm{reg}}(\mathcal{F})$, then

$$d_{\mathrm{reg}}(\mathcal{F}) \geq \max.\mathrm{GB}.\deg(\mathcal{F}).$$

Example

Let $\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1\} \subseteq K[x_1, x_2]$. Then $\mathcal{F}^{\mathrm{top}} = \{x_1x_2, x_2^2\}$ and $(x_1x_2, x_2^2)_\ell = \langle x_1^{\ell-1}x_2, \ldots, x_1x_2^{\ell-1}, x_2^\ell\rangle \neq R_\ell$ for all $\ell \geq 2$, so $d_{\mathrm{reg}}(\mathcal{F}) = \infty$.

If $\mathcal{F}$ is homogeneous, then $d_{\mathrm{reg}}(\mathcal{F}) = \mathrm{reg}(\mathcal{F})$ if $\mathcal{F}$ has the unique solution $x_1 = \ldots = x_n = 0$. Else $d_{\mathrm{reg}}(\mathcal{F}) = \infty$.

EXAMPLES

Example (Caminata, G.)

Let $f_1, f_2, f_3 \in R := \mathbb{F}_q[x, y]$ of degrees 7,7,8 be a polynomial system for collecting relations for index calculus on elliptic curves over $\mathbb{F}_{q^3}$.
For 150'000 randomly generated examples of cryptographic size (3 different q's, 5 elliptic curves for each q, 10'000 random points per curve)

$$(\mathcal{F}^{\text{top}})_\ell \neq R_\ell \text{ for all } \ell \geq 0 \quad \text{and} \quad \text{solv.deg}(\mathcal{F}) = 15.$$

Examples

Example (Caminata, G.)

Let $f_1, f_2, f_3 \in R := \mathbb{F}_q[x, y]$ of degrees 7,7,8 be a polynomial system for collecting relations for index calculus on elliptic curves over $\mathbb{F}_{q^3}$.
For 150'000 randomly generated examples of cryptographic size (3 different q's, 5 elliptic curves for each q, 10'000 random points per curve)

$$(\mathcal{F}^{\text{top}})_\ell \neq R_\ell \text{ for all } \ell \geq 0 \quad \text{and} \quad \text{solv.deg}(\mathcal{F}) = 15.$$

The degree of regularity may be smaller than the solving degree.

Example (Caminata, G.)

Let $f_1, f_2, f_3 \in R := \mathbb{F}_q[x, y]$ of degree 3 be a polynomial system for collecting relations for index calculus on elliptic curves over $\mathbb{F}_{q^3}$.
For 150'000 randomly generated examples of cryptographic size as above

$$\text{solv.deg}(\mathcal{F}) = 5 > 4 = d_{\text{reg}}(\mathcal{F}).$$

Another example

The gap btwn the solving degree and the degree of regularity can be large.

Example (Bigdeli, De Negri, Dizdarevic, G., Minko, Tsakou)

Let $f_1 = x^5 + y^5 + z^5 - 1, f_2 = x^3 + y^3 + z^2 - 1, f_3 = y^6 - 1, f_4 = z^6 - 1 \in R = \mathbb{F}_7[x, y, z]$. Let

$$\mathcal{F} := \left\{ \prod_{j=1}^{3} f_{i_j} \,\middle|\, 1 \leq i_1 \leq i_2 \leq i_3 \leq 4 \right\} \cup \{x^7 - x, y^7 - y, z^7 - z\}.$$

Using Magma one can compute

$$\text{solv. deg}(\mathcal{F}) = 24 > 15 = d_{\text{reg}}(\mathcal{F}).$$

- The solving degree is computed with Magma.
- $\mathcal{F}$ contains equations of degree $18 > 15 = d_{\text{reg}}(\mathcal{F})$.

Degree falls

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

Definition (Doubois, Gama – Ding, Yang)

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

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

$(h_1, \ldots, h_m)$ is a syzygy of $f_1^{\text{top}}, \ldots, f_m^{\text{top}}$ modulo $(x_1^q, \ldots, x_n^q)$.

This is called a degree fall since

$$\deg\left(\sum_{i=1}^m h_i f_i\right) < d = \deg(h_j f_j) \text{ for all } j.$$

Trivial degree falls and first fall degree

Trivial degree falls and corresponding trivial syzygies come from:

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

Example

$\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1\} \subseteq \mathbb{F}_q[x_1, x_2]$, $q \geq 3$, has $\mathcal{F}^{\text{top}} = \{x_1x_2, x_2^2\}$.

The trivial syzygies of $\mathcal{F}^{\text{top}}$ are $\langle (x_2^2, -x_1x_2), ((x_1x_2)^{q-1}, 0), (0, x_2^{2(q-1)}) \rangle$, while $(x_2, -x_1), (0, x_2^{q-2})$ are non-trivial syzygies.

Trivial degree falls and first fall degree

Trivial degree falls and corresponding trivial syzygies come from:

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

Example

$\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1\} \subseteq \mathbb{F}_q[x_1, x_2]$, $q \geq 3$, has $\mathcal{F}^{\text{top}} = \{x_1x_2, x_2^2\}$.

The trivial syzygies of $\mathcal{F}^{\text{top}}$ are $\langle (x_2^2, -x_1x_2), ((x_1x_2)^{q-1}, 0), (0, x_2^{2(q-1)}) \rangle$, while $(x_2, -x_1), (0, x_2^{q-2})$ are non-trivial syzygies.

Definition

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

$$
\begin{aligned}
d_{\text{ff}}(\mathcal{F}) &= \min\{d \in \mathbb{N} \mid \text{a non-trivial degree fall occurs in } \deg d\} \\
&= \min\{d \in \mathbb{N} \mid \text{there is a non-trivial syzygy of } \deg d\}
\end{aligned}
$$

Trivial degree falls and first fall degree

Trivial degree falls and corresponding trivial syzygies come from:

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

Example

$\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1\} \subseteq \mathbb{F}_q[x_1, x_2]$, $q \geq 3$, has $\mathcal{F}^{\text{top}} = \{x_1x_2, x_2^2\}$.

The trivial syzygies of $\mathcal{F}^{\text{top}}$ are $\langle (x_2^2, -x_1x_2), ((x_1x_2)^{q-1}, 0), (0, x_2^{2(q-1)}) \rangle$, while $(x_2, -x_1), (0, x_2^{q-2})$ are non-trivial syzygies. Hence $d_{\text{ff}}(\mathcal{F}) = 3$.

Definition

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

$$\begin{aligned} d_{\text{ff}}(\mathcal{F}) &= \min\{d \in \mathbb{N} \mid \text{a non-trivial degree fall occurs in } \deg d\} \\ &= \min\{d \in \mathbb{N} \mid \text{there is a non-trivial syzygy of } \deg d\} \end{aligned}$$

First fall degree and solving degree

Example

$\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1, x_1^{q-1} - 1\} \subseteq \mathbb{F}_q[x_1, x_2]$ has $\mathcal{F}^{\mathrm{top}} = \{x_1x_2, x_2^2, x_1^{q-1}\}$, with non-trivial syzygies $(x_2, -x_1, 0), (x_1^{q-2}, 0, -x_2), (0, x_2^{q-2}, 0), (0, 0, x_1)$. Hence

$$d_{\mathrm{ff}}(\mathcal{F}) = 3 \leq q - 1 = \mathrm{solv.deg}(\mathcal{F}).$$

First fall degree and solving degree

Example

$\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1, x_1^{q-1} - 1\} \subseteq \mathbb{F}_q[x_1, x_2]$ has $\mathcal{F}^{\mathrm{top}} = \{x_1x_2, x_2^2, x_1^{q-1}\}$, with non-trivial syzygies $(x_2, -x_1, 0), (x_1^{q-2}, 0, -x_2), (0, x_2^{q-2}, 0), (0, 0, x_1)$. Hence

$$d_{\mathrm{ff}}(\mathcal{F}) = 3 \leq q - 1 = \mathrm{solv.deg}(\mathcal{F}).$$

Example

$\mathcal{F} = \{x_1 + x_2, x_2^2 - 1\} \subseteq \mathbb{F}_q[x_1, x_2]$, $q \geq 3$ has $\mathcal{F}^{\mathrm{top}} = \{x_1, x_2^2\}$.
The trivial syzygies of x_1, x_2^2 are $\langle (x_2^2, -x_1), (x_1^{q-1}, 0), (0, x_2^{2(q-1)}) \rangle$.
The only non-trivial syzygy is $(0, x_2^{q-2})$. Hence

$$d_{\mathrm{ff}}(\mathcal{F}) = q > 2 = \mathrm{solv.deg}(\mathcal{F}).$$

The last fall degree

$\mathcal{F} \subseteq R = K[x_1, \ldots, x_n]$

Definition (Huang, Kosters, Yang, Yeo)

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

The last fall degree

$\mathcal{F} \subseteq R = K[x_1, \ldots, x_n]$

Definition (Huang, Kosters, Yang, Yeo)

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

Definition

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

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

The last fall degree

$\mathcal{F} \subseteq R = K[x_1, \ldots, x_n]$

Definition (Huang, Kosters, Yang, Yeo)

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

Definition

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

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

If $\mathcal{F}$ is homogeneous, then $V_{\mathcal{F},d} = (\mathcal{F})_{\leq d}$ for all $d \in \mathbb{N}$ and $d_{\mathrm{lf}}(\mathcal{F}) = 0$.

Example and properties

Example

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

$$V_{\mathcal{F},3} = V_{\mathcal{F},2} + x_1V_{\mathcal{F},2} + x_2V_{\mathcal{F},2} + (x_1+1)R_{\leq 2} = (\mathcal{F})_{\leq 3}.$$

Then $d_{\mathrm{lf}}(\mathcal{F}) = 3 = \mathrm{solv.deg}(\mathcal{F})$.

Example and properties

Example

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

$$V_{\mathcal{F},3} = V_{\mathcal{F},2} + x_1V_{\mathcal{F},2} + x_2V_{\mathcal{F},2} + (x_1+1)R_{\leq 2} = (\mathcal{F})_{\leq 3}.$$

Then $d_{\mathrm{lf}}(\mathcal{F}) = 3 = \mathrm{solv.deg}(\mathcal{F})$.

Algorithm (Huang, Kosters, Yang, Yeo)

Assume that $\mathcal{F}$ has finitely many solutions. There is a linear algebra based algorithm which computes the solutions of $\mathcal{F}$ and whose complexity is upper bounded by an exponential function of $d_{\mathrm{lf}}(\mathcal{F})$.

This is only meaningful for non-homogeneous systems.

Last fall degree and solving degree

Unlike the solving degree, the last fall degree is independent of the choice of a degree-compatible term order and of coordinate changes.

Last fall degree and solving degree

Unlike the solving degree, the last fall degree is independent of the choice of a degree-compatible term order and of coordinate changes.

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

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

Last fall degree and solving degree

Unlike the solving degree, the last fall degree is independent of the choice of a degree-compatible term order and of coordinate changes.

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

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

If $\mathcal{F}$ is homogeneous, then $d_{\mathrm{lf}}(\mathcal{F}) = 0$ and we recover that $\mathrm{solv.deg}(\mathcal{F}) = \mathrm{max.GB.deg}(\mathcal{F})$.

The witness degree

Let $K = \mathbb{F}_2$ and $\mathcal{F} = \{f_1, \ldots, f_{m-n}, x_1^2 + x_1, \ldots, x_n^2 + x_n\}$, $\deg(f_i) = d_i$

$I = (\mathcal{F})$, $I_{\leq d} = \{f \in I : \deg(f) \leq d\}$, $R_{\leq d} = \langle x^a : |a| \leq d \rangle$

$W_{\leq d} = \{\sum_{i=1}^{m-n} h_i f_i + \sum_{i=1}^{n} \ell_i (x_i^2 + x_i),\ h_i \in R_{\leq d-d_i},\ \ell_i \in R_{\leq d-2}\}$

Definition (Bardet, Faugère, Salvy, Spaenlehauer)

The witness degree of $\mathcal{F}$ is the least d s.t. $W_{\leq d} = I_{\leq d}$ and $\max.\mathrm{GB}.\deg(\mathcal{F}) \leq d$

$$d_{\mathrm{wit}}(\mathcal{F}) = \max\{\min\{d \in \mathbb{N} \mid W_{\leq d} = I_{\leq d}\}, \max.\mathrm{GB}.\deg(\mathcal{F})\}.$$

Wintess degree, regularity, and solving degree

Wintess degree, regularity, and solving degree

Theorem (Bardet, Faugère, Salvy, Spaenlehauer)

If $\mathcal{F}$ has no solutions, then

$$d_{\text{wit}}(\mathcal{F}) \leq d_{\text{reg}}(\mathcal{F}^h) = \text{reg}(\mathcal{F}^h).$$

Wintess degree, regularity, and solving degree

Theorem (Bardet, Faugère, Salvy, Spaenlehauer)

If $\mathcal{F}$ has no solutions, then

$$d_{\mathrm{wit}}(\mathcal{F}) \leq d_{\mathrm{reg}}(\mathcal{F}^h) = \mathrm{reg}(\mathcal{F}^h).$$

Example

$\mathcal{F} = \{x_1x_2 + x_2, x_1^2 + 1, x_2^2 + 1\}$ has max. GB. $\deg(\mathcal{F}) = 2$ and
$W_0 = W_1 = 0,\ W_2 = \langle x_1x_2 + x_2, x_1^2 + 1, x_2^2 + 1\rangle$ and

$$W_3 = W_2 + x_1 W_2 + x_2 W_2 + \langle x_1 + 1\rangle \subsetneq (\mathcal{F})_{\leq 3}.$$

Then $d_{\mathrm{wit}}(\mathcal{F}) > 3 = \mathrm{solv.}\deg(\mathcal{F})$.

Summarizing

- the degree of regularity is an upper bound for the largest degree of an element in a drl Gröbner basis,
- the degree of regularity and the first fall degree are heuristic estimates for the solving degree,
- the last fall degree and the largest degree of an element in the reduced Gröbner basis of $\mathcal{F}$ together determine the solving degree,
- the witness degree is a lower bound on the degree of regularity and on the Castenuovo-Mumford regularity of $\mathcal{F}^h$, for a system $\mathcal{F}$ that has no solutions.

Hilbert series and regular sequences

$J \subseteq S = K[x_0, \dots, x_n]$ homogeneous,

Definition

The Hilbert series of S/J is the formal power series

$$HS_{S/J}(z) = \sum_{d \geq 0} \dim_k(S_d/J_d) z^d.$$

Hilbert series and regular sequences

$J \subseteq S = K[x_0, \ldots, x_n]$ homogeneous, $\mathcal{F} = \{f_1, \ldots, f_m\}$, $d_i = \deg(f_i)$

Definition

The Hilbert series of S/J is the formal power series

$$HS_{S/J}(z) = \sum_{d \geq 0} \dim_k(S_d/J_d) z^d.$$

Definition

$f_1^h, \ldots, f_m^h$ is a regular sequence if multiplication by f_i^h is injective modulo $(f_1^h, \ldots, f_{i-1}^h)$ for all i. Equivalently, if

$$HS_{S/(\mathcal{F}^h)}(z) = \frac{\prod_{i=1}^m (1 - z^{d_i})}{(1-z)^{n+1}}$$

Regular sequences only exist for $m \leq n + 1$.

Regular and semiregular sequences

$\mathcal{F} = \{f_1, \ldots, f_m\}$, $d_i = \deg(f_i)$, for $h(z) \in \mathbb{Z}[[z]]$ let

$$[h(z)] := \sum_{d=0}^{\Delta} h_d z^d, \text{ where } \Delta = \sup\{d \geq 0 \mid h_0, \ldots, h_d > 0\}.$$

Definition (Pardue – Bardet, Faugère, Salvy – Bigdeli, De Negri, Dizdarevic, G., Minko, Tsakou)

$\mathcal{F}$ is a (cryptographic) semiregular sequence if

$$HS_{S/(\mathcal{F}^h)}(z) = \left[\frac{\prod_{i=1}^{m}(1 - z^{d_i})}{(1 - z)^{n+1}} \right]$$

Regular and semiregular sequences

$\mathcal{F} = \{f_1, \ldots, f_m\}$, $d_i = \deg(f_i)$, for $h(z) \in \mathbb{Z}[[z]]$ let

$$[h(z)] := \sum_{d=0}^{\Delta} h_d z^d, \text{ where } \Delta = \sup\{d \geq 0 \mid h_0, \ldots, h_d > 0\}.$$

Definition (Pardue – Bardet, Faugère, Salvy – Bigdeli, De Negri, Dizdarevic, G., Minko, Tsakou)

$\mathcal{F}$ is a (cryptographic) semiregular sequence if

$$HS_{S/(\mathcal{F}^h)}(z) = \left[\frac{\prod_{i=1}^{m}(1 - z^{d_i})}{(1-z)^{n+1}}\right]$$

Example

- $x_0^{d_0}, x_1^{d_1}, \ldots, x_n^{d_n}$ is a regular sequence in $K[x_0, \ldots, x_n]$
- x^2, xy, y^2 is a semiregular sequence in $k[x,y]$, since

$$\left[\frac{(1-z^2)^3}{(1-z)^2}\right] = [(1+z)^2(1-z^2)] = [1+2z-2z^3-z^4] = 1+2z = HS_{K[x,y]/(x^2,xy,y^2)}(z)$$

Are random sequences (semi)regular?

Many authors define a random system as one where the coefficients are chosen uniformly at random in the ground field.

Are random sequences (semi)regular?

Many authors define a random system as one where the coefficients are chosen uniformly at random in the ground field.

Conjecture (Pardue)

Semiregular sequences over an infinite field are generic, i.e., semiregular sequences form a dense open subset of the set of all sequences of given degrees $d_1, \dots, d_m$, wrt the Zariski topology.

There is evidence in favor of Pardue's Conjecture and the equivalent Fröberg's Conjecture. E.g., they are true for regular sequences.
Over an infinite field, genericity is the right formulation of randomness.

Are random sequences (semi)regular?

Many authors define a random system as one where the coefficients are chosen uniformly at random in the ground field.

Conjecture (Pardue)

Semiregular sequences over an infinite field are generic, i.e., semiregular sequences form a dense open subset of the set of all sequences of given degrees $d_1, \ldots, d_m$, wrt the Zariski topology.

There is evidence in favor of Pardue's Conjecture and the equivalent Fröberg's Conjecture. E.g., they are true for regular sequences.
Over an infinite field, genericity is the right formulation of randomness.

Over a finite field, genericity makes no sense, as the Zariski topology is the discrete topology.
The case of $\mathbb{F}_2$ was studied by Hodges, Molinas, Schlather. They provide mixed evidence. Other finite fields have not yet been studied.

Castelnuovo-Mumford regularity of semiregular sequences

For a semiregular sequence

$$\mathrm{reg}(\mathcal{F}^h) = d_{\mathrm{reg}}(\mathcal{F}^h)$$

so in principle it can be computed via

$$HS_{S/(\mathcal{F}^h)}(z) = \left[\frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^{n+1}} \right]$$

Example

$n=2,\ m=5,\ d_1=\ldots=d_5=2,\ \mathcal{F}$ semiregular

$$HS_{S/(\mathcal{F}^h)}(z) = \left[\frac{(1-z^2)^5}{(1-z)^3} \right] = [1+3z+z^2-5z^3+\ldots] = 1+3z+z^2$$

hence $\mathrm{solv.deg}(\mathcal{F}) \leq \mathrm{reg}(\mathcal{F}^h) = 3$, if $\mathcal{F}^h$ is in generic coordinates.

Solving degree of semiregular sequences

Asymptotic formulas for $m = n + c$ and $m = cn$, for $n \to \infty$, were given by Bardet, Faugère, Salvy.

$\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R = K[x_1, \ldots, x_n]$, $\deg(f_i) = d_i$, $d_1 \leq \ldots \leq d_m$
$\mathcal{F}$ semiregular sequence, $\mathcal{F}^h \subseteq S = K[x_0, \ldots, x_n]$ in generic coordinates

If $m = n, n+1$, then $\operatorname{solv.deg}(\mathcal{F}) \leq d_1 + \ldots + d_m - m + 1.$

Theorem (Bigdeli, De Negri, Dizdarevic, G., Minko, Tsakou)

Let $m \geq n+2$. Assume wlog $d_{n+2} \leq d_1 + \cdots + d_{n+1} - n - 1$. Then

$$\operatorname{solv.deg}(\mathcal{F}) \leq \left\lfloor \frac{d_1 + \cdots + d_{n+2} - n - 2}{2} \right\rfloor + 1.$$

In particular, if $d_1 = \cdots = d_{n+2} = d$, then

$$\operatorname{solv.deg}(\mathcal{F}) \leq \left\lfloor \frac{(d-1)n}{2} \right\rfloor + d.$$

Solving degree of semiregular sequences

$\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R = K[x_1, \ldots, x_n]$, $\deg(f_i) = d_i$, $d_1 = \ldots = d_m = 2$
$\mathcal{F}$ semiregular sequence, $\mathcal{F}^h \subseteq S = K[x_0, \ldots, x_n]$ in generic coordinates

Theorem (Bigdeli, De Negri, Dizdarevic, G., Minko, Tsakou)

$$\text{solv.}\deg(\mathcal{F}) \leq \begin{cases} \lfloor n/2 \rfloor + 2 & \text{if } m = n+2, \\ \lceil (5 + n - \sqrt{5+n})/2 \rceil & \text{if } m = n+3, \\ \lceil (7 + n - \sqrt{19+3n})/2 \rceil & \text{if } m = n+4, \\ \left\lceil (9 + n - \sqrt{23 + 3n + \sqrt{2}\sqrt{170 + 45n + 3n^2}})/2 \right\rceil & \text{if } m = n+5, \\ \left\lceil (11 + n - \sqrt{45 + 5n + \sqrt{2}\sqrt{368 + 85n + 5n^2}})/2 \right\rceil & \text{if } m \geq n+6. \end{cases}$$

Generic sequences of quadrics

$\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R = K[x_1, \ldots, x_n]$, $\deg(f_i) = 2$
$\mathcal{F}^h \subseteq S = K[x_0, \ldots, x_n]$ contains a regular sequence of $n+1$ quadratic polynomials, $\mathcal{F}^h$ in generic coordinates.

We use a famous conjecture by Eisenbud, Green, Harris on the Hilbert series of an ideal containing a regular sequence of homogeneous quadratic polynomials.

Generic sequences of quadrics

$\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R = K[x_1, \dots, x_n]$, $\deg(f_i) = 2$
$\mathcal{F}^h \subseteq S = K[x_0, \dots, x_n]$ contains a regular sequence of $n+1$ quadratic polynomials, $\mathcal{F}^h$ in generic coordinates.

Theorem (Bigdeli, De Negri, Dizdarevic, G., Minko, Tsakou)

Assume that the EGH Conjecture holds. Let α be the unique integer such that $\sum_{i=n+1-\alpha}^{n+1} i < m \leq \sum_{i=n-\alpha}^{n+1} i$. Then

$$\operatorname{solv.deg}(\mathcal{F}) \leq n + 1 - \alpha.$$

Example

- $n = 2$, $m = 5$: $\alpha = 0$ since $3 < m \leq 3 + 2$, hence $\operatorname{solv.deg}(\mathcal{F}) \leq 3$,
- $n = 100$, $m = 600$, $\alpha = 5$ since

$101 + 100 + 99 + 98 + 97 + 96 < m \leq 101 + 100 + 99 + 98 + 97 + 96 + 95$, hence $\operatorname{solv.deg}(\mathcal{F}) \leq 96$.

References:

- M. Bardet, *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et a la cryptographie*
- M. Bardet, J. C. Faugère, B. Salvy, P. J. Spaenlehauer, *On the complexity of solving quadratic boolean systems*
- M. Bardet, J. C. Faugère, B. Salvy, B. Y. Yang, *Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems*
- D. Bayer, M. Stillman, *A criterion for detecting m-regularity*
- M. Bigdeli, M. M. Dizdarevic, E. De Negri, E. Gorla, R. Minko, S. Tsakou, *Semi-regular sequences and other random systems of equations*
- A. Caminata, E. Gorla, *Solving multivariate polynomial systems and an invariant from commutative algebra*
- A. Caminata, E. Gorla, *The complexity of MinRank*
- A. Caminata, E. Gorla, *Last fall degree and solving degree*, upcoming
- J. Ding, B. Y. Yang, *Degree of regularity for HFEv and HFEv-*
- D. Eisenbud, M. Green, J. Harris, *Higher Castelnuovo Theory*
- J. C. Faugère, P. Gianni, D. Lazard, T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*
- A. Galligo, *A propos du théorème de préparation de Weierstrass*
- E. Gorla, C. Petit, D. Müller, *Stronger bounds on the cost of computing Gröbner bases for HFE systems*
- V. Dubois, N. Gama, *The degree of regularity of HFE systems*
- T. J. Hodges, S. D. Molina, J. Schlather, *On the existence of semi-regular sequences*
- M. D. Huang, M. Kosters, Y. Yang, S. L. Yeo *On the last fall degree of zero-dimensional Weil descent systems*
- D. Lazard, *Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations*
- K. Pardue, *Generic sequences of polynomials*