Structured Polynomial Systems in Cryptography

Jean-Charles Faugère
Cryptography: assess the security

**Public key cryptography**: security rely on the difficulty of solving a difficult mathematical problem

- Number theory: e.g. elliptic curve, integer factorization

  **Quantum Computer**
  Serious threat: NIST competition

- Other problems:
  - Code Based Crypto
  - Multivariate Crypto
  - Lattice Based Crypto
  - ...

  **Algebraic Cryptanalysis**:
  - Model the problem with algebraic equations
  - Evaluate the practical/theoretical complexity
PoSSo Problem: find a solution of

\[
\begin{cases}
  f_1(X_1, \ldots, X_n) = 0 \\
  \quad \ldots \\
  f_m(X_1, \ldots, X_n) = 0
\end{cases}
\]

\[ f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n] \text{ finite field} \]

Goal: find all the solutions / exact methods

- Resultants
- Border Bases
- Triangular Sets
- SAT solvers

This talk: Gröbner bases
PoSSo Problem: find a solution of

\[
\begin{aligned}
f_1(X_1,\ldots,X_n) &= 0 \\
\cdots \\
f_m(X_1,\ldots,X_n) &= 0
\end{aligned}
\]

\[f_1,\ldots,f_m \in \mathbb{F}_q[X_1,\ldots,X_n]\] finite field

Problem coming from crypto:

- over \textbf{finite fields} $\mathbb{F}_q$
- \textbf{large number of variables}: $> 80$
- \textbf{structured systems}: symmetries, determinantal eqs, multi-homogeneity, sparse, overdetermined, …
- need to evaluate \textbf{precisely} the complexity: Hilbert Series, …

NP-hard problem even over $\mathbb{F}_2$

However …
Non toy problems can be solved with **Gröbner** bases

- [Crypto 2003] HFE Challenge broken using Gröbner bases: 80 dense equations and 80 variables over $F_2$

- [Eurocrypt 2006] Polynomial Equivalence Problems: system with 506 unknowns and 12696 quadratic equations


- [Crypto 2008] 9 variables only but dense equations of degree 9 and the size of the input file was 3.4 Gbytes / the number of solutions was 259545.

**Why** it was possible to compute the corresponding Gröbner bases?
Gröbner bases: algorithms overview

Buchberger
Critical Pairs Algorithm

F4 algorithm
Rely heavily on sparse linear algebra

F5 / Signature based algorithm
Build full rank matrices
Complexity = Hilbert Series

Macaulay/Sylvester
Linear Algebra
Need a bound

We know explicitly trivial syzygies:
\[ f_j f_i - f_i f_j \]
or \[ f_i \cdot f_i - f_i \]

Predict \( \text{LM} \ GB([f_1, \ldots, f_k]) \)
Polynomial System Solving: finite number of solutions

\[ f_1 = \ldots = f_m = 0 \]

Gaussian Elimination of matrices up to degree \( d_{\text{max}} \)

\[ O \left( \left( \frac{n + d_{\text{max}}}{n} \right)^{\omega} \right) \]

Linear Algebra in \( \mathbb{K}[x]/I \)

\[ x_i = h_i(x_n) \]

\( \tilde{O}(\#\text{Sols}^\omega) \)

GB Complexity driven by the maximal degree reached: \( d_{\text{max}} \)

Gröbner: total degree

- Buchberger (1965)
- F4
- F5
- Signature based

Gröbner: lexicographical

\( \tilde{O}(\#\text{Sols}) \)

Factorization
Bounding the maximal degree

**Prop.** For $n$ regular equations of degree $d_i$ in $\mathbb{K}[x_1,\ldots,x_n]$:

Macaulay Bound: 
\[
d_{\text{max}} = 1 + \sum_{i=1}^{n} (d_i - 1) \quad \text{[Lazard, Giusti]}
\]
\[
d_{\text{max}} = n + 1 \quad \text{(quadratic eqs)}
\]

**Prop.** For $m = \alpha n$

semi-regular quadratic

equations in $\mathbb{K}[x_1,\ldots,x_n]$:
\[
d_{\text{max}} \approx (\alpha - \frac{1}{2} - \sqrt{\alpha(\alpha - 1)})n \quad \text{[Bardet, F., Salvy]}
\]
Bounding the maximal degree - Elliptic Curve

Elliptic curve over $\mathbb{F}_{q^n}$

Group Law:

$$(x_1, y_1) \oplus (x_2, y_2) \mapsto (F_x, F_y)$$ - rational functions

Decomposition Problem:

$R \in E(\mathbb{F}_{q^n})$: find $P_1, \ldots, P_n$ such that $R = P_1 \oplus \ldots \oplus P_n$

$I$ ideal generated by the equations

Then $I \cap \mathbb{F}_{q^n}[x_1, \ldots, x_n] = \langle S_n(x_1, \ldots, x_n) \rangle$

$S_n(x_1, \ldots, x_n)$ symmetric polynomial (Semaev): $S_n(e_1, \ldots, e_n)$

If we impose $x_i \in \mathbb{F}_q$, then $e_i \in \mathbb{F}_q$

$S_n(e_1, \ldots, e_n) = 0 \longrightarrow S_{n,1}(e_1, \ldots, e_n) = \cdots = S_{n,n}(e_1, \ldots, e_n) = 0$ (in $\mathbb{F}_q$)

Zero-dimensional problem
Bounding the maximal degree - Elliptic Curve

Edwards curve over $\mathbb{F}_{q^n}
\begin{equation*}
ax^2 + y^2 = 1 + dx^2y^2
\end{equation*}
[Bernstein, Lange]

LEX Gröbner basis:

\[
\begin{align*}
e_1 + h_1(e_{n-1}, e_n) \\
e_2 + h_2(e_{n-1}, e_n) \\
&\vdots \\
e_{n-2} + h_{n-2}(e_{n-1}, e_n) \\
h_{n-1}(e_{n-1}, e_n) \\
h_n(e_n)
\end{align*}
\]

with $\deg(h_n) = 2^{(n-1)^2}$ and $\deg_{e_{n-1}}(h_{n-1}) = 2^{n-1}$

2-torsion point $T_2$: $2T_2 = T_2 \oplus T_2 = 0$

Action on the points (geometry)

\[
R = P_1 \oplus P_2 \oplus \cdots \oplus P_n = (P_1 \oplus T_2) \oplus (P_2 \oplus T_2) \oplus \cdots \oplus P_n = 0
\]

For an even number of $T_2$
Bounding the maximal degree - Elliptic Curve

Coxeter Group $D_n$:

$$ S_n(y_1, \ldots, y_n) \in \mathbb{F}_q[y_1, \ldots, y_n]^{D_n} = \mathbb{F}_q[E_1, \ldots, E_{n-1}, e_n] $$

where $E_i = e_i(y_1^2, \ldots, y_n^2)$ the $i^{th}$ elementary symmetric polynomial.

**LEX Gröbner** basis:

\[
\begin{align*}
E_1 + h_1(e_n) \\
E_2 + h_2(e_n) \\
& \vdots \\
E_{n-1} + h_{n-1}(e_n) \\
h_n(e_n) \text{ of degree } 2^{(n-1)^2}
\end{align*}
\]

For instance, when $n=5$ deg $I = 1048576 \rightarrow 65536$ (NIST -IPSEC- Oakley)
Bounding the maximal degree - Elliptic Curve

For instance, when $n=5$ $\deg I = 1048576 \rightarrow 65536$

Is it enough to understand the complexity? $d_{\text{max}}$?

Very far from a regular sequence!
Bounding the maximal degree - Elliptic Curve

For instance, when \( n=5 \) \( \deg I = 1048576 \rightarrow 65536 \)

Put weight on the variables: \( w_i \leftarrow x_i \) (Quasi-homogeneous system)

\[
d_{\text{max}} \leq \sum_{i=1}^{n} (d_i - w_i) + \max\{w_j\}
\]

Complexity divided by \((\prod_i w_i)^3\)

[Safey el Din, Verron, F, 2016]

\[
w = (1,1,\ldots,1)\\
w = (2,2,2,2,1)
\]
Real computation: DLP challenge

Elliptic curve: $xy + y^2 - x^3 = cste$ over $\mathbb{F}_{2^{4\times 29}} = \mathbb{F}_{2^{116}}$
Cardinal of the group: $20769187434139310549529495610151239 \approx 2^{114}$

Index Calculus:

**Phase 1**: Harvesting (decomposition problem):
Need to compute $72 \times 10^9$ Gröbner bases (each computation $0.7/0.9$ msec)
Total time to generate the matrix: $\approx 14$ days

**Phase 2**: Linear Algebra
Sparse matrix of size: $748 \times 10^6 \times 134 \times 10^6$
computation: JG Dumas, C Pernet, P Giorgi, C Bouvier
Multivariate Problem - Minrank

**Multivariate** crypto: HFE Problem (Hidden field equation)

public key is a system of \( n \) dense/quadratic equations in \( n \) variables over \( \mathbb{F}_q \)

By **construction** the number of variables in the system is **artificial**.

\[
\begin{align*}
\text{Initial System} & \quad S \times \mathbb{F}(T \times X) \quad \text{Public Key}
\end{align*}
\]

**MinVar Problem**: **Reduce the number of variables**

Can we find a linear combination of the equations and a linear change of variables to decrease the number of variables?

**Minrank Problem**

\[ f_i \text{ matrix representation } Q_i \]

Find \( \lambda_i \) s.t. \( \text{rank}\left(\sum \lambda_i Q_i\right) = r < n \)
Multivariate Problem - Minrank

Minrank Problem

Find $\lambda_i$ s.t. $\text{rank}(M) = r < n$ where $M = \sum \lambda_i Q_i$

Equations (Minors):
rank of all the $(r+1)$-minors of $M$ are 0

Explicit Hilbert series of the ideal of the $(r+1)$-minors of a matrix of variables
A. Conca and J. Herzog 1994

Kernel Equations:
find $n-r$ vectors in the kernel

$$M \times \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ \vdots & \vdots & \vdots \end{bmatrix} = 0$$

Bilinear equations in $(\lambda_i)$ and $(a_i, b_i, \ldots)$
Bilinear systems

\[ f_i = \sum a_{i,j} x_i y_j = 0 \] with \( X = \{x_0, \ldots, x_{n_x}\} \) and \( Y = \{y_0, \ldots, y_{n_y}\} \)

**First task:** find trivial syzygies:

\[
\begin{bmatrix}
  s_1 & \cdots & s_n
\end{bmatrix}
\begin{bmatrix}
  x_0 \\
  \vdots \\
  x_{n_x}
\end{bmatrix}
= 0 \quad \text{(Euler relation)}
\]
Bilinear systems

\[ f_i = \sum a_{i,j} x_i y_j = 0 \] with \( X = \{x_0, \ldots, x_n\} \) and \( Y = \{y_0, \ldots, y_n\} \)

**First task:** find trivial syzygies:

\[
\begin{bmatrix}
    s_1 & \ldots & s_n
\end{bmatrix} \in \text{Ker}_L \text{Jac}_X(F)
\]
Bilinear systems

\[ f_i = \sum a_{i,j} x_i y_j = 0 \] with \( X = \{x_0, \ldots, x_{n_x}\} \) and \( Y = \{y_0, \ldots, y_{n_y}\} \)

**First task:** find trivial syzygies:

\[
\begin{bmatrix}
s_1 & \ldots & s_n
\end{bmatrix} \in \text{Ker}_L \text{Jac}_X(F)
\]

\[
J = \begin{pmatrix}
a_1 & a_2 \\
b_1 & b_2 \\
c_1 & c_2
\end{pmatrix}
\]

then

\[
\begin{vmatrix}
a_1 & a_2 & a_i \\
b_1 & b_2 & b_i \\
c_1 & c_2 & c_i
\end{vmatrix} = 0 \text{ (for } i = 1, 2)\]

\[
s_1 = \begin{vmatrix}
b_1 & c_1 \\
b_2 & c_2
\end{vmatrix}, \quad s_2 = -\begin{vmatrix}
a_1 & c_1 \\
a_2 & c_2
\end{vmatrix}, \quad s_3 = \begin{vmatrix}
a_1 & b_1 \\
a_2 & b_2
\end{vmatrix}
\]
Bilinear systems

\[ f_i = \sum a_{i,j} x_i y_j = 0 \] with \( X = \{ x_0, \ldots, x_{n_x} \} \) and \( Y = \{ y_0, \ldots, y_{n_y} \} \)

Thanks to the Euler relation we can predict the syzygies:

\[
\begin{vmatrix} f_i & f_j \\ f_i & f_j \end{vmatrix} = 0 \quad i \neq j, \quad \begin{vmatrix} f_1 & f_2 & f_3 \\ \frac{\partial f_1}{\partial x_0} & \frac{\partial f_2}{\partial x_0} & \frac{\partial f_3}{\partial x_0} \\ \frac{\partial f_1}{\partial x_1} & \frac{\partial f_2}{\partial x_1} & \frac{\partial f_3}{\partial x_1} \end{vmatrix} = 0, \quad \begin{vmatrix} f_1 & f_2 & f_3 \\ \frac{\partial f_1}{\partial y_j} \end{vmatrix} = 0
\]

**F_5**: to avoid them we need the GB of the maximal minors of \( \text{Jac}_x(F) \)

**Theorem** Bernstein, Sturmfels and Zelevinski

\( M \) a \( p \times q \) matrix whose entries are variables. For any monomial ordering, maximal minors of \( M \) are a universal Gröbner basis of the associated ideal.
**Bilinear systems**

\[ f_i = \sum a_{i,j} x_i y_j = 0 \] with \( X = \{ x_0, \ldots, x_n \} \) and \( Y = \{ y_0, \ldots, y_n \} \)

Thanks to the Euler relation we can **predict** the syzygies:

\[
\begin{vmatrix}
  f_i & f_j \\
  f_i & f_j \\
\end{vmatrix} = 0 \quad i \neq j,
\]

\[
\begin{vmatrix}
  f_1 & f_2 & f_3 \\
  \frac{\partial f_1}{\partial x_0} & \frac{\partial f_2}{\partial x_0} & \frac{\partial f_3}{\partial x_0} \\
  \frac{\partial f_1}{\partial x_1} & \frac{\partial f_2}{\partial x_1} & \frac{\partial f_3}{\partial x_1} \\
\end{vmatrix} = 0,
\]

\[
\begin{vmatrix}
  f_1 & f_2 & f_3 \\
  \frac{\partial f_i}{\partial y_j} \\
\end{vmatrix} = 0
\]

**F<sub>5</sub> : to avoid them** we need the GB of the maximal minors of \( \text{Jac}_X(F) \)

**Theorem**

\( M \) a \( p \times q \) **matrix** whose entries linear forms. For any monomial ordering, **maximal minors** of \( M \) are a **grevlex** Gröbner basis of the associated ideal.
Bilinear systems

\[ f_i = \sum a_{i,j} x_i y_j = 0 \] with \( X = \{ x_0, \ldots, x_{n_x} \} \) and \( Y = \{ y_0, \ldots, y_{n_y} \} \)

**In the affine case**, no reduction to 0

**Complexity** F. Safey El Din, Spaenlehauer

**Degree of regularity** of a generic 0-dim **affine** bilinear system for the grevlex ordering:

\[ d_{\text{reg}} \leq 2 + \min(n_x, n_y). \]

Resultant approach: Emiris, Mantzaflaris, Tsigaridas

- Can solve the system in **polynomial time** in the number of solutions
- Can solve the system in **polynomial time** if \( n_x \) is fixed

**DLP - Finite Fields:**

Joux \( L(1/4 + o(1)) \) algorithm

GB are used in DLP challenges

Ad hoc method

Multihomogeneous case?
NTRU Problem (field version)

Given $h(X) \in \mathbb{F}_q[X]$ of degree $n$, find $f(X), g(X)$ with coefficients 0 or 1

$$h(x) = \frac{f(X)}{g(X)} \mod X^n - 1$$

Equations:

$G(X) = \sum x_i X^i$ then $F(X) = G(X) h(X) \mod X^n - 1$

Equations:

$$\begin{cases} 
F_i^2 - F_i \text{ where } F_i = \text{coeff}(F, X^i) \\
x_i^2 - x_i
\end{cases}$$

$I$ the ideal is **globally invariant** by the action of $G = C_n$

$\sigma Eq_i \rightarrow Eq_{i+1}$ where $\sigma = (1, 2, \ldots, n)$
Abelian Group action

Example: $\mathbb{F}_{521}[X]$

$$f = -145 (y_1^2 + y_2^3 + y_3^4 + y_4^2 + y_5^2) + 30 (y_1 y_2 + y_2 y_3 + y_3 y_4 + y_4 y_1) - 79 (y_1 y_3 + y_2 y_4 + y_3 y_1 + y_4 y_2) - 34 (y_1 + y_2 + y_3 + y_4 + y_5) + 370$$

We diagonalize the group:

$$\sigma = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{find } Q \text{ s.t. } Q \sigma Q^{-1} = \begin{bmatrix} w & 0 & 0 & 0 & 0 \\ 0 & w^2 & 0 & 0 & 0 \\ 0 & 0 & w^3 & 0 & 0 \\ 0 & 0 & 0 & w^4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

where $w^5 = 1$.

New variables

$$y_1 \quad y_2 \quad y_3 \quad y_4 \quad y_5 = Q^{-1} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$$

$$\sigma f = f \rightarrow 32 x_1 x_4 + 487 x_2 x_3 + 378 x_5^2 + 487 x_5 + 370$$

Define a new grading: $\Gamma(x_1^{\alpha_1} x_2^{\alpha_2} \cdots) = \alpha_1 + 2\alpha_2 + \cdots \mod n$
Abelian Group action

Non symmetric example: \( \mathbb{F}_{521}[X] \)

\[
f = -145y_1^2 + 30y_1y_2 - 79y_1y_3 - 79y_1y_4 + 30y_1y_5 - 145y_2^2 + 30y_2y_3 - 79y_2y_4 - 79y_2y_5 - 145y_3^2 + 30y_3y_4 - 79y_3y_5 - 145y_4^2 + 30y_4y_5 - 145y_5^2 - 34y_1 - 34y_2 - 34y_3 - 34y_4 - 34y_5 + 370
\]

New variables

\[
\begin{bmatrix}
y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5
\end{bmatrix} = Q^{-1}
\begin{bmatrix}
x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4
\end{bmatrix}
\]

\[
f \rightarrow 319x_1x_4 + 410x_2x_3 + 284x_5^2 + 410x_5 + 74 + 97x_1x_5 + 89x_2x_4 + 341x_3^2 + 514x_1
\]

\[
+ 351x_1^2 + 494x_2x_3 + 111x_3x_4 + 353x_2 + 249x_1x_2 + 282x_3x_5 + 134x_4^2 + 178x_3
\]

\[
+ 192x_1x_3 + 7x_2^2 + 195x_4x_5 + 114x_4
\]

\((f, \sigma f, \sigma^2 f, \ldots) \rightarrow \text{Split } f \text{ in 5 small components}\)

[F., Svartz, F, 2013]

Complexity divided by \(|G|^2\)

when \(G\) is an abelian group.
Abelian Group action

Non symmetric example: $\mathbb{F}_{5^{21}}[X]$

Support of the polynomials: monomials $x_i x_j$ s.t. $i + j = \text{cste} \mod 5$

$f \rightarrow \begin{align*}
319x_1x_4 + 410x_2x_3 + 284x_5^2 + 410x_5 + 74 + 97x_1x_5 + 89x_2x_4 + 341x_3^2 + 514x_1 \\
+ 351x_1^2 + 494x_2x_5 + 111x_3x_4 + 353x_2 + 249x_1x_2 + 282x_3x_5 + 134x_4^2 + 178x_3 \\
+ 192x_1x_3 + 7x_2^2 + 195x_4x_5 + 114x_4
\end{align*}
\equiv 0, 1, 2, 3, 4 \mod 5

(f, \sigma f, \sigma^2 f, ...) \rightarrow \text{Split } f \text{ in 5 small components}

[F., Svartz, F, 2013]

Complexity divided by $|G|^2$

when $G$ is an abelian group.

Can we use the sparsity?
Unified approach: Sparse Gröbner Bases

**Sparse Systems**: classical theme in Polynomial System Solving

Toric geometry during the 70s/80s: toric (or sparse) elimination theory.

**Resultants**: The sparse structure and the connection with toric geometry have also been incorporated to the theory of resultants
   Canny, D’Andrea, Dickenstein, Emiris, Kriek, Tsigaridas, …

**Polyhedral homotopy methods**: Huber, Sturmfels, Sottile, …

**Gröbner bases for sparse systems**: Cifuentes, Parrilo, Sturmfels, …
   In particular, computational aspects of toric geometry and Gröbner bases are investigated in [Sturmfels].

**Sparse effective Nullstellensatze**: Rojas, Sombra, …
Unified approach: Sparse Gröbner Basis

Unified approach based on monomial sparsity

- Consider only monomials in the initial Support: polytope $\mathcal{P}$
- Multiply these monomials $\sim 2\mathcal{P} = \{u \times v \mid (u, v) \in \mathcal{P}^2\}$
Sparse Gröbner Basis: keep the initial support!

Convex Case

\[ f = c_0 + c_1 x + c_2 xy + c_3 x^2 + c_4 x^2 y + c_5 x^2 y^2 \]

Monomials of degree 1:
\[ M_1 = \text{Support}(f) \]

Monomials of degree 2:
\[ M_2 = \{ u \times v \mid (u, v) \in M_1 \times M_1 \} \]

…

Monomials of degree d:
\[ M_d = \{ u \times v \mid (u, v) \in M_{d-1} \times M_1 \} \]

Non Convex Case

\[ f = c_0 + c_1 x^2 + c_2 xy + c_3 y^2 \]

Macaulay Matrix in degree d

\[
M_d = \begin{pmatrix}
t_{1,1} f_1 & \cdots & \\
t_{1,2} f_1 & \cdots & \\
\vdots & \cdots & \\
t_{2,1} f_2 & \cdots & \\
\vdots & \cdots & \\
\end{pmatrix}
\]

all products \( t f_i, t \in M_{d-\deg(f_i)} \)
Sparse Gröbner Basis: keep the initial support!

Convex Case

\[ f = c_0 + c_1 x + c_2 xy + c_3 x^2 + c_4 x^2 y + c_5 x^2 y^2 \]

Non Convex Case

\[ f = c_0 + c_1 x^2 + c_2 xy + c_3 y^2 \]

Goal

- dedicated algorithm
- complexity? \( d_{\text{max}} \) ?
- Hilbert Series?
Unified approach: Sparse Gröbner Basis

Unified approach based on monomial sparsity

- Consider only monomials in the initial Support: polytope $\mathcal{P}$
- Multiply these monomials $\leadsto 2\mathcal{P} = \{u \times v \mid (u, v) \in \mathcal{P}^2\}$

$\mathcal{P}$: initial Support

$2\mathcal{P}$

$3\mathcal{P}$

New Unified Approach: Sparse Gröbner bases

- New $F_5$ and FGLM Algorithms.
- New view on the design of GB Algorithms.
- New representation of the sols

Complexity in the convex case + regularity assumptions

$\max d_i \leq n + 2 - F(\mathcal{P}) + \sum (d_i - 1)$

where $F(\mathcal{P}) = \min \{k \mid \text{interior}(k \cdot \mathcal{P}) \cap \mathbb{N}^n \neq \emptyset\}$

combinatorial properties of $\mathcal{P}$

[F., Spaenlehauer, Svartz 2014]
Example: multilinear equations

\[ \sum a_{i,j,k,\ldots} x_i y_j z_k \cdots \]

\[ f = \sum c_{\alpha_1,\ldots,\alpha_l} x^{\alpha_1} y^{\alpha_2} z^{\alpha_3} \ldots \]

Newton polytope: \( \mathcal{P} = \Delta_{n_1} \times \cdots \times \Delta_{n_\ell} \)
where \( \Delta_j \) is the standard simplex

\( \beta(\Delta_{n_1} \times \cdots \times \Delta_{n_\ell}) \) has an interior point iff for all \( i, \beta \Delta_{n_i} \) has an interior point.

\( \alpha \Delta_n \) has an interior point if \( \alpha > n \).

\[ F(\mathcal{P}) = 1 + \max(n_1, \ldots, n_\ell). \]

\[ d_{\text{max}} \leq n + 2 - F(\mathcal{P}) = n + 1 - \max(n_1, \ldots, n_\ell) \]

Hilbert series: \( HS(t) = \sum \frac{(n_1^{-1}) \cdots (n_\ell^{-1}) t^d}{(1-t)} \)
Applications

Bilinear systems \((X,Y)\):

remove automatically all syzygies

\[
d_{\text{max}} \leq n_X + n_Y + 1 - \max(n_X, n_Y) = 1 + \min(n_X, n_Y)
\]

Multihomogeneous \((X_1, \ldots, X_\ell)\) of degree \((d_1, \ldots, d_\ell)\)

\[
d_{\text{max}} \leq n + 2 - \max_{i \in \{1, \ldots, \ell\}} \left(\left\lceil \frac{n_{X_i} + 1}{d_i} \right\rceil \right)
\]
Application to McEliece (Code based crypto)

An alternate code $A_t(x,y)$ is the kernel of

$$H_t(x,y) = \begin{pmatrix}
y_0 & y_1 & \cdots & y_{n-1} \\
y_0x_0 & y_1x_1 & \cdots & y_{n-1}x_{n-1} \\
\vdots & \vdots & \ddots & \vdots \\
y_0x_0^{t-1} & y_1x_1^{t-1} & \cdots & y_{n-1}x_{n-1}^{t-1}
\end{pmatrix}$$

Polynomial system:
Given a public matrix $G = (g_{i,j})$
then $H_t(X,Y)G^T = 0$

$$\begin{cases}g_{i,0}Y_0X_0^j + \ldots + g_{i,n-1}Y_{n-1}X_{n-1}^j = 0, \text{ with } 0 \leq i < k \text{ and } 0 \leq j < t\end{cases}$$

[$\text{McEliece, 1978}$] # variables $\approx 2048$, # equations $\approx 26200$

Abnormal behavior of the computation (Hilbert series)

Goppa Code Distinguishing problem: distinguishing the matrix of a Goppa code from a random matrix

polynomial-time algorithm (high-rate codes)

[$\text{Gauthier-Umanã, Otmani, Perret, Tillich}$]
The non convex case

\[
\left\{
\begin{align*}
    f_1(X_1,\ldots,X_n) &= 0 \\
    \vdots \\
    f_m(X_1,\ldots,X_n) &= 0
\end{align*}
\right.
\]

such that \( f_1,\ldots,f_m \in \mathbb{K}[X_1,\ldots,X_n] \) and random monomial support \( M \supset \{1\} \) of size \( n+k+1 \), degree 2.

Compute explicit representations of the solutions, or certify that there are none via the Nullstellensatz:

\[
M \ni f_i = \sum_{t \in M} c_t t \\
\text{c_t \text{ generic coefficients}}
\]

Problem

\[
\sum_{i=1}^{m} f_i g_i = 1
\]

Complexity: link with graph theory (see also [Cifuentes,Parrilo])
**The non convex case**

**M** subset of monomials of degree \( \leq 2 \)

**Theorem**

\( \nu(M) \) the matching number of the graph associated to **M**.

\((f_1, \ldots, f_m)\) \( n \) variables with support **M** and **generic coefficients**:

If \( m \geq |M| - \frac{\sqrt{1+8\nu(M)}-1}{2} \), the following sparse certificate can be computed in polynomial time:

\[
\sum_{i=1}^{m} f_i \, h_i = 1 \quad \text{with } h_i \in M
\]

**Example**

Let \( M = \{1, x_1^2, x_2^2, x_3^2, x_3, x_4, x_1x_2, x_2x_3, x_3x_4\} \).

**Graph G:**

Vertices \( S = \{x_0 = 1\} \cup \{x_1, \ldots, x_n\} \)

Edges \( E = \{(i, j) \mid x_i \, x_j \in M, \, i \neq j\} \)

**Example**

Let \( M = \{1, x_1^2, x_2^2, x_3^2, x_3, x_4, x_1x_2, x_2x_3, x_3x_4\} \).

**Graph G:**

\( \nu(M) = 2 \)
How often it is true?

\[ \text{Theorem} \]

**M** is distributed uniformly at random (and contain the constant 1)

\[ \#M = n + k + 1 \text{ where } k \text{ is a constant} \]

If \( \#\{x_i^2 \in M\} = \Omega(n^\beta) \), for \( \beta > \frac{1}{2} \), then the probability that

\[ m \geq |M| - \frac{\sqrt{1 + 8\nu(M)} - 1}{2} \]

tends towards 1 as \( n \) grows.

[F., Spaenlehauer, Svartz 2016]
Probability of success

Conjecture: probability of success is not 0 even for a random system

\[ \#M \text{ of size } n+2 \text{ and } S_n = \left\lfloor n^\beta \right\rfloor \]
Can solve systems with > 60000 variables

# M of size $n+2$ and $\# \text{squares} = \left\lfloor n^\beta \right\rfloor$

- $\beta = 0.9$
- $\beta = 0.85$
- $\beta = 0.8$
- $\beta = 0.7$
- $\beta = 0.6$
- $\beta = 0.55$
- $\beta = 0.5$
- $\beta = 0.4$

Elapsed time (seconds)
Thank you!