Résolution de systèmes polynomiaux structurés et applications en Cryptologie

Pierre-Jean Spaenlehauer

University of Western Ontario – Ontario Research Center for Computer Algebra

Magali Bardet, Jean-Charles Faugère,
Mohab Safey El Din, Bruno Salvy

Séminaire CARAMEL, LORIA
17/01/2013

0-*dimensional polynomial systems in applications*

$f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$,
where $\mathbb{K}$ is a field

$$\left\{ \begin{array}{rcl} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{array} \right. \Rightarrow$$

list the solutions in
$\overline{\mathbb{K}}^n$
$\mathbb{K}^n$
$\mathbb{R}^n$

0-*dimensional polynomial systems in applications*

$f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$,
where $\mathbb{K}$ is a field

$$\left\{ \begin{array}{rcl} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{array} \right. \Rightarrow$$

list the solutions in
$\overline{\mathbb{K}}^n$
$\mathbb{K}^n$
$\mathbb{R}^n$

NP-hard problem when $\mathbb{K}$ is finite (**Bézout theorem** $\rightsquigarrow d^n$ solutions).

0-dimensional polynomial systems in applications

$f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$,
where $\mathbb{K}$ is a field

$$\left\{ \begin{array}{rcl} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{array} \right. \Rightarrow$$

list the solutions in
$\overline{\mathbb{K}}^n$
$\mathbb{K}^n$
$\mathbb{R}^n$

NP-hard problem when $\mathbb{K}$ is finite (**Bézout theorem** $\rightsquigarrow d^n$ solutions).

Methods and algorithms

- Homotopy (symbolic/numeric)
- Geometric resolution
- Triangular sets
- **Gröbner bases**
  $\rightsquigarrow$ adapted to every field

0-dimensional polynomial systems in applications

$f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n]$,
where $\mathbb{K}$ is a field

$$\left\{ \begin{array}{rcl} f_1(x_1, \dots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \dots, x_n) & = & 0 \end{array} \right. \Rightarrow$$

list the solutions in
$\overline{\mathbb{K}}^n$
$\mathbb{K}^n$
$\mathbb{R}^n$

NP-hard problem when $\mathbb{K}$ is finite (**Bézout theorem** $\rightsquigarrow d^n$ solutions).

Methods and algorithms

- Homotopy (symbolic/numeric)
- Geometric resolution
- Triangular sets
- **Gröbner bases**
  $\rightsquigarrow$ adapted to every field

Algebraic cryptanalysis

- Algebraic **modeling** of cryptographic primitives
- **Finite fields**
- Complexity analysis
  $\rightsquigarrow$ Security estimates

0-dimensional polynomial systems in applications

$f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is a field

$$\left\{ \begin{array}{rcl} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{array} \right. \Rightarrow$$

list the solutions in
$\overline{\mathbb{K}}^n$
$\mathbb{K}^n$
$\mathbb{R}^n$

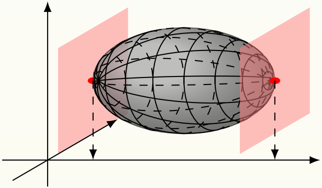
NP-hard problem when $\mathbb{K}$ is finite (**Bézout theorem** $\rightsquigarrow$ d^n solutions).

Methods and algorithms

- Homotopy (symbolic/numeric)
- Geometric resolution
- Triangular sets
- **Gröbner bases**
  $\rightsquigarrow$ adapted to every field

Real geometry and Optimization

- Field of **rationals**
- **Critical point** method
- **Optimization** under polynomial constraints



Algebraic cryptanalysis

- Algebraic **modeling** of cryptographic primitives
- **Finite fields**
- Complexity analysis
  $\rightsquigarrow$ Security estimates

0-dimensional polynomial systems in applications

$f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is a field

$$\begin{cases} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{cases} \Rightarrow$$

list the solutions in
$\overline{\mathbb{K}}^n$
$\mathbb{K}^n$
$\mathbb{R}^n$

NP-hard problem when $\mathbb{K}$ is finite (**Bézout theorem** $\rightsquigarrow d^n$ solutions).

Methods and algorithms

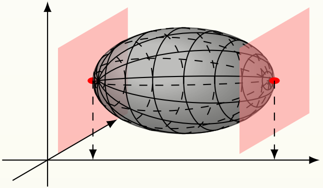
- Homotopy (symbolic/numeric)
- Geometric resolution
- Triangular sets
- **Gröbner bases**
  $\rightsquigarrow$ adapted to every field

Algebraic cryptanalysis

- Algebraic **modeling** of cryptographic primitives
- **Finite fields**
- Complexity analysis
  $\rightsquigarrow$ Security estimates

Real geometry and Optimization

- Field of **rationals**
- **Critical point** method
- **Optimization** under polynomial constraints



My **Ph.D. thesis**: **impact of structures in GB computations**

Less solutions than a dense system. Experimentally, **easier** to solve.

Less solutions than a dense system. Experimentally, **easier** to solve.

Structure	**number of solutions**	**example**
		$n_x = 9, \ n_y = 3$
dense	$2^{n_x+n_y}$	4 096
bilinear	$\binom{n_x+n_y}{n_x}$	**84**
		$r = 8, \ p = 11, \ q = 12$
dense	$(r+1)^{(p-r)(q-r)}$	282 429 536 481
determinantal	$\prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$	**4 723 719**

Less solutions than a dense system. Experimentally, **easier** to solve.

Structure	number of solutions	example
		$n_x = 9,\ n_y = 3$
dense	$2^{n_x+n_y}$	4 096
bilinear	$\binom{n_x+n_y}{n_x}$	**84**
		$r = 8,\ p = 11,\ q = 12$
dense	$(r+1)^{(p-r)(q-r)}$	282 429 536 481
determinantal	$\prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$	**4 723 719**

Critical questions

- **Complexity?**: **polynomial** in the number of solutions? **polynomial** in the number of variables?
- **Dedicated algorithms?**: how to exploit the **structures** to obtain **efficient solving** techniques?
- **Validation and Applications?**: which structures? systematic **methods of analysis**? experimental **validation** (asymptotic vs. practical complexity)?

0-dimensional solving strategy

$f_1 = \cdots = f_m = 0$		**Complexity**	**Algorithms**
$\Downarrow$ "grevlex" Gb	**Row Echelon** forms of Macaulay matrices up to degree d_{reg}	$O\left(m\binom{n+d_{reg}}{n}^{\omega}\right)$	**Buchberger (1965)** F_4 **(Faugère 1999)** F_5 **(Faugère 2002)**
$\Downarrow$ "lex" Gb	**Linear algebra** in $\frac{\mathbb{K}[\mathbf{X}]}{I}$ as a $\mathbb{K}$-vect. space of dim. $\mathrm{DEG}(I)$ $\rightsquigarrow g(u) = 0, x_i = h_i(u)$	$O\left(n\mathrm{DEG}(I)^3\right)$	**FGLM** Faugère, Gianni, Lazard, Mora (1993)

0-dimensional solving strategy

$f_1 = \cdots = f_m = 0$		Complexity	Algorithms
$\Downarrow$ "grevlex" Gb	**Row Echelon** forms of Macaulay matrices up to degree $\mathrm{d_{reg}}$	$O\left(m\binom{n+\mathrm{d_{reg}}}{n}^{\omega}\right)$	**Buchberger (1965)** F_4 **(Faugère 1999)** F_5 **(Faugère 2002)**
$\Downarrow$ "lex" Gb	**Linear algebra** in $\frac{\mathbb{K}[\mathbf{X}]}{I}$ as a $\mathbb{K}$-vect. space of dim. $\mathrm{DEG}(I)$ $\rightsquigarrow g(u) = 0, x_i = h_i(u)$	$O\left(n\mathrm{DEG}(I)^3\right)$	**FGLM** Faugère, Gianni, Lazard, Mora (1993)

Macaulay matrix in degree d

$f_1 = \cdots = f_p = 0, \deg(f_i) = d_i$
Rows: all products tf_i where $t \in \mathrm{Monomials}(d - d_i)$.
Columns: monomials of degree d.

$$\begin{array}{cc} & m_1 \succ \cdots \succ m_\ell \\ \begin{array}{c} t_1 f_1 \\ \vdots \\ t_k f_p \end{array} & \left(\begin{array}{ccc} & & \\ & & \\ & & \end{array}\right) \end{array}$$

0-dimensional solving strategy

$f_1 = \cdots = f_m = 0$		Complexity	Algorithms
$\Downarrow$ "grevlex" Gb	**Row Echelon** forms of Macaulay matrices up to degree $\mathrm{d_{reg}}$	$O\left(m\binom{n+\mathrm{d_{reg}}}{n}^{\omega}\right)$	**Buchberger (1965)** F_4 **(Faugère 1999)** F_5 **(Faugère 2002)**
$\Downarrow$ "lex" Gb	**Linear algebra** in $\frac{\mathbb{K}[\mathbf{X}]}{I}$ as a $\mathbb{K}$-vect. space of dim. $\mathrm{DEG}(I)$ $\rightsquigarrow g(u) = 0, x_i = h_i(u)$	$O\left(n\mathrm{DEG}(I)^3\right)$	**FGLM** Faugère, Gianni, Lazard, Mora (1993)

Macaulay matrix in degree d

$f_1 = \cdots = f_p = 0, \deg(f_i) = d_i$
Rows: all products tf_i where $t \in \mathrm{Monomials}(d - d_i)$.
Columns: monomials of degree d.

$$\begin{array}{cc} & m_1 \succ \cdots \succ m_\ell \\ \begin{array}{c} t_1 f_1 \\ \vdots \\ t_k f_p \end{array} & \left(\begin{array}{ccc} & & \\ \\ \\ \end{array} \right) \end{array}$$

Degree of regularity:
maximal degree reached

Hilbert series:
generating series of the rank defects

$$\mathrm{HS}(t) = \sum_{d \in \mathbb{N}} \dim(\mathbb{K}[X]_d / I_d) t^d$$

$$\mathrm{d_{reg}} = \deg(\mathrm{HS}) + 1$$

Overview

1. Introduction
2. MinRank
    1. Determinantal ideals
    2. Multi-homogeneous systems
    3. Applications in Cryptology
3. Quadratic boolean systems

The MinRank problem

$r \in \mathbb{N}$. $M_0, \ldots, M_n$: $n+1$ matrices of size $q \times q$.

MinRank

find $\lambda_1, \ldots, \lambda_n$ such that

$$\textbf{Rank}\left(M_0 - \sum_{i=1}^{n} \lambda_i M_i\right) \leq r$$

The MinRank problem

$r \in \mathbb{N}$. $M_0, \ldots, M_n$: $n+1$ matrices of size $q \times q$.

MinRank

find $\lambda_1, \ldots, \lambda_n$ such that

$$\textbf{Rank}\left(M_0 - \sum_{i=1}^{n} \lambda_i M_i\right) \leq r$$

- **Multivariate** generalization of the **EigenValue** problem.
- Applications in **cryptology**, **coding theory**, **geometry**, ...
  Kipnis/Shamir Crypto'99
  Courtois Crypto'01
- Fundamental **NP-hard** problem of **linear algebra**.

Buss, Frandsen, Shallit.
J. of Computer and System Sciences. 1999.
The computational complexity of some problems of linear algebra.

Two algebraic modelings

$$\mathbf{M} = M_0 - \sum_{i=1}^{n} \lambda_i M_i,$$

q: size of the matrices, **r**: target rank

$$\mathbf{M} = M_0 - \sum_{i=1}^{n} \lambda_i M_i,$$

q: size of the matrices, **r**: target rank

The minors modeling

$$\mathbf{Rank}(\mathbf{M}) \leq r$$
$$\Updownarrow$$
all minors of size $(r+1)$ of $\mathbf{M}$ vanish.

- $\binom{q}{r+1}^2$ equations of degree $r+1$.
- n variables.

Few variables, lots of equations, high degree !!

Two algebraic modelings

$$\mathbf{M} = M_0 - \sum_{i=1}^{n} \lambda_i M_i,$$

q: size of the matrices, **r**: target rank

The minors modeling

$$\mathbf{Rank}(\mathbf{M}) \leq r$$
$$\Updownarrow$$
all minors of size $(r+1)$ of $\mathbf{M}$ vanish.

- $\binom{q}{r+1}^2$ equations of degree $r+1$.
- n variables.

Few variables, lots of equations, high degree !!

The Kipnis-Shamir modeling

$\mathbf{Rank}(\mathbf{M}) \leq r \Leftrightarrow \exists x^{(1)}, \dots, x^{(q-r)} \in \mathbf{Ker}(\mathbf{M})$.

$$\mathbf{M} \cdot \begin{pmatrix} & I_{q-r} & \\ x_1^{(1)} & \dots & x_1^{(q-r)} \\ \vdots & \vdots & \vdots \\ x_r^{(1)} & \dots & x_r^{(q-r)} \end{pmatrix} = 0$$

- $q(q-r)$ bilinear equations.
- $n + r(q-r)$ variables.

Two algebraic modelings

$$\mathbf{M} = M_0 - \sum_{i=1}^{n} \lambda_i M_i,$$

q: size of the matrices, **r**: target rank

The minors modeling

$$\mathbf{Rank}(\mathbf{M}) \leq r$$
$$\Updownarrow$$
all minors of size $(r+1)$ of $\mathbf{M}$ vanish.

- $\binom{q}{r+1}^2$ equations of degree $r+1$.
- n variables.

Few variables, lots of equations, high degree !!

The Kipnis-Shamir modeling

$\mathbf{Rank}(\mathbf{M}) \leq r \Leftrightarrow \exists x^{(1)}, \dots, x^{(q-r)} \in \mathbf{Ker}(\mathbf{M})$.

$$\mathbf{M} \cdot \begin{pmatrix} & I_{q-r} & \\ x_1^{(1)} & \dots & x_1^{(q-r)} \\ \vdots & \vdots & \vdots \\ x_r^{(1)} & \dots & x_r^{(q-r)} \end{pmatrix} = 0$$

- $q(q-r)$ bilinear equations.
- $n + r(q-r)$ variables.

- **Complexity** of solving MinRank using Gröbner bases techniques?
- **Comparison** of the two modelings?
- **Number** of solutions?

Faugère, Levy-dit-Vehel, Perret.
Crypto '08.
Cryptanalysis of MinRank.

	System $\longrightarrow$ **grevlex GB**	$\xrightarrow[\text{Change of ordering}]{}$ **lex GB.**
Complexity	$O\left(\binom{n}{q}^2 \binom{n+\mathrm{d_{reg}}}{\mathrm{d_{reg}}}^{\omega}\right)$	$O\left(n \cdot \#Sol^3\right)$

Faugère, Levy-dit-Vehel, Perret.
Crypto '08.
Cryptanalysis of MinRank.

	System $\longrightarrow$ **grevlex GB**	$\xrightarrow{\text{Change of ordering}}$ **lex GB**.
Complexity	$O\left(\binom{n}{q}^2 \binom{n+d_{reg}}{d_{reg}}^{\omega}\right)$	$O\left(n \cdot \#Sol^3\right)$

q: size of the matrices, **n**: number of matrices, **r**: target rank. $\mathbf{n} = (\mathbf{q}-\mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n=(q-r)^2$		$d_{reg} \le q(q-r)+1$
# Sol	$< \binom{q}{r}^{q-r}$	
Complexity		polynomial in q when n is fixed ?

Determinantal systems

Let $r < q < p$ be integers and M be the $p \times q$ matrix

$$\mathsf{M} = \begin{bmatrix} f_{1,1} & \cdots & \cdots & f_{1,q} \\ \vdots & \ldots & \ldots & \vdots \\ f_{p,1} & \cdots & \cdots & f_{p,q} \end{bmatrix}$$

with $f_{i,j} \in \mathbb{K}[x_1, \ldots, x_n]$ of degree D.
The **evaluation** of M at $\mathbf{x} \in \overline{\mathbb{K}}^n$ is denoted by $\mathsf{M}_{\mathbf{x}}$.

Determinantal systems

Let $r < q < p$ be integers and M be the $p \times q$ matrix

$$\mathsf{M} = \begin{bmatrix} f_{1,1} & \cdots & \cdots & f_{1,q} \\ \vdots & \cdots & \cdots & \vdots \\ f_{p,1} & \cdots & \cdots & f_{p,q} \end{bmatrix}$$

with $f_{i,j} \in \mathbb{K}[x_1, \ldots, x_n]$ of degree D.
The **evaluation** of M at $\mathbf{x} \in \overline{\mathbb{K}}^n$ is denoted by $\mathsf{M}_{\mathbf{x}}$.

Generalized MinRank Problem

Describe the set $V \subset \overline{\mathbb{K}}^n$ of points $\mathbf{x} \in \overline{\mathbb{K}}^k$ such that $\mathrm{rank}(\mathsf{M}_{\mathbf{x}}) \leq r$.

$\rightsquigarrow$ **polynomial system solving** problem: $\mathrm{Minors}_{r+1}(M) = 0$

Main results (ISSAC 2010 + generalization submitted)
with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D.

	System $\longrightarrow$ grevlex GB	$\xrightarrow[\text{Change of ordering}]{}$ lex GB.
Complexity	$O\left(\binom{\mathbf{p}}{\mathbf{r+1}}\binom{\mathbf{q}}{\mathbf{r+1}}\binom{\mathbf{n}+\mathbf{d}_{\mathbf{reg}}}{\mathbf{d}_{\mathbf{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot\#\mathbf{Sol}^3\right)$

Main results (ISSAC 2010 + generalization submitted)

with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D.

	System $\longrightarrow$ **grevlex GB**	$\xrightarrow{\text{Change of ordering}}$ **lex GB.**
Complexity	$O\left(\binom{\mathbf{p}}{\mathbf{r+1}}\binom{\mathbf{q}}{\mathbf{r+1}}\binom{\mathbf{n+d_{reg}}}{\mathbf{d_{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot\#\mathbf{Sol}^3\right)$

Zero-dimensional case $(n = (p-r)(q-r))$

New bounds *under genericity assumptions*

$\mathrm{d_{reg}} = Dr(q-r) + (D-1)(p-r)(q-r) + 1 < (pD-1)(p-r)(q-r) + 1$

Main results (ISSAC 2010 + generalization submitted)

with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D.

	System $\longrightarrow$	grevlex GB $\xrightarrow[\text{Change of ordering}]{}$ lex GB.
Complexity	$O\left(\binom{\mathbf{p}}{\mathbf{r+1}}\binom{\mathbf{q}}{\mathbf{r+1}}\binom{\mathbf{n}+\mathbf{d}_{\mathrm{reg}}}{\mathbf{d}_{\mathrm{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot \#\mathbf{Sol}^3\right)$

Zero-dimensional case $(n = (p-r)(q-r))$

New bounds *under genericity assumptions*

$$\mathrm{d}_{\mathrm{reg}} = Dr(q-r) + (D-1)(p-r)(q-r) + 1 < (pD-1)(p-r)(q-r) + 1$$

$$\#Sol = D^{(p-r)(q-r)} \prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!} < (pD)^{(p-r)(q-r)}$$

Main results (ISSAC 2010 + generalization submitted)

with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D.

	System $\longrightarrow$ grevlex GB	$\xrightarrow{\text{Change of ordering}}$ lex GB.
Complexity	$O\left(\binom{\mathbf{p}}{\mathbf{r}+1}\binom{\mathbf{q}}{\mathbf{r}+1}\binom{\mathbf{n}+\mathbf{d}_{\mathbf{reg}}}{\mathbf{d}_{\mathbf{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot\#\mathbf{Sol}^3\right)$

Zero-dimensional case ($n = (p-r)(q-r)$)

New bounds *under genericity assumptions*

$$\mathrm{d}_{\mathrm{reg}} = Dr(q-r) + (D-1)(p-r)(q-r) + 1 < (pD-1)(p-r)(q-r)+1$$

$$\#Sol = D^{(p-r)(q-r)} \prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!} < (pD)^{(p-r)(q-r)}$$

$\rightsquigarrow$ new **complexity bounds** for the solving the Generalized MinRank Problem;
$\rightsquigarrow$ families of Generalized MinRank Problems that can be solved in complexity **polynomial** in the **number of solutions**.

Roadmap of the proof

$$\mathscr{D} = \text{Minors}_{r+1} \begin{pmatrix} v_{1,1} & \cdots & v_{1,q} \\ \vdots & \ddots & \vdots \\ v_{p,1} & \cdots & v_{p,q} \end{pmatrix}$$

Entries are **variables**

$r \times r$ matrix: $A_{i,j}(t) = \sum_\ell \binom{p-i}{\ell}\binom{q-j}{\ell} t^\ell$

$$\mathscr{D} = \mathrm{Minors}_{r+1} \begin{pmatrix} v_{1,1} & \cdots & v_{1,q} \\ \vdots & \ddots & \vdots \\ v_{p,1} & \cdots & v_{p,q} \end{pmatrix}$$

Thom/Porteous 71, Giambelli 04, Harris/Tu 84
The **degree** of $\mathscr{D}$ is

$$\prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$$

Conca/Herzog AMS'94, *Abhyankar '88*
The **Hilbert series** of $\mathscr{D}$ is

$$\mathrm{HS}_{\mathscr{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{pq-(p-r)(q-r)}}$$

$r \times r$ matrix: $A_{i,j}(t) = \sum_\ell \binom{p-i}{\ell}\binom{q-j}{\ell} t^\ell$

Roadmap of the proof

$$\mathscr{D} = \text{Minors}_{r+1} \begin{pmatrix} v_{1,1} & \cdots & v_{1,q} \\ \vdots & \ddots & \vdots \\ v_{p,1} & \cdots & v_{p,q} \end{pmatrix}$$

Thom/Porteous 71, Giambelli 04, Harris/Tu 84

The **degree** of $\mathscr{D}$ is

$$\prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$$

Conca/Herzog AMS'94, *Abhyankar '88*

The **Hilbert series** of $\mathscr{D}$ is

$$\text{HS}_{\mathscr{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{pq-(p-r)(q-r)}}$$

$r \times r$ matrix: $A_{i,j}(t) = \sum_{\ell} \binom{p-i}{\ell}\binom{q-j}{\ell} t^{\ell}$

$$\mathcal{I} = \text{Minors}_{r+1} \begin{pmatrix} f_{1,1} & \cdots & f_{1,q} \\ \vdots & \ddots & \vdots \\ f_{p,1} & \cdots & f_{p,q} \end{pmatrix}$$

Entries are **polynomials**

Roadmap of the proof

$$\mathscr{D} = \mathrm{Minors}_{r+1}\begin{pmatrix} v_{1,1} & \cdots & v_{1,q} \\ \vdots & \ddots & \vdots \\ v_{p,1} & \cdots & v_{p,q} \end{pmatrix}$$

Thom/Porteous 71, Giambelli 04, Harris/Tu 84

The **degree** of $\mathscr{D}$ is

$$\prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$$

Conca/Herzog AMS'94, *Abhyankar '88*

The **Hilbert series** of $\mathscr{D}$ is

$$\mathrm{HS}_{\mathscr{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{pq-(p-r)(q-r)}}$$

$r \times r$ matrix: $A_{i,j}(t) = \sum_\ell \binom{p-i}{\ell}\binom{q-j}{\ell} t^\ell$

$$\mathcal{I} = \mathrm{Minors}_{r+1}\begin{pmatrix} f_{1,1} & \cdots & f_{1,q} \\ \vdots & \ddots & \vdots \\ f_{p,1} & \cdots & f_{p,q} \end{pmatrix}$$

Entries are **polynomials**

transfer of properties of $\mathcal{D}$ by adding $\langle v_{i,j} - f_{i,j} \rangle$

Roadmap of the proof

$$\mathscr{D} = \mathrm{Minors}_{r+1}\begin{pmatrix} v_{1,1} & \cdots & v_{1,q} \\ \vdots & \ddots & \vdots \\ v_{p,1} & \cdots & v_{p,q} \end{pmatrix}$$

Thom/Porteous 71, Giambelli 04, Harris/Tu 84

The **degree** of $\mathscr{D}$ is

$$\prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$$

Conca/Herzog AMS'94, *Abhyankar '88*

The **Hilbert series** of $\mathscr{D}$ is

$$\mathrm{HS}_{\mathscr{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{pq-(p-r)(q-r)}}$$

$r \times r$ matrix: $A_{i,j}(t) = \sum_\ell \binom{p-i}{\ell}\binom{q-j}{\ell} t^\ell$

transfer of properties of $\mathcal{D}$ by adding $\langle v_{i,j} - f_{i,j} \rangle$

$$\mathcal{I} = \mathrm{Minors}_{r+1}\begin{pmatrix} f_{1,1} & \cdots & f_{1,q} \\ \vdots & \ddots & \vdots \\ f_{p,1} & \cdots & f_{p,q} \end{pmatrix}$$

The **degree** of $\mathcal{I}$ is

$$D^{(p-r)(q-r)} \prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$$

The **Hilbert series** of $\mathcal{I}$ is

$$\mathrm{HS}_{\mathcal{I}}(t) = \frac{\det(A(t^D))(1-t^D)^{(p-r)(q-r)}}{t^{\binom{r}{2}}(1-t)^n}$$

Roadmap of the proof

$$\mathscr{D} = \text{Minors}_{r+1}\begin{pmatrix} v_{1,1} & \cdots & v_{1,q} \\ \vdots & \ddots & \vdots \\ v_{p,1} & \cdots & v_{p,q} \end{pmatrix}$$

Thom/Porteous 71, Giambelli 04, Harris/Tu 84
The **degree** of $\mathscr{D}$ is

$$\prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$$

Conca/Herzog AMS'94, *Abhyankar '88*
The **Hilbert series** of $\mathscr{D}$ is

$$\text{HS}_{\mathscr{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{pq-(p-r)(q-r)}}$$

$r \times r$ matrix: $A_{i,j}(t) = \sum_\ell \binom{p-i}{\ell}\binom{q-j}{\ell} t^\ell$

transfer of properties of $\mathcal{D}$ by adding $\langle v_{i,j} - f_{i,j} \rangle$

$$\mathcal{I} = \text{Minors}_{r+1}\begin{pmatrix} f_{1,1} & \cdots & f_{1,q} \\ \vdots & \ddots & \vdots \\ f_{p,1} & \cdots & f_{p,q} \end{pmatrix}$$

The **degree** of $\mathcal{I}$ is

$$D^{(p-r)(q-r)} \prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$$

The **Hilbert series** of $\mathcal{I}$ is

$$\text{HS}_{\mathcal{I}}(t) = \frac{\det(A(t^D))(1-t^D)^{(p-r)(q-r)}}{t^{\binom{r}{2}}(1-t)^n}$$

Ingredients of the proof:

- **Cohen-Macaulay** rings;
- **quasi-homogeneous** polynomials.

	System $\longrightarrow$	**grevlex GB** $\xrightarrow[\text{Change of ordering}]{}$ **lex GB**.
Complexity	$O\left(\binom{n}{q}^2 \binom{n+\mathrm{d_{reg}}}{\mathrm{d_{reg}}}^\omega\right)$	$O\left(n \cdot \#Sol^3\right)$

q: size of the matrices, **n**: number of matrices, **r**: target rank. $\mathbf{n} = (\mathbf{q}-\mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n=(q-r)^2$		$\mathrm{d_{reg}} \le q(q-r)+1$
# Sol		$< \binom{q}{r}^{q-r}$
Complexity		poly(q)??

MinRank – Complexity of the minors modeling

	System	$\longrightarrow$	grevlex GB	$\xrightarrow[\text{Change of ordering}]{}$	lex GB.
Complexity	$O\left(\binom{n}{q}^2 \binom{n+\mathrm{d_{reg}}}{\mathrm{d_{reg}}}^{\omega}\right)$			$O\left(n \cdot \#Sol^3\right)$	

q: size of the matrices, **n**: number of matrices, **r**: target rank. $\mathbf{n} = (\mathbf{q}-\mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q-r)^2$	$\boxed{\text{New}}$ $\mathbf{r}(\mathbf{q}-\mathbf{r})+\mathbf{1}$	$\mathrm{d_{reg}} \leq q(q-r)+1$
# Sol		$< \binom{q}{r}^{q-r}$
Complexity		poly(q)??

MinRank – Complexity of the minors modeling

	System $\longrightarrow$ **grevlex GB**	$\xrightarrow[\text{Change of ordering}]{}$ **lex GB.**
Complexity	$O\left(\binom{n}{q}^2\binom{n+\mathsf{d}_{\mathrm{reg}}}{\mathsf{d}_{\mathrm{reg}}}^{\omega}\right)$	$O\left(n\cdot\#Sol^3\right)$

$\mathbf{q}$: size of the matrices, $\mathbf{n}$: number of matrices, $\mathbf{r}$: target rank. $\mathbf{n}=(\mathbf{q}-\mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n=(q-r)^2$	New $\mathbf{r}(\mathbf{q}-\mathbf{r})+\mathbf{1}$	$\mathsf{d}_{\mathrm{reg}}\leq q(q-r)+1$
# Sol	New $\prod_{i=0}^{q-r-1}\frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}<\binom{q}{r}^{q-r}$	
Complexity		$\mathrm{poly}(q)$??

MinRank – Complexity of the minors modeling

	System $\longrightarrow$ grevlex GB $\xrightarrow[\text{Change of ordering}]{}$ lex GB.	
Complexity	$O\left(\binom{n}{q}^2 \binom{n+\mathrm{d_{reg}}}{\mathrm{d_{reg}}}^{\omega}\right)$	$O\left(n \cdot \#Sol^3\right)$

q: size of the matrices, **n**: number of matrices, **r**: target rank. $\mathbf{n} = (\mathbf{q}-\mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q-r)^2$	$\boxed{\text{New}}$ $\mathbf{r}(\mathbf{q}-\mathbf{r})+\mathbf{1}$	$\mathrm{d_{reg}} \leq q(q-r)+1$
# Sol	$\boxed{\text{New}}$ $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!} < \binom{q}{r}^{q-r}$	
Complexity	$O(q^{3n})$	$\mathrm{poly}(q)$??

Complexity **polynomial** in q;

MinRank – Complexity of the minors modeling

	System $\longrightarrow$ grevlex GB	$\xrightarrow[\text{Change of ordering}]{}$ lex GB.
Complexity	$O\left(\binom{n}{q}^2 \binom{n+d_{reg}}{d_{reg}}^{\omega}\right)$	$O\left(n \cdot \#Sol^3\right)$

q: size of the matrices, **n**: number of matrices, **r**: target rank. $\mathbf{n} = (\mathbf{q}-\mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q-r)^2$	$\boxed{\text{New}}$ $\mathbf{r}(\mathbf{q}-\mathbf{r})+\mathbf{1}$	$d_{reg} \leq q(q-r)+1$
# Sol	$\boxed{\text{New}}$ $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!} < \binom{q}{r}^{q-r}$	
Complexity	$O(q^{3n})$	poly(q)??

Complexity **polynomial** in q;
Compatible genericity assumptions;

Overview

Relation between bilinear and determinantal systems

$F = (f_1, \dots, f_m) \in \mathbb{K}[x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}]^m$: system of **bilinear equations**.

$$\mathrm{jac}_X(F) = \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial x_0} & \cdots & \frac{\partial f_m}{\partial x_{n_x}} \end{pmatrix} \qquad \mathrm{jac}_Y(F) = \begin{pmatrix} \frac{\partial f_1}{\partial y_0} & \cdots & \frac{\partial f_1}{\partial y_{n_y}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial y_0} & \cdots & \frac{\partial f_m}{\partial y_{n_y}} \end{pmatrix}$$

Euler relations

$$f = \sum x_j \frac{\partial f}{\partial x_j} = \sum y_j \frac{\partial f}{\partial y_j}.$$

$$\mathrm{jac}_X(F) \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{n_x} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} \qquad \mathrm{jac}_Y(F) \cdot \begin{pmatrix} y_0 \\ \vdots \\ y_{n_y} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}$$

Relation between bilinear and determinantal systems

$F = (f_1, \ldots, f_m) \in \mathbb{K}[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]^m$: system of **bilinear equations**.

$$\mathrm{jac}_X(F) = \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial x_0} & \cdots & \frac{\partial f_m}{\partial x_{n_x}} \end{pmatrix} \qquad \mathrm{jac}_Y(F) = \begin{pmatrix} \frac{\partial f_1}{\partial y_0} & \cdots & \frac{\partial f_1}{\partial y_{n_y}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial y_0} & \cdots & \frac{\partial f_m}{\partial y_{n_y}} \end{pmatrix}$$

Euler relations

$$f = \sum x_j \frac{\partial f}{\partial x_j} = \sum y_j \frac{\partial f}{\partial y_j}.$$

$$\mathrm{jac}_X(F) \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{n_x} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} \qquad \mathrm{jac}_Y(F) \cdot \begin{pmatrix} y_0 \\ \vdots \\ y_{n_y} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}$$

$$f_1 = \cdots = f_m = 0 \Longrightarrow \mathbf{Minors}_{n_x+1}(\mathbf{jac}_X(\mathbf{F})) = \mathbf{0}$$

Relation between bilinear and determinantal systems

$F = (f_1, \dots, f_m) \in \mathbb{K}[x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}]^m$: system of **bilinear equations**.

$$\mathrm{jac}_X(F) = \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial x_0} & \cdots & \frac{\partial f_m}{\partial x_{n_x}} \end{pmatrix} \qquad \mathrm{jac}_Y(F) = \begin{pmatrix} \frac{\partial f_1}{\partial y_0} & \cdots & \frac{\partial f_1}{\partial y_{n_y}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial y_0} & \cdots & \frac{\partial f_m}{\partial y_{n_y}} \end{pmatrix}$$

Euler relations

$$f = \sum x_j \frac{\partial f}{\partial x_j} = \sum y_j \frac{\partial f}{\partial y_j}.$$

$$\mathrm{jac}_X(F) \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{n_x} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} \qquad \mathrm{jac}_Y(F) \cdot \begin{pmatrix} y_0 \\ \vdots \\ y_{n_y} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}$$

$$f_1 = \cdots = f_m = 0 \Longrightarrow \mathbf{Minors}_{n_x+1}(\mathbf{jac}_X(\mathbf{F})) = \mathbf{0}$$

$$\Rightarrow d_{reg} \leq \min(n_x, n_y) + 1.$$

Main results (J. of Symbolic Computation 2011)

with J.-C. Faugère, M. Safey El Din

	Giusti Lazard Macaulay	Bardet Faugère Salvy	New results:
	$m \leq n$	$m = \alpha n$	**bilinear** $m \leq n_x + n_y$
reductions to 0	F_5 criterion		extended F_5 crit.
subclass	regularity	semi-regularity	biregularity
Hilbert series	$\dfrac{\prod(1-t^{d_i})}{(1-t)^n}$	$\left[\dfrac{\prod(1-t^{d_i})}{(1-t)^n}\right]_+$	$\dfrac{Q(t_1,t_2)}{(1-t_1)^{n_x}(1-t_2)^{n_y}}$
complexity	$\approx 2^{\omega n}$	$\approx 2^{\omega\left(\alpha-1/2-\sqrt{\alpha(\alpha-1)}\right)n}$	$\approx 2^{\omega \min(n_x,n_y)}$

Main results (J. of Symbolic Computation 2011)

with J.-C. Faugère, M. Safey El Din

	Giusti, Lazard, Macaulay	*Bardet, Faugère, Salvy*	New results:
	$m \leq n$	$m = \alpha n$	**bilinear** $m \leq n_x + n_y$
reductions to 0	F_5 criterion		extended F_5 crit.
subclass	regularity	semi-regularity	biregularity
Hilbert series	$\dfrac{\prod(1-t^{d_i})}{(1-t)^n}$	$\left[\dfrac{\prod(1-t^{d_i})}{(1-t)^n}\right]_+$	$\dfrac{Q(t_1,t_2)}{(1-t_1)^{n_x}(1-t_2)^{n_y}}$
complexity	$\approx 2^{\omega n}$	$\approx 2^{\omega\left(\alpha-1/2-\sqrt{\alpha(\alpha-1)}\right)n}$	$\approx 2^{\omega \min(n_x,n_y)}$

- New theoretical **complexity bounds**. Experimentally observed.
- New classes of **affine bilinear systems** solved in polynomial time.

$$\rightsquigarrow \min(n_x,n_y) \text{ bounded} \Rightarrow \begin{cases} \text{poly in } n_x+n_y \\ \text{poly in \textbf{nb. solutions}}. \end{cases}$$

	System $\longrightarrow$	grevlex GB $\xrightarrow[\text{Change of ordering}]{}$	lex GB.
Complexity	$O\left(\binom{n}{q}^2\binom{n+\mathrm{d_{reg}}}{\mathrm{d_{reg}}}^\omega\right)$		$O\left(n\cdot\#Sol^3\right)$

q: size of the matrices, **n**: number of matrices, **r**: target rank. $\mathbf{n}=(\mathbf{q}-\mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n=(q-r)^2$	$\boxed{\text{New}}$ $\mathbf{r(q-r)+1}$	$\mathrm{d_{reg}}\leq \qquad < q(q-r)+1$
# Sol	$\boxed{\text{New}}$ $\displaystyle\prod_{i=0}^{q-r-1}\frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$	
Complexity	$O(q^{3n})$	

	System $\longrightarrow$	**grevlex GB** $\underset{\text{Change of ordering}}{\longrightarrow}$ **lex GB**.
Complexity	$O\left(\binom{n}{q}^2 \binom{n+\mathrm{d_{reg}}}{\mathrm{d_{reg}}}^\omega\right)$	$O\left(n \cdot \#Sol^3\right)$

q: size of the matrices, **n**: number of matrices, **r**: target rank. $\mathbf{n} = (\mathbf{q} - \mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q-r)^2$	$\boxed{\text{New}}$ $\mathbf{r(q-r)+1}$	$\boxed{\text{New}}$ $\mathrm{d_{reg}} \leq \quad (q-r)^2 + 2 \quad < q(q-r)+1$
# Sol	$\boxed{\text{New}}$ $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$	
Complexity	$O(q^{3n})$	

MinRank – Complexity of Kipnis-Shamir modeling

	System $\longrightarrow$ grevlex GB	$\xrightarrow[\text{Change of ordering}]{}$ lex GB.
Complexity	$O\left(\binom{n}{q}^2 \binom{n+\mathsf{d}_{\mathsf{reg}}}{\mathsf{d}_{\mathsf{reg}}}^{\omega}\right)$	$O\left(n \cdot \#Sol^3\right)$

q: size of the matrices, **n**: number of matrices, **r**: target rank. $\mathbf{n} = (\mathbf{q} - \mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q-r)^2$	$\boxed{\text{New}}$ $\mathbf{r}(\mathbf{q}-\mathbf{r})+\mathbf{1}$	$\boxed{\text{New}}$ $\mathsf{d}_{\mathsf{reg}} \leq (q-r)^2 + 2 < q(q-r)+1$
# Sol	$\boxed{\text{New}}$ $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$	
Complexity	$O(q^{3n})$	$O(q^{3(n+2)})$: **polynomial** in q

	System $\longrightarrow$	**grevlex GB** $\xrightarrow[\text{Change of ordering}]{}$ **lex GB**.
Complexity	$O\left(\binom{n}{q}^2 \binom{n+\mathrm{d_{reg}}}{\mathrm{d_{reg}}}^\omega\right)$	$O\left(n \cdot \#Sol^3\right)$

$\mathbf{q}$: size of the matrices, $\mathbf{n}$: number of matrices, $\mathbf{r}$: target rank. $\mathbf{n} = (\mathbf{q}-\mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q-r)^2$	New $\mathbf{r(q-r)+1}$	$\mathrm{d_{reg}} \leq$ New $(q-r)^2+2$ $< q(q-r)+1$
# Sol	New $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$	
Complexity	$O(q^{3n})$	$O(q^{3(n+2)})$: **polynomial** in q

But...

	System $\longrightarrow$ grevlex GB	$\xrightarrow{\text{Change of ordering}}$ lex GB.
Complexity	$O\left(\binom{n}{q}^2 \binom{n+\mathrm{d_{reg}}}{\mathrm{d_{reg}}}^{\omega}\right)$	$O\left(n \cdot \#Sol^3\right)$

q: size of the matrices, **n**: number of matrices, **r**: target rank. $\mathbf{n} = (\mathbf{q}-\mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n=(q-r)^2$	New $\mathbf{r(q-r)+1}$	New $\mathrm{d_{reg}} \leq (q-r)^2+2 < q(q-r)+1$
# Sol	New $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$	
Complexity	$O(q^{3n})$	$O(q^{3(n+2)})$: **polynomial** in q

But... different **genericity assumptions** $\rightsquigarrow$ bound not sharp

	System $\longrightarrow$	**grevlex GB** $\xrightarrow[\text{Change of ordering}]{}$ **lex GB**.
Complexity	$O\left(\binom{n}{q}^2\binom{n+\mathrm{d_{reg}}}{\mathrm{d_{reg}}}^\omega\right)$	$O\left(n\cdot\#Sol^3\right)$

q: size of the matrices, **n**: number of matrices, **r**: target rank. $\mathbf{n}=(\mathbf{q}-\mathbf{r})^2$.

	Minors	Kipnis-Shamir
Degree of regularity when $n=(q-r)^2$	$\boxed{\text{New}}$ $\mathbf{r(q-r)+1}$	$\mathrm{d_{reg}} \leq \underset{\boxed{\text{New}}}{(q-r)^2+2} < q(q-r)+1$
# Sol	$\boxed{\text{New}}$ $\displaystyle\prod_{i=0}^{q-r-1}\frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$	
Complexity	$O(q^{3n})$	$O(q^{3(n+2)})$: **polynomial** in q

But... different **genericity assumptions** $\rightsquigarrow$ bound not sharp

to be continued. . .

Courtois. Asiacrypt'01.

Efficient zero-knowledge authentication based on a linear algebra problem MinRank.

$\mathbb{K} = \mathbf{GF(65521)}$ $\color{red}{(\mathbf{m}, \mathbf{k}, \mathbf{r})}$: k matrices of size $m \times m$. Target rank: r.

Challenge	A	B			C
	$(6,9,3)$	$(7,9,4)$	$(8,9,5)$	$(9,9,6)$	$(11,9,8)$
degree	**980**	**4116**	**14112**	**41580**	259545
	Minors modeling				
d_{reg}	10	13	16	19	
F_5 time	**1.1s**	**28.4s**	**544s**	**9048s**	-
F_5 mem	**488 MB**	**587 MB**	**1213 MB**	**5048 MB**	-
$\log_2$(Nb op.)	**21.5**	**25.9**	**29.2**	**32.7**	
FGLM time	**0.5s**	**28.5s**	**1033s**	**22171s**	-
	Kipnis-Shamir modeling				
d_{reg}	5	6	7		
F_5 time	**30s**	**3795s**	**328233s**	∞	
F_5 mem	**407 MB**	**3113 MB**	**58587 MB**		
$\log_2$(Nb op.)	**30.5**	**37.1**	**43.4**		
FGLM time	**35s**	**2580s**	∞		

Experimental results

Courtois. Asiacrypt'01.

Efficient zero-knowledge authentication based on a linear algebra problem MinRank.

$\mathbb{K} = \mathbf{GF(65521)}$ $\quad$ $(\mathbf{m}, \mathbf{k}, \mathbf{r})$: k matrices of size $m \times m$. Target rank: r.

Challenge	**A**	**B**			**C**
	$(6,9,3)$	$(7,9,4)$	$(8,9,5)$	$(9,9,6)$	$(11,9,8)$
degree	**980**	**4116**	**14112**	**41580**	259545
	Minors modeling				
d_{reg}	10	13	16	19	
F_5 time	**1.1s**	**28.4s**	**544s**	**9048s**	-
F_5 mem	**488 MB**	**587 MB**	**1213 MB**	**5048 MB**	-
$\log_2$(Nb op.)	**21.5**	**25.9**	**29.2**	**32.7**	
FGLM time	**0.5s**	**28.5s**	**1033s**	**22171s**	-
	Kipnis-Shamir modeling				
d_{reg}	5	6	7		
F_5 time	**30s**	**3795s**	**328233s**	∞	
F_5 mem	**407 MB**	**3113 MB**	**58587 MB**		
$\log_2$(Nb op.)	**30.5**	**37.1**	**43.4**		
FGLM time	**35s**	**2580s**	∞		

Computational bottleneck: computing the minors.

Computing effort needed for solving **Challenge C**:

238 days on 64 quadricore processors.

Multi-homogeneous systems

Bilinear systems: particular case of **multi-homogeneous** systems

Multi-homogeneity

$f \in \mathbb{K}[X^{(1)}, \ldots, X^{(\ell)}]$ is **multi-homogeneous** of multi-degree $(d_1, \ldots, d_\ell)$ if for all $\lambda_1, \ldots, \lambda_\ell$,

$$f(\lambda_1 X^{(1)}, \ldots, \lambda_\ell X^{(\ell)}) = \lambda_1^{d_1} \ldots \lambda_\ell^{d_\ell} f(X^{(1)}, \ldots, X^{(\ell)}).$$

Multi-homogeneous systems

Bilinear systems: particular case of **multi-homogeneous** systems

Multi-homogeneity

$f \in \mathbb{K}[X^{(1)}, \ldots, X^{(\ell)}]$ is **multi-homogeneous** of multi-degree $(d_1, \ldots, d_\ell)$ if for all $\lambda_1, \ldots, \lambda_\ell$,

$$f(\lambda_1 X^{(1)}, \ldots, \lambda_\ell X^{(\ell)}) = \lambda_1^{d_1} \ldots \lambda_\ell^{d_\ell} f(X^{(1)}, \ldots, X^{(\ell)}).$$

- Real algebraic **geometry**
  [*Safey/Trébuchet* 06, *Bank/Giusti/Heintz/Safey/Schost* AAECC'10].

Multi-homogeneous systems

Bilinear systems: particular case of **multi-homogeneous** systems

Multi-homogeneity

$f \in \mathbb{K}[X^{(1)}, \ldots, X^{(\ell)}]$ is **multi-homogeneous** of multi-degree $(d_1, \ldots, d_\ell)$ if for all $\lambda_1, \ldots, \lambda_\ell$,

$$f(\lambda_1 X^{(1)}, \ldots, \lambda_\ell X^{(\ell)}) = \lambda_1^{d_1} \ldots \lambda_\ell^{d_\ell} f(X^{(1)}, \ldots, X^{(\ell)}).$$

- Real algebraic **geometry**
  [*Safey/Trébuchet* 06, *Bank/Giusti/Heintz/Safey/Schost* AAECC'10].
- $\rightsquigarrow$ **Crypto**

Overview

Based on **alternant codes**:

- secret key: a **parity-check** matrix of the form

$$H = \begin{pmatrix} y_0 & y_1 & \cdots & y_{n-1} \\ y_0 x_0 & y_1 x_1 & \cdots & y_{n-1} x_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ y_0 x_0^{t-1} & y_1 x_1^{t-1} & \cdots & y_n x_n^{t-1} \end{pmatrix},$$

  where $x_i, y_j \in \mathbb{F}_{2^m}$, with $x_0, \ldots, x_n$ pairwise distinct and $y_j \neq 0$.
- public key: a **generator matrix** G of the same code.

Modeling of McEliece cryptosystem

Based on **alternant codes**:

- secret key: a **parity-check** matrix of the form

$$H = \begin{pmatrix} y_0 & y_1 & \cdots & y_{n-1} \\ y_0 x_0 & y_1 x_1 & \cdots & y_{n-1} x_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ y_0 x_0^{t-1} & y_1 x_1^{t-1} & \cdots & y_n x_n^{t-1} \end{pmatrix},$$

  where $x_i, y_j \in \mathbb{F}_{2^m}$, with $x_0, \ldots, x_n$ pairwise distinct and $y_j \neq 0$.
- public key: a **generator matrix** G of the same code.

Problem

Given G, find H such that $H \cdot G^t = \mathbf{0}$!

Based on **alternant codes**:

- secret key: a **parity-check** matrix of the form

$$H = \begin{pmatrix} y_0 & y_1 & \cdots & y_{n-1} \\ y_0 x_0 & y_1 x_1 & \cdots & y_{n-1} x_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ y_0 x_0^{t-1} & y_1 x_1^{t-1} & \cdots & y_n x_n^{t-1} \end{pmatrix},$$

  where $x_i, y_j \in \mathbb{F}_{2^m}$, with $x_0, \ldots, x_n$ pairwise distinct and $y_j \neq 0$.
- public key: a **generator matrix** G of the same code.

Problem

Given G, find H such that $H \cdot G^t = \mathbf{0}$!

$$\rightsquigarrow \forall i, j, \quad g_{i,0} y_0 x_0^j + \cdots + g_{i,n-1} y_{n-1} x_{n-1}^j = 0.$$

$\Rightarrow$ **Bi-homogeneous structure** !!

Cryptanalysis of compact variants of McEliece

Compact variants

Goal: reduce the size of the keys.

- **Quasi-cyclic** variant: Berger/Cayrel/Gaborit/Otmani Africacrypt'09;
- **Dyadic** variant: Misoczy/Barreto SAC'09.

Compact variants

Goal: reduce the size of the keys.

- **Quasi-cyclic** variant: Berger/Cayrel/Gaborit/Otmani Africacrypt'09;
- **Dyadic** variant: Misoczy/Barreto SAC'09.

Faugère/Otmani/Perret/Tilich, Eurocrypt'2010

$\Rightarrow$ add **redundancy** to the polynomial system
$\rightsquigarrow$ linear equations $\rightsquigarrow$ less variables.

Compact variants

Goal: reduce the size of the keys.

- **Quasi-cyclic** variant: Berger/Cayrel/Gaborit/Otmani Africacrypt'09;
- **Dyadic** variant: Misoczy/Barreto SAC'09.

Faugère/Otmani/Perret/Tilich, Eurocrypt'2010

$\Rightarrow$ add **redundancy** to the polynomial system
$\rightsquigarrow$ linear equations $\rightsquigarrow$ less variables.
Moreover, the system is still over-determined and one can extract a subsystem containing only **powers of two**:

$$\rightsquigarrow \forall i, j \textbf{ a power of two !!}, \quad g_{i,0} y_0 x_0^j + \cdots + g_{i,n-1} y_{n-1} x_{n-1}^j = 0.$$

Compact variants

Goal: reduce the size of the keys.

- **Quasi-cyclic** variant: Berger/Cayrel/Gaborit/Otmani Africacrypt'09;
- **Dyadic** variant: Misoczy/Barreto SAC'09.

Faugère/Otmani/Perret/Tilich, Eurocrypt'2010

$\Rightarrow$ add **redundancy** to the polynomial system
$\rightsquigarrow$ linear equations $\rightsquigarrow$ less variables.
Moreover, the system is still over-determined and one can extract a subsystem containing only **powers of two**:

$$\rightsquigarrow \forall i, j \textbf{ a power of two !!}, \quad g_{i,0} y_0 x_0^j + \cdots + g_{i,n-1} y_{n-1} x_{n-1}^j = 0.$$

Decomposing the subsystem over the field $\mathbb{F}_2$

$$\Rightarrow \textbf{Bilinear system with } n_x \ll n_y \textbf{ !!!}$$

Cryptanalysis of compact variants of McEliece

Compact variants

Goal: reduce the size of the keys.

- **Quasi-cyclic** variant: Berger/Cayrel/Gaborit/Otmani Africacrypt'09;
- **Dyadic** variant: Misoczy/Barreto SAC'09.

Faugère/Otmani/Perret/Tilich, Eurocrypt'2010

$\Rightarrow$ add **redundancy** to the polynomial system
$\rightsquigarrow$ linear equations $\rightsquigarrow$ less variables.
Moreover, the system is still over-determined and one can extract a subsystem containing only **powers of two**:

$$\rightsquigarrow \forall i,j \textbf{ a power of two !!}, \quad g_{i,0}\,y_0\,x_0^j + \cdots + g_{i,n-1}\,y_{n-1}\,x_{n-1}^j = 0.$$

Decomposing the subsystem over the field $\mathbb{F}_2$

$$\Rightarrow \textbf{Bilinear system with } n_x \ll n_y \textbf{ !!!}$$

Theoretical and **Practical attacks** on the quasi-cyclic and dyadic variants of McEliece !!

Algebraic cryptanalysis of (multi-)HFE

Patarin, Eurocrypt'96
Billet/Patarin/Seurin, ICSCC'08
Ding/Schmitt/Werner, Information Security, 2008
Granboulan/Joux/Stern, CRYPTO'06

$$P(x) = \sum_{0 \le i,j \le r} p_{i,j} x^{q^i + q^j} \in \mathbb{F}_{q^n}, \text{ with } r \ll n$$

$\rightsquigarrow$ **low-rank** quadratic form $(\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$

Algebraic cryptanalysis of (multi-)HFE

Patarin, Eurocrypt'96
Billet/Patarin/Seurin, ICSCC'08
Ding/Schmitt/Werner, Information Security, 2008
Granboulan/Joux/Stern, CRYPTO'06

$$P(x) = \sum_{0 \le i,j \le r} p_{i,j} x^{q^i + q^j} \in \mathbb{F}_{q^n}, \text{ with } r \ll n$$

$\rightsquigarrow$ **low-rank** quadratic form $(\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$
masked by linear transforms !!

Algebraic cryptanalysis of (multi-)HFE

Patarin, Eurocrypt'96
Billet/Patarin/Seurin, ICSCC'08
Ding/Schmitt/Werner, Information Security, 2008
Granboulan/Joux/Stern, CRYPTO'06

$$P(x) = \sum_{0 \leq i,j \leq r} p_{i,j} x^{q^i + q^j} \in \mathbb{F}_{q^n}, \text{ with } r \ll n$$

$\rightsquigarrow$ **low-rank** quadratic form $(\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$
masked by linear transforms !!

$\Rightarrow$ the **secret polynomial** can be recovered by solving a **MinRank problem**.

Bettale/Faugère/Perret, PKC 2011

The **complexity** of solving this MinRank problem is conjectured to be bounded above by

$$O\left(n^{(r+1)\omega}\right).$$

- $\rightsquigarrow$ key-recovery attack with **polynomial complexity** in n!!
- $\rightsquigarrow$ attacks on **odd-characteristic** variants;
- $\rightsquigarrow$ generalizations to **multi-HFE**.

Overview

Find **zeros** in $\mathbb{F}_2^n$ of **quadratic polynomials** $f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$.

Boolean systems (J. of Complexity 2012)

with M. Bardet, J.-C. Faugère, B. Salvy

Find **zeros** in $\mathbb{F}_2^n$ of **quadratic polynomials** $f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$.

State of the art:

- Worst case complexity $4 \cdot 2^n \log(n)$ (*Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir*, CHES'10).
- Exponentially better bounds conjectured (*Yang, Chen, Courtois*).

Boolean systems (J. of Complexity 2012)

with M. Bardet, J.-C. Faugère, B. Salvy

Find **zeros** in $\mathbb{F}_2^n$ of **quadratic polynomials** $f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$.

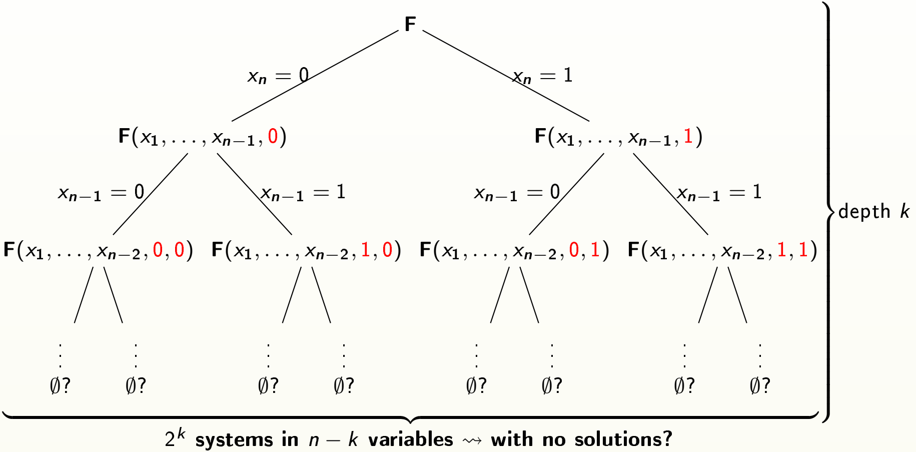
State of the art:

- Worst case complexity $4 \cdot 2^n \log(n)$ (*Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir*, CHES'10).
- Exponentially better bounds conjectured (*Yang, Chen, Courtois*).

Main algorithmic result $\rightsquigarrow$ **Algorithm**:

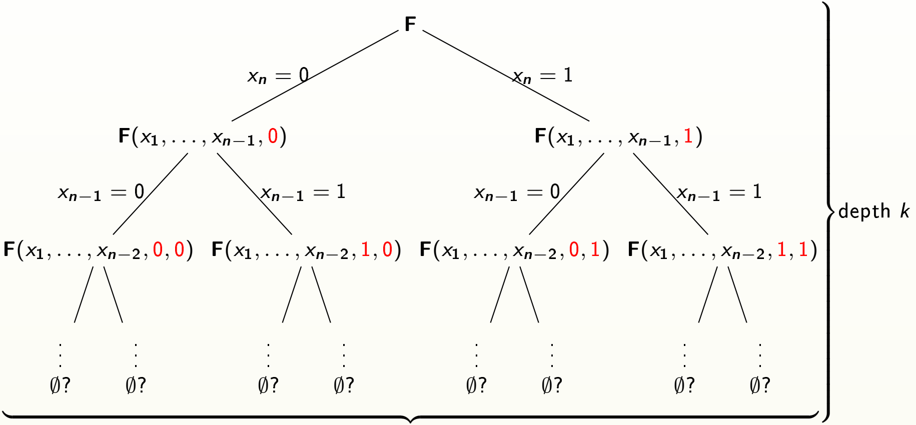
Exhaustive search + sparse linear algebra **pruning branches** in the search tree

Algorithm



$\mathbf{F}$
$x_n = 0$
$x_n = 1$
$\mathbf{F}(x_1, \ldots, x_{n-1}, 0)$
$\mathbf{F}(x_1, \ldots, x_{n-1}, 1)$
$x_{n-1} = 0$
$x_{n-1} = 1$
$x_{n-1} = 0$
$x_{n-1} = 1$
$\mathbf{F}(x_1, \ldots, x_{n-2}, 0, 0)$
$\mathbf{F}(x_1, \ldots, x_{n-2}, 1, 0)$
$\mathbf{F}(x_1, \ldots, x_{n-2}, 0, 1)$
$\mathbf{F}(x_1, \ldots, x_{n-2}, 1, 1)$
$\emptyset?$ $\emptyset?$ $\emptyset?$ $\emptyset?$ $\emptyset?$ $\emptyset?$ $\emptyset?$ $\emptyset?$
depth k
2^k **systems in** $n-k$ **variables** $\rightsquigarrow$ **with no solutions?**

Algorithm



2^k **systems in** $n-k$ **variables** $\rightsquigarrow$ **with no solutions?**

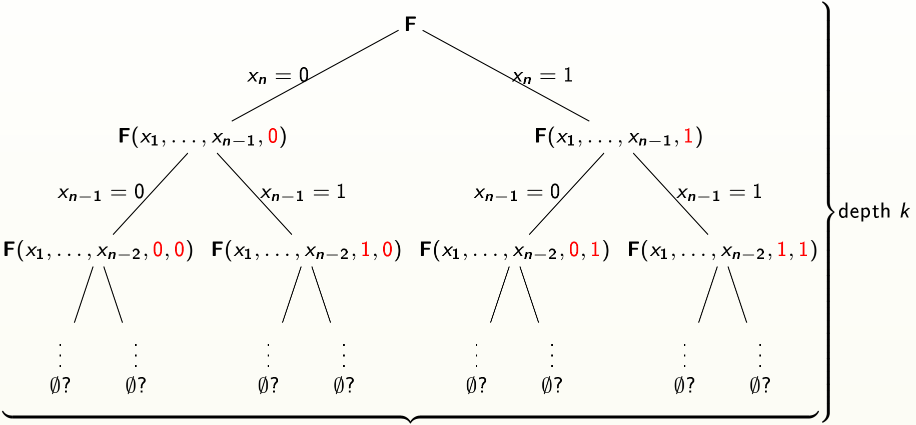
Hilbert Nullstellensatz

$\mathbf{F}(x_1, \ldots, x_{n-k}, a_{n-k+1}, \ldots, a_n)$ has no solution in $\mathbb{F}_2^{n-k}$

$$\Updownarrow$$

$$1 \in \langle \mathbf{F}, x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle$$

Algorithm



2^k **systems in** $n - k$ **variables** $\rightsquigarrow$ **with no solutions?**

Hilbert Nullstellensatz

$\mathbf{F}(x_1, \ldots, x_{n-k}, a_{n-k+1}, \ldots, a_n)$ has no solution in $\mathbb{F}_2^{n-k}$

$$\Updownarrow$$

$$1 \in \langle \mathbf{F}, x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle$$

Can be tested by solving **a linear system** involving the **Macaulay matrix**

Algorithm BooleanSolve

Input: $m, n, k \in \mathbb{N}$ such that $m \geq n > k$
$f_1, \ldots, f_m$ quadratic polynomials in $\mathbb{F}_2[x_1, \ldots, x_n]$.
Output: The set of boolean solutions of the system $f_1 = \cdots = f_m = 0$.

Algorithm BooleanSolve

Input: $m, n, k \in \mathbb{N}$ such that $m \geq n > k$
$f_1, \ldots, f_m$ quadratic polynomials in $\mathbb{F}_2[x_1, \ldots, x_n]$.
Output: The set of boolean solutions of the system $f_1 = \cdots = f_m = 0$.

$S := \emptyset$.
$d_0 :=$ some integer. **(choice of a bound)**

Input: $m, n, k \in \mathbb{N}$ such that $m \geq n > k$
$f_1, \ldots, f_m$ quadratic polynomials in $\mathbb{F}_2[x_1, \ldots, x_n]$.
Output: The set of boolean solutions of the system $f_1 = \cdots = f_m = 0$.

$S := \emptyset$.
d_0:= some integer. **(choice of a bound)**

For all $(a_{n-k+1}, \ldots, a_n) \in \mathbb{F}_2^k$
For i from 1 to m **(specialization)**
$\tilde{f}_i(x_1, \ldots, x_{n-k}) := f_i(x_1, \ldots, x_{n-k}, a_{n-k+1}, \ldots, a_n) \in \mathbb{F}_2[x_1, \ldots, x_{n-k}]$.
EndFor

Algorithm BooleanSolve

Input: $m, n, k \in \mathbb{N}$ such that $m \geq n > k$
$f_1, \ldots, f_m$ quadratic polynomials in $\mathbb{F}_2[x_1, \ldots, x_n]$.
Output: The set of boolean solutions of the system $f_1 = \cdots = f_m = 0$.

$S := \emptyset$.
$d_0 :=$ some integer. **(choice of a bound)**

For all $(a_{n-k+1}, \ldots, a_n) \in \mathbb{F}_2^k$
    For i from 1 to m **(specialization)**
        $\tilde{f}_i(x_1, \ldots, x_{n-k}) := f_i(x_1, \ldots, x_{n-k}, a_{n-k+1}, \ldots, a_n) \in \mathbb{F}_2[x_1, \ldots, x_{n-k}]$.
    EndFor
    M := **boolean Macaulay matrix** of $(\tilde{f}_1, \ldots, \tilde{f}_m)$ in degree d_0.
    If the system $\mathbf{u} \cdot \mathrm{M} = \begin{pmatrix} 0 & \ldots & 0 & 1 \end{pmatrix}$ is inconsistent **(pruning)**
        T := solutions of the system $(\tilde{f}_1 = \cdots = \tilde{f}_m = 0)$ (exhaustive search).
        For all $(t_1, \ldots, t_{n-k}) \in T$
            $S := S \cup \{(t_1, \ldots, t_{n-k}, a_{n-k+1}, \ldots, a_n)\}$.
        EndFor
    EndIf
EndFor
Return S.

Work plan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\rightsquigarrow$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\rightsquigarrow$ $d_0 \sim M(\gamma)n$ when $k = (1-\gamma)n$
2. Sizes of the **Macaulay matrices** (function of k)?
3. Complexity of the **consistency tests** (function of k)?
   $O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$
4. Find optimal k for **asymptotic complexity**?
   - Gauss: $k = 0.73n$;
   - Coppersmith-Winograd: $k = 0.60n$
   - Wiedemann: $k = 0.45n$.
5. Degeneracy phenomenoms?
   $\rightsquigarrow$ γ-strong semi-regularity.
6. Feasibility and applications?

Work plan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\rightsquigarrow$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\rightsquigarrow$ $d_0 \sim M(\gamma)n$ when $k = (1-\gamma)n$
2. Sizes of the **Macaulay matrices** (function of k)?
3. Complexity of the **consistency tests** (function of k)?
   $O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$
4. Find optimal k for **asymptotic complexity**?
   - Gauss: $k = 0.73n$;
   - Coppersmith-Winograd: $k = 0.60n$
   - Wiedemann: $k = 0.45n$.
5. Degeneracy phenomenoms?
   $\rightsquigarrow$ γ-strong semi-regularity.
6. Feasibility and applications?

Work plan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\rightsquigarrow$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\rightsquigarrow$ $d_0 \sim M(\gamma)n$ when $k = (1-\gamma)n$
2. Sizes of the **Macaulay matrices** (function of k)?
3. Complexity of the **consistency tests** (function of k)?
   $O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$
4. Find optimal k for **asymptotic complexity**?
   - Gauss: $k = 0.73n$;
   - Coppersmith-Winograd: $k = 0.60n$
   - Wiedemann: $k = 0.45n$.
5. Degeneracy phenomenoms?
   $\rightsquigarrow$ γ-strong semi-regularity.
6. Feasibility and applications?

Work plan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\rightsquigarrow$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\rightsquigarrow$ $d_0 \sim M(\gamma)n$ when $k = (1-\gamma)n$
2. Sizes of the **Macaulay matrices** (function of k)?
3. Complexity of the **consistency tests** (function of k)?
   $O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$
4. Find optimal k for **asymptotic complexity**?
   - Gauss: $k = 0.73n$;
   - Coppersmith-Winograd: $k = 0.60n$
   - Wiedemann: $k = 0.45n$.
5. Degeneracy phenomenoms?
   $\rightsquigarrow$ γ-strong semi-regularity.
6. Feasibility and applications?

Work plan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\rightsquigarrow$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\rightsquigarrow$ $d_0 \sim M(\gamma)n$ when $k = (1-\gamma)n$
2. Sizes of the **Macaulay matrices** (function of k)?
3. Complexity of the **consistency tests** (function of k)?
   $O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$
4. Find optimal k for **asymptotic complexity**?
   - Gauss: $k = 0.73n$;
   - Coppersmith-Winograd: $k = 0.60n$
   - Wiedemann: $k = 0.45n$.
5. Degeneracy phenomenoms?
   $\rightsquigarrow$ γ-strong semi-regularity.
6. Feasibility and applications?

Work plan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\rightsquigarrow$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\rightsquigarrow$ $d_0 \sim M(\gamma)n$ when $k = (1-\gamma)n$
2. Sizes of the **Macaulay matrices** (function of k)?
3. Complexity of the **consistency tests** (function of k)?
   $O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$
4. Find optimal k for **asymptotic complexity**?
   - Gauss: $k = 0.73n$;
   - Coppersmith-Winograd: $k = 0.60n$
   - Wiedemann: $k = 0.45n$.
5. Degeneracy phenomenoms?
   $\rightsquigarrow$ γ-strong semi-regularity.
6. Feasibility and applications?

Complexity

Linear solving – Wiedemann's algorithm

A linear system $A \cdot \mathbf{x} = \mathbf{b}$ can be solved within $\widetilde{O}(\mathrm{size}(A)^2)$ operations and $\widetilde{O}(\mathrm{size}(A))$ **evaluations** of the linear function $\mathbf{u} \mapsto A \cdot \mathbf{u}$.

$\rightsquigarrow$ exploits the **sparsity** of the **Macaulay matrix**
$+$ **Certificates** (*Lobo/Giesbrecht/Saunders*)

Complexity

Linear solving – Wiedemann's algorithm

A linear system $A \cdot \mathbf{x} = \mathbf{b}$ can be solved within $\widetilde{O}(\mathrm{size}(A)^2)$ operations and $\widetilde{O}(\mathrm{size}(A))$ **evaluations** of the linear function $\mathbf{u} \mapsto A \cdot \mathbf{u}$.

$\rightsquigarrow$ exploits the **sparsity** of the **Macaulay matrix**
+ **Certificates** (*Lobo/Giesbrecht/Saunders*)

Complexity analysis

Under precise *algebraic assumptions*, if $m = n$, the **complexity** is

- $O\left(2^{0.841n}\right)$ with a **deterministic** variant;
- $O\left(2^{0.791n}\right)$ with a **probabilistic** variant.

+ **generalizations** when $m = \alpha n$ $(\alpha \geq 1)$.

Complexity

Linear solving – Wiedemann's algorithm

A linear system $A \cdot \mathbf{x} = \mathbf{b}$ can be solved within $\widetilde{O}(\mathrm{size}(A)^2)$ operations and $\widetilde{O}(\mathrm{size}(A))$ **evaluations** of the linear function $\mathbf{u} \mapsto A \cdot \mathbf{u}$.

$\rightsquigarrow$ exploits the **sparsity** of the **Macaulay matrix**
+ **Certificates** (*Lobo/Giesbrecht/Saunders*)

Complexity analysis

Under precise *algebraic assumptions*, if $m = n$, the **complexity** is

- $O\left(2^{0.841n}\right)$ with a **deterministic** variant;
- $O\left(2^{0.791n}\right)$ with a **probabilistic** variant.

+ **generalizations** when $m = \alpha n$ $(\alpha \geq 1)$.

Experiments

- **Algebraic assumptions** are verified with prob. close to 1.
- Probabilistic variant: when $n = m$, **more efficient** than exhaustive search when $n \geq 200 \rightsquigarrow$ Crypto applications (QUAD).

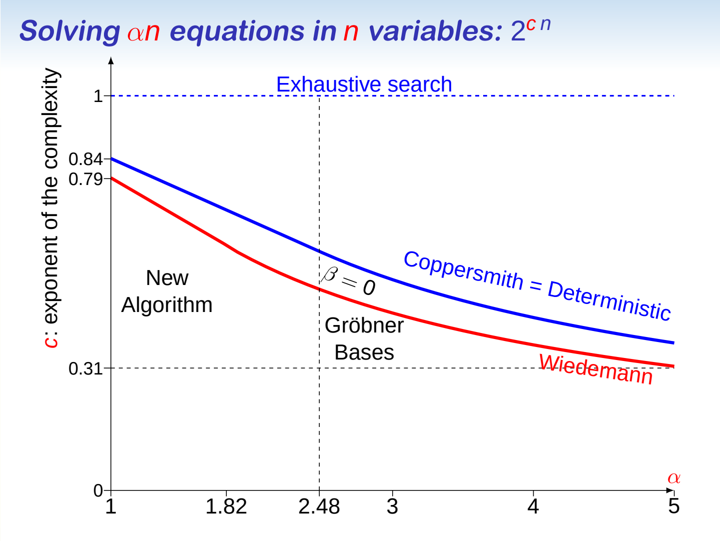


Figure: Exponent of the complexity in terms of α

Structures have an impact on the complexity of the solving process in algebraic cryptanalysis !

Design techniques, key **size reduction**,... $\overset{\text{Structure}}{\longleftrightarrow}$ potential **algebraic attacks**.

Structures have an impact on the complexity of the solving process in algebraic cryptanalysis !

Design techniques, key **size reduction**,... $\xleftrightarrow{\text{Structure}}$ potential **algebraic attacks**.

Algorithmic improvements

- Minrank Challenge $(8, 9, 5)$
  [Crypto 2008] **328233s** $\longrightarrow$ [Issac 2010] **935s** $\longrightarrow$ [Pasco 2010] **73s**

Conclusion and Perspectives

Structures have an impact on the complexity of the solving process in algebraic cryptanalysis !

Design techniques, key **size reduction**,... $\overset{\textbf{Structure}}{\longleftrightarrow}$ potential **algebraic attacks**.

Algorithmic improvements

- Minrank Challenge $(8, 9, 5)$
  [Crypto 2008] **328233s** $\longrightarrow$ [Issac 2010] **935s** $\longrightarrow$ [Pasco 2010] **73s**

Perspectives

- Dedicated F_5 algorithm for multi-homogeneous systems.
- Dedicated algorithm for **determinantal systems**?

Long term perspectives

Challenges

- **Systematic methodologies** for the analysis of **structures** (Hilbert series, degree of regularity, tools for commutative algebra and algebraic geometry, invariants,. . .).

Challenges

- Systematic methodologies for the analysis of **structures** (Hilbert series, degree of regularity, tools for commutative algebra and algebraic geometry, invariants,...).
- Impact of ring isomorphisms on Gröbner bases computations ($\rightsquigarrow$ **multivariate Cryptography**).

Long term perspectives

Challenges

- **Systematic methodologies** for the analysis of **structures** (Hilbert series, degree of regularity, tools for commutative algebra and algebraic geometry, invariants,...).
- Impact of **ring isomorphisms** on Gröbner bases computations ($\rightsquigarrow$ **multivariate Cryptography**).
- **Algorithmic framework** for structured systems and implementation (representation of polynomials, parallelism,...).

Challenges

- **Systematic methodologies** for the analysis of **structures** (Hilbert series, degree of regularity, tools for commutative algebra and algebraic geometry, invariants, . . .).
- Impact of **ring isomorphisms** on Gröbner bases computations ($\rightsquigarrow$ **multivariate Cryptography**).
- **Algorithmic framework** for structured systems and implementation (representation of polynomials, parallelism, . . .).

Thank you!