Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology

Jean–Charles Faugère Mohab Safey El Din
Pierre–Jean Spaenlehauer

UPMC – CNRS – INRIA Paris - Rocquencourt
LIP6 – SALSA team

ISSAC 2010
July 28, 2010

The *MinRank* problem

$r \in \mathbb{N}$. $M_0, \ldots, M_k$: $k+1$ matrices of size $m \times m$.

MinRank

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

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

- **Multivariate** generalization of the **EigenValue** problem.
- Applications in **cryptology**, **coding theory**, **geometry**, ...
  Kipnis/Shamir Crypto'99
  Faugère/Levy-dit-Vehel/Perret Crypto'08,...
- 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.

$$\mathbf{M} = M_0 - \sum_{i=1}^{k} \lambda_i M_i.$$

$$\mathbf{M} = M_0 - \sum_{i=1}^{k} \lambda_i M_i.$$

The minors modeling

$$\mathbf{Rank}(\mathbf{M}) \leq r$$

$$\Updownarrow$$

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

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

Few variables, lots of equations, high degree !!

$$\mathbf{M} = M_0 - \sum_{i=1}^{k} \lambda_i M_i.$$

The minors modeling

$$\mathbf{Rank}(\mathbf{M}) \leq r$$

$$\Updownarrow$$

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

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

Few variables, lots of equations, high degree !!

The Kipnis-Shamir modeling

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

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

- $m(m-r)$ bilinear equations.
- $k + r(m-r)$ variables.

$$\mathbf{M} = M_0 - \sum_{i=1}^{k} \lambda_i M_i.$$

The minors modeling

$$\mathbf{Rank}(\mathbf{M}) \leq r$$

$$\Updownarrow$$

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

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

Few variables, lots of equations, high degree !!

The Kipnis-Shamir modeling

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

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

- $m(m-r)$ bilinear equations.
- $k + r(m-r)$ variables.

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

Main results

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

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

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

	Minors	Kipnis-Shamir
Degree of regularity when $k=(m-r)^2$		$\mathrm{d_{reg}} \leq \boxed{\text{old}}\ m(m-r)+1$
# Sol		$< \boxed{\text{old}}\ \binom{m}{r}^{m-r}$
Complexity		

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

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

	Minors	Kipnis-Shamir	
Degree of regularity when $k=(m-r)^2$	New $\mathbf{r(m-r)+1}$	New $\mathbf{d_{reg}} \leq (\mathbf{m}-\mathbf{r})^2+\mathbf{1} \ll m(m-r)+1$	old
# Sol	New $\prod_{\mathbf{i=0}}^{\mathbf{m-r-1}} \frac{\mathbf{i!(m+i)!}}{\mathbf{(m-1-i)!(m-r+i)!}} < \binom{m}{r}^{m-r}$		old
Complexity			

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

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

	Minors	Kipnis-Shamir	
Degree of regularity when $k=(m-r)^2$	New $\mathbf{r(m-r)+1}$	New $\mathbf{d_{reg}} \leq (\mathbf{m}-\mathbf{r})^2+\mathbf{1}$	old $\ll m(m-r)+1$
# Sol	New $\prod_{\mathbf{i=0}}^{\mathbf{m-r-1}} \frac{\mathbf{i!(m+i)!}}{\mathbf{(m-1-i)!(m-r+i)!}}$		old $< \binom{m}{r}^{m-r}$
Complexity	$O(m^{\omega k})$	$O(m^{\omega(k+1)})$	

Main results

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

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

	Minors	Kipnis-Shamir	
Degree of regularity when $k=(m-r)^2$	New $\mathbf{r(m-r)+1}$	New $d_{reg} \leq (\mathbf{m}-\mathbf{r})^2+\mathbf{1}$	old $\ll m(m-r)+1$
# Sol	New $\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}$	old $< \binom{m}{r}^{m-r}$	
Complexity	$O(m^{\omega k})$	$O(m^{\omega(k+1)})$	

Both modelings $\longrightarrow$ polynomial complexity when $\mathbf{k}=(\mathbf{m}-\mathbf{r})^2$ is fixed.

New Crypto challenge broken: 10 generic matrices of size 11×11 target rank 8, $\mathbb{K}=\mathrm{GF}(65521)$.

Faugère/Safey/S.
Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and Complexity. *arXiv:1001.4004*

Theorem

For a **generic** affine 0-dimensional bilinear system over $\mathbb{K}[x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}]$,

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

Sharp bound in practice !

Faugère/Safey/S.
Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and Complexity. *arXiv:1001.4004*

Theorem

For a **generic** affine 0-dimensional bilinear system over $\mathbb{K}[x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}]$,

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

Sharp bound in practice !

Asymptotic complexity

Assumption: KS systems behave like generic affine bilinear systems.
When $k = (m-r)^2$ is fixed, the **complexity** of the **Gröbner basis** computation of the **Kipnis-Shamir** modeling is

$$O\left(\binom{2k + m(m-r) + 1}{(m-r)^2 + 1}^{\omega}\right) \underset{m \to \infty}{=} O\left(m^{\omega(k+1)}\right).$$

$$f_1 = \ldots = f_q = 0$$
Bilinear system of $\mathbb{K}[X, Y]$

$$\iff \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_q}{\partial x_0} & \cdots & \frac{\partial f_q}{\partial x_{n_x}} \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{n_x} \end{pmatrix} = 0.$$

$$f_1 = \ldots = f_q = 0$$
Bilinear system of $\mathbb{K}[X, Y]$

$$\iff \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_q}{\partial x_0} & \cdots & \frac{\partial f_q}{\partial x_{n_x}} \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{n_x} \end{pmatrix} = 0.$$

A Theorem of Bernstein, Sturmfels and Zelevinski

M a $p \times q$ **matrix** whose entries are **variables**. The maximal minors of M are a **universal** Gröbner basis of the associated ideal.

$$f_1 = \ldots = f_q = 0 \text{ Bilinear system of } \mathbb{K}[X, Y] \iff \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_X}} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_q}{\partial x_0} & \cdots & \frac{\partial f_q}{\partial x_{n_X}} \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{n_X} \end{pmatrix} = 0.$$

A Theorem of Bernstein, Sturmfels and Zelevinski

M a $p \times q$ **matrix** whose entries are **variables**. The maximal minors of M are a **universal** Gröbner basis of the associated ideal.

Theorem (Faugère/Safey/S. 2010)

M a k-variate $p \times q$ **linear matrix**. Generically, a grevlex GB of $\langle \text{Minors}(M) \rangle$: **linear combination** of the generators.

$$f_1 = \ldots = f_q = 0 \text{ Bilinear system of } \mathbb{K}[X, Y] \iff \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_q}{\partial x_0} & \cdots & \frac{\partial f_q}{\partial x_{n_x}} \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{n_x} \end{pmatrix} = 0.$$

A Theorem of Bernstein, Sturmfels and Zelevinski

M a $p \times q$ **matrix** whose entries are **variables**. The maximal minors of M are a **universal** Gröbner basis of the associated ideal.

Theorem (Faugère/Safey/S. 2010)

M a k-variate $p \times q$ **linear matrix**. Generically, a grevlex GB of $\langle \text{Minors}(M) \rangle$: **linear combination** of the generators.

Cramer's rule + **elimination** ideal $\rightarrow$ $\mathbf{d_{reg}} \leq \min(n_x, n_y) + 1$.

Related to **Determinantal ideals**.

What is known

- **Determinantal** ideals: *Bernstein/Zelevinsky* J. of Alg. Comb. 93, *Bruns/Conca* 98, *Sturmfels/Zelevinsky* Adv. Math. 98, *Conca/Herzog* AMS'94, *Lascoux* 78, *Abhyankar* 88...
- **Geometry** of determinantal varieties: *Room* 39, *Fulton* Duke Math. J. 91, *Giusti/Merle* Int. Conf. on Alg. Geo. 82...
- **Polar varieties**: *Bank/Giusti/Heintz/Safey/Schost* AAECC'10,*Bank/Giusti/Heintz/Pardo* J. of Compl. 05, *Safey/Schost* ISSAC'03, *Teissier* Pure and Appl. Math. 91...

Properties of determinantal ideals

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

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

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

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

$$\text{HS}_{\mathcal{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{(2m-r)r}}.$$

$$A_{i,j}(t) = \sum_{\ell} \binom{m-i}{\ell}\binom{m-j}{\ell} t^{\ell}.$$

Properties of determinantal ideals

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

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

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

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

$$\text{HS}_{\mathcal{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{(2m-r)r}}.$$

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

$$A_{i,j}(t) = \sum_{\ell} \binom{m-i}{\ell}\binom{m-j}{\ell} t^{\ell}.$$

Properties of determinantal ideals

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

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

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

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

$$\text{HS}_{\mathcal{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{(2m-r)r}}.$$

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

$$A_{i,j}(t) = \sum_{\ell} \binom{m-i}{\ell}\binom{m-j}{\ell} t^{\ell}.$$

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

Properties of determinantal ideals

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

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

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

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

$$\text{HS}_{\mathcal{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{(2m-r)r}}.$$

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

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

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

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

$$\text{HS}_{\mathcal{I}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{k-(m-r)^2}}.$$

$$A_{i,j}(t) = \sum_{\ell} \binom{m-i}{\ell}\binom{m-j}{\ell} t^{\ell}.$$

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

Degree of regularity for a 0-dim ideal $=$ 1$+$ degree of the **Hilbert series**.

Corollary

The **degree of regularity** of $\mathcal{I}$ is generically equal to

$$\mathbf{d_{reg}} = r(m-r)+1.$$

Degree of regularity for a 0-dim ideal $=$ 1$+$ degree of the **Hilbert series**.

Corollary

The **degree of regularity** of $\mathcal{I}$ is generically equal to

$$\mathbf{d_{reg}} = r(m-r)+1.$$

Number of matrices and rank defect fixed. 0-dimensional case.

Corollary: asymptotic complexity

When $k=(m-r)^2$ is fixed, then the **complexity** of the **Gröbner basis** computation of the **minors** modeling is

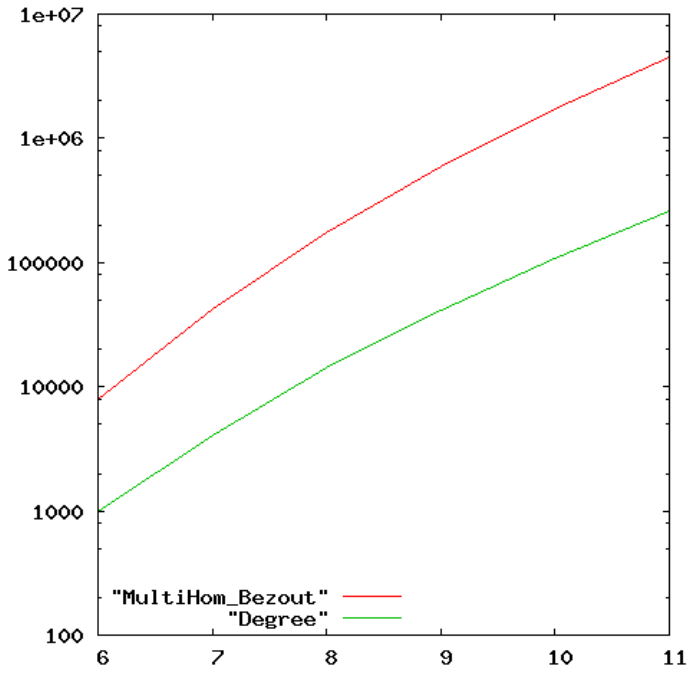
$$O\left(\binom{k+m(m-r)+1}{k}^{\omega}\right) \underset{m\to\infty}{=} O\left(m^{\omega k}\right).$$

Generic number of solutions

The **number of solutions** of a **generic MinRank** problem with $k = (m-r)^2$ is

$$\#Sol = \prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}$$

$$\underset{m\to\infty}{\sim} m^k \prod_{i=0}^{m-r-1} \frac{i!}{(m-r+i)!}.$$



Complexity of the change of ordering

The **complexity of FGLM** is $O\left(\#Sol^{\omega}\right)$. If $k = (m-r)^2$, then

$$O\left(\#Sol^{\omega}\right) = O\left(m^{\omega k}\right).$$

Summary

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

Summary

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

	Minors	Kipnis-Shamir
Degree of regularity when $k=(m-r)^2$	$r(m-r)+1$	$\leq (m-r)^2+1$
# Sol	$\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}$	
Complexity	$O(m^{\omega k})$	$O(m^{\omega(k+1)})$

Complexity of the **change of ordering**: $O\left(m^{\omega k}\right)$.

Summary

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

	Minors	Kipnis-Shamir
Degree of regularity when $k=(m-r)^2$	$r(m-r)+1$	$\leq (m-r)^2+1$
# Sol	$\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}$	
Complexity	$O(m^{\omega k})$	$O(m^{\omega(k+1)})$

Complexity of the **change of ordering**: $O\left(m^{\omega k}\right)$.

Over-determined systems: $k<(m-r)^2$.

Experimental results

Courtois. Asiacrypt'01.

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

$\mathbb{K} = \mathbf{GF(65521)}$ $(\mathbf{m}, \mathbf{k}, \mathbf{r})$: $k+1$ matrices of size $m \times m$. Target rank: r.

Challenge	**A**	**B**				**C**
	$(6,9,3)$	$(7,9,4)$	$(8,9,5)$	$(9,9,6)$	$(10,9,7)$	$(11,9,8)$
degree	**980**	**4116**	**14112**	**41580**	**108900**	259545
MH Bézout	8000	42875	175616	592704	1728000	4492125
	Minors					
F_5 time	**1.1s**	**37s**	**935s**	**18122s**	**229094s**	
F_5 mem	**488 MB**	**587 MB**	**1213 MB**	**5048 MB**	**25719MB**	
$\log_2$(Nb op.)	**21.5**	**25.9**	**29.2**	**32.7**	**35.2**	
FGLM time	**1.7s**	**97.2s**				
	Kipnis-Shamir					
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.

$\mathbb{K} = \mathbf{GF(65521)}$ $(\mathbf{m}, \mathbf{k}, \mathbf{r})$: $k+1$ matrices of size $m \times m$. Target rank: r.

Challenge	**A**	**B**				**C**
	$(6,9,3)$	$(7,9,4)$	$(8,9,5)$	$(9,9,6)$	$(10,9,7)$	$(11,9,8)$
degree	**980**	**4116**	**14112**	**41580**	**108900**	259545
MH Bézout	8000	42875	175616	592704	1728000	4492125
	Minors					
F_5 time	**1.1s**	**37s**	**935s**	**18122s**	**229094s**	
F_5 mem	**488 MB**	**587 MB**	**1213 MB**	**5048 MB**	**25719MB**	
$\log_2$(Nb op.)	**21.5**	**25.9**	**29.2**	**32.7**	**35.2**	
FGLM time	**1.7s**	**97.2s**				
	Kipnis-Shamir					
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.

Experimental results

Courtois. Asiacrypt'01.

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

$\mathbb{K} = \mathbf{GF(65521)}$ $(\mathbf{m}, \mathbf{k}, \mathbf{r})$: $k+1$ matrices of size $m \times m$. Target rank: r.

Challenge	**A**	**B**				**C**
	$(6,9,3)$	$(7,9,4)$	$(8,9,5)$	$(9,9,6)$	$(10,9,7)$	$(11,9,8)$
degree	**980**	**4116**	**14112**	**41580**	**108900**	259545
MH Bézout	8000	42875	175616	592704	1728000	4492125
	Minors					
F_5 time	**1.1s**	**37s**	**935s**	**18122s**	**229094s**	
F_5 mem	**488 MB**	**587 MB**	**1213 MB**	**5048 MB**	**25719MB**	
$\log_2$(Nb op.)	**21.5**	**25.9**	**29.2**	**32.7**	**35.2**	
FGLM time	**1.7s**	**97.2s**				
	Kipnis-Shamir					
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.

Conclusion

- **Comparison** of two **algebraic** formulations.
- Complexity results on the **MinRank** problem from the **Gröbner basis** viewpoint.
- Lead to significant **algorithmic** improvements confirmed by **experiments**.
- Algebraic **cryptanalysis** of the **Courtois authentification scheme**.

Conclusion

- **Comparison** of two **algebraic** formulations.
- Complexity results on the **MinRank** problem from the **Gröbner basis** viewpoint.
- Lead to significant **algorithmic** improvements confirmed by **experiments**.
- Algebraic **cryptanalysis** of the **Courtois authentification scheme**.

Further algorithmic improvements

- Minrank Challenge $(8, 9, 5)$
  [Crypto 2008] **328233s** $\longrightarrow$ [Issac 2010] **935s** $\longrightarrow$ [Pasco 2010] **73s**
- **Multi-homogeneous** variant of the F_5 algorithm.

Conclusion

- **Comparison** of two **algebraic** formulations.
- Complexity results on the **MinRank** problem from the **Gröbner basis** viewpoint.
- Lead to significant **algorithmic** improvements confirmed by **experiments**.
- Algebraic **cryptanalysis** of the **Courtois authentification scheme**.

Further algorithmic improvements

- Minrank Challenge $(8, 9, 5)$
  [Crypto 2008] **328233s** $\longrightarrow$ [Issac 2010] **935s** $\longrightarrow$ [Pasco 2010] **73s**
- **Multi-homogeneous** variant of the F_5 algorithm.

Perspectives

- Practical **bottleneck** for MinRank: computing the minors.
- Extension to **polynomial** matrices/Computation of **critical points**.
- **Symmetric** matrices.