Gröbner Bases of Bihomogeneous Ideals Generated by Polynomials of Bidegree (1,1): Algorithms, Complexity and Applications

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

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

Séminaire Algorithms – INRIA
2010/04/26

Bilinear polynomials

Bihomogeneous

$$f(x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}) = \sum a_{i,j} x_i y_j.$$

Affine

$$f^{(a)}(x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}) = f^{(h)}(1, x_1, \ldots, x_{n_x}, 1, y_1, \ldots, y_{n_y}).$$

- **Important class** of polynomials.
- Often encountered in practice.
- Different nature of the variables.
- Related to determinantal ideals.

- Cryptanalysis of **MinRank**
  [*Faugère/Levy/Perret* CRYPTO'08, *Faugère/Safey/S.* ISSAC'10].
- Cryptanalysis of **MacEliece**
  [*Faugère/Otmani/Perret/Tilich* EUROCRYPT'10].
- Real algebraic **geometry**
  [*Safey/Trébuchet* 06, *Bank/Giusti/Heintz/Safey/Schost* AAECC'10].

MinRank *(linear algebra, cryptology, coding theory)*

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

$$\text{Rank}\left(\sum_{i=1}^{k} \lambda_i M_i\right) \leq r \Rightarrow \left(\sum_{i=1}^{k} \lambda_i M_i\right) x^{(j)} = 0.$$

Extension: **Lagrange multipliers** *(geometry, optimisation)*

Maximize $f(x)$ with the constraints $g_i(x) = 0$:

$$\text{grad}\left(\lambda_0 f(x) + \sum \lambda_i g_i(x)\right) = 0.$$

Macaulay matrix in degree d

$I = \langle f_1, \ldots, f_p \rangle$ $\quad \deg(f_i) = d_i$ $\quad \succ$ a monomial ordering

Rows: all products tf_i where $t \in \text{Monomials}(d - d_i)$.
Columns: monomials of degree d.

$$\begin{array}{c} \\ t_1 f_1 \\ \vdots \\ t_k f_p \end{array} \begin{array}{c} m_1 \succ \cdots \succ m_\ell \\ \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} \end{array}$$

row echelon forms of the **Macaulay matrices** $\Longrightarrow$ **Gröbner basis**.

Macaulay matrix in degree d

$$I = \langle f_1, \ldots, f_p \rangle \qquad \deg(f_i) = d_i \qquad \succ \text{ a monomial ordering}$$

Rows: all products tf_i where $t \in \text{Monomials}(d - d_i)$.
Columns: monomials of degree d.

$$\begin{array}{c} \\ t_1 f_1 \\ \vdots \\ t_k f_p \end{array} \begin{array}{c} m_1 \succ \cdots \succ m_\ell \\ \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} \end{array}$$

row echelon forms of the **Macaulay matrices** $\Longrightarrow$ **Gröbner basis**.

Problem

Rank defect $\Longrightarrow$ useless computations.

tf_i **reduces to zero**: the associated row in the Macaulay matrix becomes zero after reduction.

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

- New theoretical **complexity bounds**. Confirmed by experiments.
- New classes of bilinear systems which can be solved in polynomial time.
- Direct application to **Crypto** problems.

Definition

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

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

Previous work

- Multihomogeneous **elimination** [*Rémond* 01].
- Multihomogeneous **Bézout** theorem [*VanDerWaerden* 28, *Safey/Trébuchet* 06].
- Multihomogeneous **homotopy** methods [*Morgan/Sommese* Applied Math. and Comp. 87, *Wampler* Num. Math. 93].
- Multihomogeneous **resultants** [*Canny/Emiris* JSC'95, *Dickenstein/Emiris* JSC'03, *Mantzaflaris/Emiris* ISSAC'09, *Jeronimo/Sabia* JSC'07, *McCoy* AMS'33, *Weyman/Zelevinski* J. of Alg. Geom. 94].

Gröbner bases

I a **polynomial ideal**. Gröbner basis (w.r.t. a monomial ordering): $G \subset I$ a finite set of polynomials such that $\mathrm{LM}(I) = \langle \mathrm{LM}(G) \rangle$.

- **Buchberger** [*Buchberger* Ph.D. 65].
- $\mathbf{F_4}$ [*Faugère* J. of Pure and Appl. Alg. 99].
- $\mathbf{F_5}$ [*Faugère* ISSAC'02].

$\longrightarrow$ Polynomial System Solving.

Study of a class of systems from the viewpoint of **Gröbner bases**:

1. Avoid computing **zero**.

Study of a class of systems from the viewpoint of **Gröbner bases**:

1. Avoid computing **zero**.
2. Characterize a "nice" subclass of systems.

Study of a class of systems from the viewpoint of **Gröbner bases**:

1. Avoid computing **zero**.
2. Characterize a "nice" subclass of systems.
3. Generic **Hilbert series**.

Study of a class of systems from the viewpoint of **Gröbner bases**:

1. Avoid computing **zero**.
2. Characterize a "nice" subclass of systems.
3. Generic **Hilbert series**.
4. Complexity analysis.

F_5 *criterion: mathematical formulation*

If $t \in \mathbf{LM}(\langle f_1, \ldots, f_{i-1} \rangle)$, then the row tf_i is reduced to zero.

F_5 *criterion: mathematical formulation*

If $t \in \mathbf{LM}(\langle f_1, \ldots, f_{i-1} \rangle)$, then the row tf_i is reduced to zero.

F_5 *criterion: algorithm*

Iterative computations of
$\mathbf{GB}(\langle f_1 \rangle), \mathbf{GB}(\langle f_1, f_2 \rangle), \ldots, \mathbf{GB}(\langle f_1, \ldots, f_p \rangle)$.

$\exists g \in \mathbf{GB}(\langle f_1, \ldots, f_{i-1} \rangle)\, s.t.\, \mathbf{LM}(g)$ divides $t \Rightarrow tf_i$ reduces to zero.

"Optimal" for regular (and semi-regular) homogeneous systems, but...

F_5 *criterion: mathematical formulation*

If $t \in \mathbf{LM}(\langle f_1, \ldots, f_{i-1} \rangle)$, then the row tf_i is reduced to zero.

F_5 *criterion: algorithm*

Iterative computations of
$\mathbf{GB}(\langle f_1 \rangle), \mathbf{GB}(\langle f_1, f_2 \rangle), \ldots, \mathbf{GB}(\langle f_1, \ldots, f_p \rangle)$.

$\exists g \in \mathbf{GB}(\langle f_1, \ldots, f_{i-1} \rangle)\, s.t.\, \mathbf{LM}(g)$ divides $t \Rightarrow tf_i$ reduces to zero.

"Optimal" for regular (and semi-regular) homogeneous systems, but...
bilinear systems are **not regular** !

$F = (f_1, \ldots, f_m)$: system of **bilinear equations**.

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

Euler relations

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

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

Euler relations

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

$$(s_1, \ldots, s_i) \in \mathbf{Syz}(f_1, \ldots, f_i) \Longleftrightarrow \sum_{k=1}^{i} s_k f_k = 0.$$

tf_i reduces to zero iff $\exists (s_1, \ldots, s_i) \in \mathbf{Syz}(f_1, \ldots, f_i)$ s.t. $\mathrm{LM}(s_i) = t$.

Euler relations

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

$$(s_1, \ldots, s_i) \in \mathbf{Syz}(f_1, \ldots, f_i) \Longleftrightarrow \sum_{k=1}^{i} s_k f_k = 0.$$

tf_i reduces to zero iff $\exists (s_1, \ldots, s_i) \in \mathbf{Syz}(f_1, \ldots, f_i)$ s.t. $\mathrm{LM}(s_i) = t$.

$(s_1, \ldots, s_i) \in \mathrm{Ker}_L(\mathrm{jac}_X(F_i))$ (resp. $\mathrm{Ker}_L(\mathrm{jac}_Y(F_i))$)
$\Rightarrow (s_1, \ldots, s_i) \in \mathbf{Syz}(f_1, \ldots, f_i)$.

Kernel of matrices whose entries are linear forms

k-variate **linear matrices** of size $p \times q$.

Proposition (Cramer's Rule)

If $p = q + 1$, then the **left kernel** of a **generic linear matrix** is generated a vector of **maximal minors**.

k-variate **linear matrices** of size $p \times q$.

Conjecture

If $p - q \geq k - 1$, then the **left kernel** of a **generic linear matrix** is generated by vectors of **maximal minors**.

Supported by experiments.

F_5 criterion

$t \in \mathrm{LM}(\langle f_1, \ldots, f_{i-1} \rangle) \Rightarrow t f_i$ **reduces to zero**.

$f_i f_j - f_j f_i = 0$.

Extended criterion

$t \in \mathrm{LM}(\langle \mathrm{Minors}(\mathrm{jac}_X(F_{i-1})) \rangle) \cup \mathrm{LM}(\langle \mathrm{Minors}(\mathrm{jac}_Y(F_{i-1})) \rangle) \Rightarrow t f_i$ **reduces to zero**.

Syzygies in $\mathrm{Ker}_L(\mathrm{jac}_X(F_i))$ and $\mathrm{Ker}_L(\mathrm{jac}_Y(F_i))$.

F_5 criterion

The **Gröbner bases** $\mathrm{GB}(f_1), \mathrm{GB}(f_1, f_2), \ldots, \mathrm{GB}(f_1, \ldots, f_m)$ are computed **iteratively**.

Extended criterion

Precompute $\mathrm{GB}(\langle \mathrm{Minors}(\mathrm{jac}_X(F_{i-1})) \rangle)$ and $\mathrm{GB}(\langle \mathrm{Minors}(\mathrm{jac}_Y(F_{i-1})) \rangle)$

What cost ?

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...
- **Geometry** of determinantal varieties: *Room* 39, *Fulton* Duke Math. J. 91, *Giusti/Merle* Int. Conf. on Alg. Geo. 82...
- **Polar varieties**: *Bank/Giusti/Heintz/Pardo* J. of Compl. 05, *Safey/Schost* ISSAC'03, *Teissier* Pure and Appl. Math. 91...

A Theorem of Bernstein, Sturmfels and Zelevinski

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

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...
- **Geometry** of determinantal varieties: *Room* 39, *Fulton* Duke Math. J. 91, *Giusti/Merle* Int. Conf. on Alg. Geo. 82...
- **Polar varieties**: *Bank/Giusti/Heintz/Pardo* J. of Compl. 05, *Safey/Schost* ISSAC'03, *Teissier* Pure and Appl. Math. 91...

A variant of a Theorem of Bernstein, Sturmfels and Zelevinski

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

$$\Longrightarrow \text{LM}(\text{Minors}(M)) = \langle \text{Monomials}_{p-q+1}(q) \rangle.$$

Algorithm – criterion

- **Maximal minors** of $\mathrm{jac}_Y(F_{i-1})$ (polynomials of degree $n_y + 1$).
- Gauss reduction.
- t is a leading monomial $\Rightarrow$ tf_i **reduces to zero**.
- Symetrically, same process with $\mathrm{jac}_X(F_{i-1})$.

Program

1. Avoid computing **zero**. ✓
2. Characterize a "nice" subclass of systems.
3. Generic **Hilbert series**.
4. Complexity analysis.

Weak biregularity: definition

$$sf_i = 0 \mod \langle f_1, \ldots, f_{i-1} \rangle \Rightarrow \begin{cases} s = 0 \mod \langle f_1, \ldots, f_{i-1} \rangle \\ s \in \langle \mathrm{Minors}(\mathrm{jac}_X(F_{i-1})) \rangle \\ s \in \langle \mathrm{Minors}(\mathrm{jac}_Y(F_{i-1})) \rangle \end{cases}$$

Weak biregularity: definition

$$sf_i = 0 \mod \langle f_1, \ldots, f_{i-1} \rangle \Rightarrow \begin{cases} s = 0 \mod \langle f_1, \ldots, f_{i-1} \rangle \\ s \in \langle \text{Minors}(\text{jac}_X(F_{i-1})) \rangle \\ s \in \langle \text{Minors}(\text{jac}_Y(F_{i-1})) \rangle \end{cases}$$

Grevlex ordering.

Theorem: generic reductions to 0

For a generic **bilinear system** $f_1, \ldots, f_m$, the reductions to zero **not detected** by the F_5 criterion are:

$$\{tf_i \mid i > n_y + 1, t \in \text{Monomials}^X_{i-n_y-2}(n_y + 1)\}$$

$$\bigcup \{tf_i \mid i > n_x + 1, t \in \text{Monomials}^Y_{i-n_x-2}(n_x + 1)\}$$

Weak biregularity: definition

$$sf_i = 0 \mod \langle f_1, \ldots, f_{i-1} \rangle \Rightarrow \begin{cases} s = 0 \mod \langle f_1, \ldots, f_{i-1} \rangle \\ s \in \langle \text{Minors}(\text{jac}_X(F_{i-1})) \rangle \\ s \in \langle \text{Minors}(\text{jac}_Y(F_{i-1})) \rangle \end{cases}$$

Grevlex ordering.

Strong biregularity: computational definition

The bilinear system $f_1, \ldots, f_m$ is **biregular** if the reductions to zero not detected by the F_5 criterion are:

$$\{tf_i \mid i > n_y + 1, t \in \text{Monomials}^X_{i-n_y-2}(n_y + 1)\}$$

$$\bigcup \{tf_i \mid i > n_x + 1, t \in \text{Monomials}^Y_{i-n_x-2}(n_x + 1)\}$$

Extended criterion for biregular systems $\longrightarrow$ **no reduction to zero**.

Theorem

Generically, **bilinear systems** are **biregular**, i.e. the set of biregular bilinear systems is a **Zariski nonempty open subset**.

Program

1. Avoid computing **zero**. ✓
2. Characterize a "nice" subclass of systems. ✓
3. Generic **Hilbert series**.
4. Complexity analysis.

Hilbert biseries:

$$\mathrm{HS}_I(t_1, t_2) = \sum \dim(\mathbb{K}[X, Y]_{\alpha,\beta}/I_{\alpha,\beta}) t_1^{\alpha} t_2^{\beta}$$

- Generating series of the **rank defects** of the Macaulay matrices.
- **Complexity analysis** [*Bardet/Faugère/Salvy* ISCPP'04].

Biseries of bilinear systems

$$\mathrm{HS}_I(t_1, t_2) = \frac{Q(t_1, t_2)}{(1 - t_1)^{n_x+1}(1 - t_2)^{n_y+1}}$$

Hilbert biseries:

$$\mathrm{HS}_I(t_1, t_2) = \sum \dim(\mathbb{K}[X, Y]_{\alpha,\beta}/I_{\alpha,\beta}) t_1^\alpha t_2^\beta$$

- Generating series of the **rank defects** of the Macaulay matrices.
- **Complexity analysis** [*Bardet/Faugère/Salvy* ISCPP'04].

Biseries of generic bilinear systems

If $f_1, \ldots, f_m$ is a **biregular bilinear system**, then the **biseries** of $I = \langle f_1, \ldots, f_m \rangle$ is:

$$\mathbf{HS}_I(t_1, t_2) = \frac{(1 - t_1 t_2)^m + \mathbf{F}(t_1, t_2, n_x, n_y) + \mathbf{F}(t_2, t_1, n_y, n_x)}{(1 - t_1)^{n_x+1}(1 - t_2)^{n_y+1}},$$

$$\mathbf{F}(t_1, t_2, n_x, n_y) = \sum_{\ell=1}^{m-(n_y+1)} (1 - t_1 t_2)^{m-(n_y+1)-\ell} t_1 t_2 (1 - t_2)^{n_y+1} [1 - (1 - t_1)^\ell \sum_{k=1}^{n_y+1} t_1^{n_y+1-k} \binom{\ell+n_y-k}{n_y+1-k}].$$

$$\mathbb{K}[X,Y]/I_{m-1} \xrightarrow{\times f_m} \mathbb{K}[X,Y]/I_{m-1}.$$

Generating series of the kernel

$$\mathbf{G}^{(m)}(t_1,t_2) = \sum \dim(\mathrm{Ker}(\times f_m)_{d_1,d_2})\, t_1^{d_1} t_2^{d_2}.$$

Recurrence

$$\mathbf{HS}_{I_m}(t_1,t_2) = (1-t_1t_2)\mathbf{HS}_{I_{m-1}} + t_1t_2\mathbf{G}^{(m-1)}(t_1,t_2).$$

A property of the syzygy module

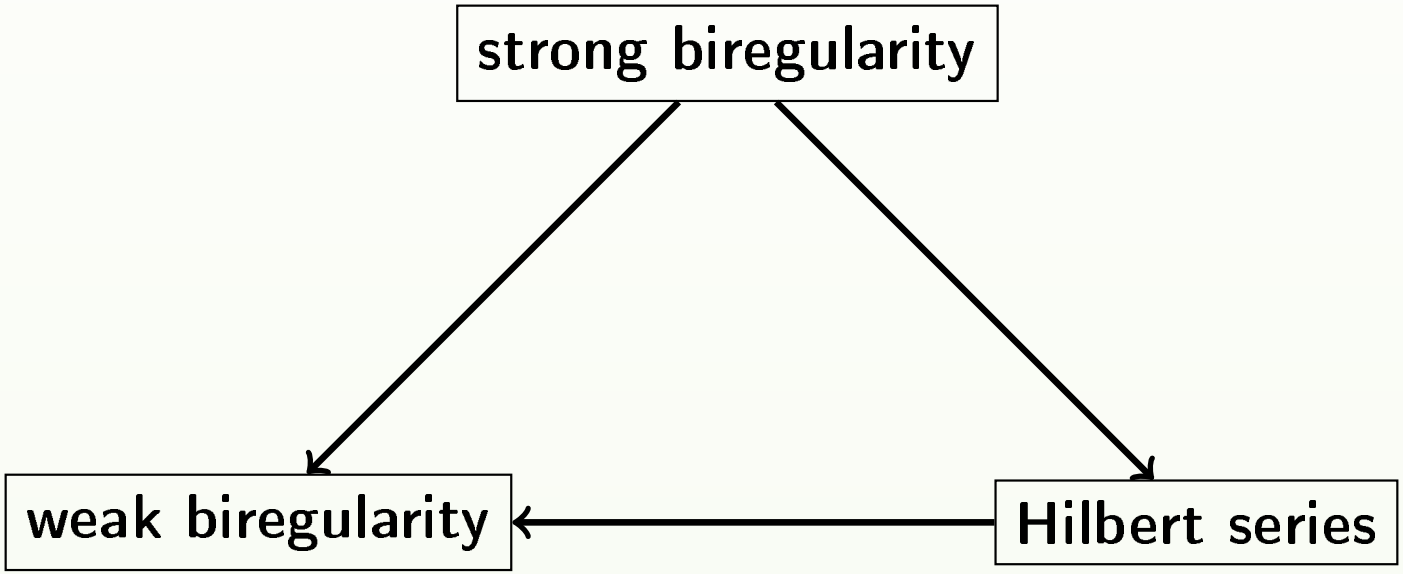
$$\mathrm{Ker}(\times f_m) = (\mathrm{Ker}(\times f_m) \cap \mathbb{K}[X]) \cup (\mathrm{Ker}(\times f_m) \cap \mathbb{K}[Y]).$$

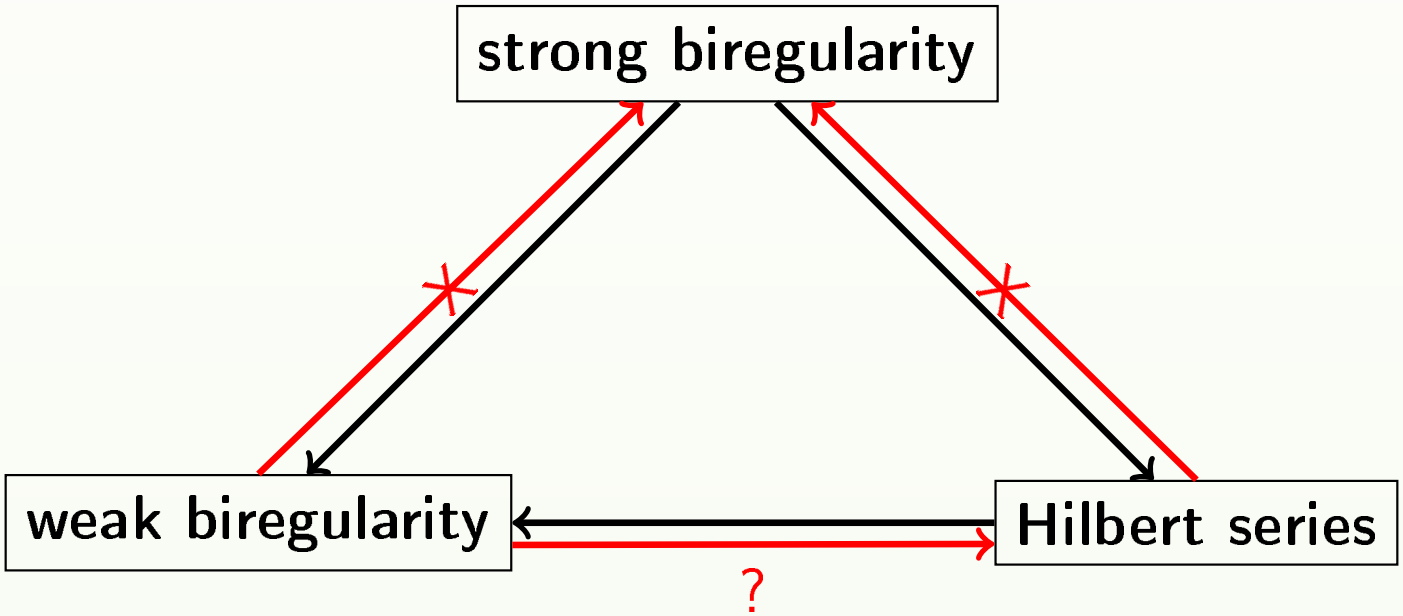
$$\Rightarrow G^{(m)}(t_1,t_2) = g_x^{(m)}(t_1) + g_y^{(m)}(t_2)$$

Finding $G^{(m)}(t_1, t_2)$

$G^{(m)}(t_1, t_2) = g_x^{(m)}(t_1) + g_y^{(m)}(t_2)$, where $g_x^{(m)}(t)$ (resp. $g_y^{(m)}(t)$) is the **generating series** of $\text{Monomials}_{m-n_x-1}(n_y+1)$ (resp. $\text{Monomials}_{m-n_y-1}(n_x+1)$):

$$\mathbf{g_x^{(m)}(t)} = \begin{cases} 0 \text{ if } m < n_y \\ \dfrac{1}{(1-t)^{n_x+1}} - \displaystyle\sum_{1 \le j \le n_y+1} \dfrac{\binom{m-j}{n_y+1-j} t^{n_y+1-j}}{(1-t)^{n_x+n_y-m+1}} \end{cases}$$


strong biregularity
weak biregularity
Hilbert series


strong biregularity
weak biregularity
Hilbert series
?

1. Avoid computing **zero**. ✓
2. Characterize a "nice" subclass of systems. ✓
3. Generic **Hilbert series**. ✓
4. Complexity analysis.

Theorem: degree of regularity

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

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

Sharp bound in practice.

Theorem: regularity

Generic **affine bilinear systems** are **regular** $\Rightarrow$ No reduction to zero during the $\mathbf{F_5}$ **Algorithm**.

Solving affine bilinear systems

The **complexity** of computing a grevlex Gröbner basis of a **zero-dimensional ideal** generated by generic affine bilinear polynomials is **upper bounded** by:

$$O(\text{Monomials}(d_{reg})^{\omega}).$$

Solving affine bilinear systems

The **complexity** of computing a grevlex Gröbner basis of a **zero-dimensional ideal** generated by generic affine bilinear polynomials is **upper bounded** by:

$$O(\text{Monomials}(\min(n_x + 1, n_y + 1))^\omega) \approx O\left(2^{\omega \min(n_x, n_y)}\right).$$

Solving affine bilinear systems

The **complexity** of computing a grevlex Gröbner basis of a **zero-dimensional ideal** generated by generic affine bilinear polynomials is **upper bounded** by:

$$O(\text{Monomials}(\min(n_x + 1, n_y + 1))^\omega) \approx O\left(2^{\omega \min(n_x, n_y)}\right).$$

- n_x constant, n_y grows $\Longrightarrow$ complexity polynomial in n_y.
- X and Y unbalanced $\Rightarrow$ **easy to solve**.
- Better than **Macaulay bound**:

$$O(\text{Monomials}(n_x + n_y + 1)^\omega) \approx O\left(2^{\omega(n_x + n_y)}\right).$$

- Complexity observed in practice !!!

Program

1. Avoid computing **zero**. ✓
2. Characterize a "nice" subclass of systems. ✓
3. Generic **Hilbert series**. ✓
4. Complexity analysis. ✓

[*Buss/Frandsen/Shallit* 96, *Courtois* Ph.D. 01, *Faugère/Levy-dit-Vehel/Perret* CRYPTO'08, *Kipnis/Shamir* CRYPTO'99]

MinRank

$M_0, \ldots, M_k$ are $k+1$ matrices $n \times n$. Given r, find $\lambda_1, \ldots, \lambda_k$ such that

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

- Fundamental **NP-hard** problem in linear algebra.
- Important problem in **multivariate cryptology**.
- Applications in **geometry**.
- Generalization of the **Eigenvalue problem**.

The Kipnis-Shamir modeling

Solve the system

$$\begin{pmatrix} m_{1,1}^{(0)} - \sum \lambda_i m_{1,1}^{(i)} & \dots & m_{1,n}^{(0)} - \sum \lambda_i m_{1,n}^{(i)} \\ \vdots & \ddots & \vdots \\ m_{n,1}^{(0)} - \sum \lambda_i m_{n,1}^{(i)} & \dots & m_{n,n}^{(0)} - \sum \lambda_i m_{n,n}^{(i)} \end{pmatrix} \cdot \begin{pmatrix} & I_{n-r} & \\ x_1^{(1)} & \dots & x_1^{(n-r)} \\ \vdots & \vdots & \vdots \\ x_r^{(1)} & \dots & x_r^{(n-r)} \end{pmatrix} = 0.$$

- polynomials are **bilinear** "by blocks".
- $\longrightarrow$ can be solved in time **polynomial** in n when the number of λ is constant.
- **Minors modeling**.

Faugère, Safey, S.
Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology.
ISSAC 2010.

Conclusion

- Solving bilinear systems using **Gröbner bases** algorithms...
- ... from **theoretical** and **practical** viewpoints.
- Applications to a concrete problem in **cryptology**.
- **Multihomogeneous** structure of the Macaulay matrices $\longrightarrow$ speed-up the computation of the **row echelon forms** (not in this talk).

What remains to do ?

- Proof of the **conjecture** about the kernel of linear matrices.
- Equivalence Hilbert series – weak biregularity ?
- **Degree of regularity** for homogeneous bilinear systems.

Perspectives

- Generalization to **multihomogeneous systems** ?
- Properties of **determinantal** ideals ?
- **Applications** ?