Gröbner Bases. Applications in Cryptology

Jean-Charles Faugère
INRIA, Université Paris 6, CNRS

Ecrypt 2007 - Samos

Properties of Gröbner bases I

$\mathbb{K}$ a field, $\mathbb{K}[x_1, \ldots, x_n]$ polynomials in n variables.

Linear systems	Polynomial equations
$\begin{cases} l_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ l_m(x_1, \ldots, x_n) = 0 \end{cases}$	$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$
$V = \mathrm{Vect}_{\mathbb{K}}(l_1, \ldots, l_m)$	Ideal generated by f_i: $I = \mathrm{Id}(f_1, \ldots, f_m)$
Triangular/diagonal basis of V	Gröbner basis of I

Definition (Buchberger)

$<$ admissible ordering (lexicographical, total degree, DRL)

$G \subset \mathbb{K}[x_1, \ldots, x_n]$ is a Gröbner basis of an ideal I if

$$\forall f \in I, \text{ exists } g \in G \text{ such that } \underset{<}{\mathrm{LT}}(g) \mid \underset{<}{\mathrm{LT}}(f)$$

Properties of Gröbner bases II

Solving algebraic systems:
Computing the algebraic variety: $\mathbb{K} \subset \mathbb{L}$ (for instance $\mathbb{L}=\overline{\mathbb{K}}$ the algebraic closure)

$$V_{\mathbb{L}} = \{(z_1, \ldots, z_n) \in \mathbb{L}^n \mid f_i(z_1, \ldots, z_n) = 0, \quad i = 1, \ldots, m\}$$

Solutions in finite fields:
We compute the Gröbner basis of $G_{\mathbb{F}_2}$ of $[f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n]$, in $\mathbb{F}_2[x_1, \ldots, x_n]$. It is a description of all the solutions of $V_{\mathbb{F}_2}$.

Properties of Gröbner bases III

Theorem

- $V_{\mathbb{F}_2} = \emptyset$ *(no solution) iff* $G_{\mathbb{F}_2} = [1]$.
- $V_{\mathbb{F}_2}$ *has exactly one solution iff* $G_{\mathbb{F}_2} = [x_1 - a_1, \ldots, x_n - a_n]$ *where* $(a_1, \ldots, a_n) \in \mathbb{F}_2^n$.

Shape position:
If $m \geq n$ and the number of solutions is finite ($\#V_K < \infty$), then *in general* the shape of a lexicographical Gröbner basis: $x_1 > \cdots > x_n$:

$$\text{Shape Position} \begin{cases} h_n(x_n)(=0) \\ x_{n-1} - h_{n-1}(x_n)(=0) \\ \vdots \\ x_1 - h_1(x_n)(=0) \end{cases}$$

Solving zero-dimensional system

When $\dim(I) = 0$ (finite number of solutions); in general:

- It is easier to compute a Gröbner Basis of I for a total degree ($<_{\mathrm{DRL}}$) ordering
- Triangular structure of Gb valid only for a lex. ordering:

$$\text{Shape Position} \begin{cases} h_n(x_n) = 0 \\ x_{n-1} = h_{n-1}(x_n) \\ \vdots \\ x_1 = h_1(x_n) \end{cases}$$

Dedicated Algorithm: efficiently change the ordering

FGLM, Gröbner Walk, LLL, ...

FGLM

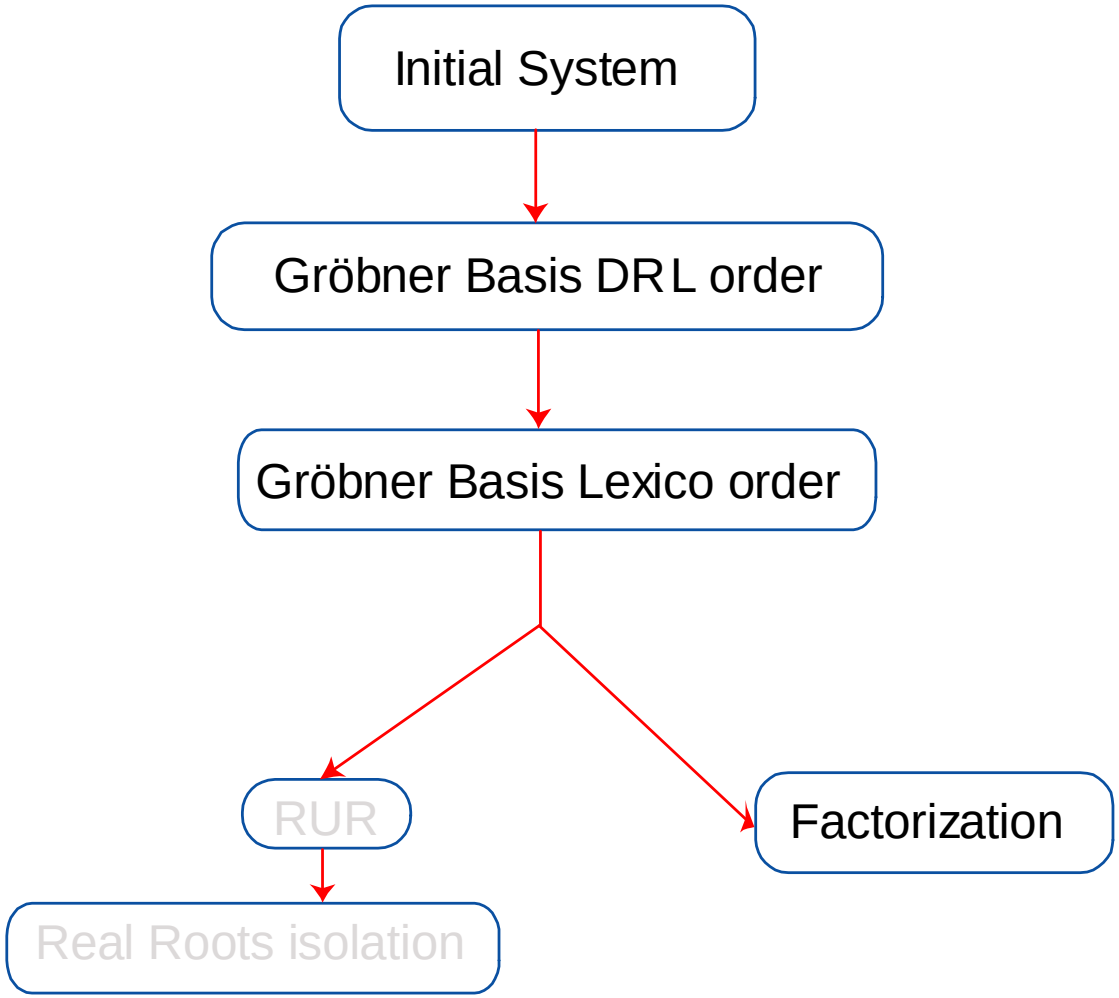
Dedicated Algorithm: efficiently change the ordering

FGLM = use only linear algebra.

Theorem (FGLM)

If $\dim(I) = 0$ *and* D=$\deg(I)$. *Assume that* G *a Gröbner basis of* I *is already computed, then* G_{new} *a Gröbner basis for the same ideal* I *and a new ordering* $<_{new}$ *can be computed in* $O(n D^3)$.

Zero dim solve



Algorithms I

Algorithms: for *computing* Gröbner bases.

- Buchberger (1965,1979,1985)
- F_4 using linear algebra (1999) (strategies)
- F_5 no reduction to zero (2002)

Linear Algebra and Matrices

Trivial link: Linear Algebra $\leftrightarrow$ Polynomials

Definition: $F = (f_1, \ldots, f_m)$, $<$ ordering. A Matrix representation M_F of F is such that

$$^TF = M_F.{}^TX$$

where X all the terms (sorted for $<$) occurring in F:

$$M_F = \begin{array}{c} \\ f_1 \\ f_2 \\ f_3 \end{array} \begin{array}{c} \begin{array}{ccc} m_1 & > m_2 & > m_3 \end{array} \\ \begin{pmatrix} & \ldots & \\ & \ldots & \\ & \ldots & \end{pmatrix} \end{array}$$

Algorithms II

Linear Algebra and Matrices

Trivial link: Linear Algebra $\leftrightarrow$ Polynomials

If Y is a vector of monomials, M a matrix then its polynomial representation is

$$^T[f_1, \ldots, f_m] = M.^T Y$$

Macaulay method

Macaulay bound (for homogeneous polynomials):

$$D = 1 + \sum_{i=1}^{m} (deg(f_i) - 1)$$

Algorithms III

We compute the matrix representation of $\{tf_i,\ deg(t) \leq D - deg(f_i),\ i = 1, \ldots, m\}$, $<_{\mathrm{DRL}}$

$$M_{\mathrm{Mac}} = \begin{array}{c} \\ t_1 f_1 \\ t_1' f_1 \\ t_2' f_2 \\ t_2 f_2 \\ t_3 f_3 \end{array} \begin{array}{c} m_1 > m_2 > m_3 > \cdots > m_r \\ \left(\begin{array}{c} \ldots \\ \ldots \\ \ldots \\ \ldots \\ \ldots \end{array} \right. \end{array}$$

Let $\tilde{M}_{\mathrm{Mac}}$ be the result of *Gaussian elimination*.

Theorem

(Lazard 83) If F is regular then the polynomial representation of $\tilde{M}_{Mac}$ is a Gröbner basis.

Efficient Algorithms

F_4 (1999) linear algebra

Efficient Algorithms

F_4 (1999) linear algebra

Small subset of rows: F_5 (2002) **full rank matrix**

Efficient Algorithms

F_4 (1999) linear algebra
Small subset of rows: F_5 (2002) **full rank matrix** $F_5/2$ (2002) **full rank matrix** GF(2) (includes Frobenius $h^2 = h$)

$$A_d = \begin{matrix} monom \times f_{i_1} \\ monom \times f_{i_2} \\ monom \times f_{i_3} \end{matrix} \begin{pmatrix} \overset{momoms\ degree\ \mathbf{d}\ in\ x_1,\ldots,x_n}{\ldots} \\ \ldots \\ \ldots \end{pmatrix}$$

F_5 the idea I

We consider the following example: (b parameter):

$$\mathcal{S}_b \begin{cases} f_3 = x^2 + 18\,xy + 19\,y^2 + 8\,xz + 5\,yz + 7\,z^2 \\ f_2 = 3\,x^2 + (7 + \ b)\,x\,y + 22\,x\,z + 11\,yz + 22\,z^2 + 8\,y^2 \\ f_1 = 6\,x^2 + 12\,xy + 4\,y^2 + 14\,xz + 9\,yz + 7\,z^2 \end{cases}$$

With Buchberger $x > y > z$:

- 5 useless reductions
- 5 useful pairs

F_5 the idea II

We proceed degree by degree.

$$A_2 = \begin{array}{c|cccccc|} & x^2 & x\,y & y^2 & x\,z & y\,z & z^2 \\ f_3 & 1 & 18 & 19 & 8 & 5 & 7 \\ f_2 & 3 & 7 & 8 & 22 & 11 & 22 \\ f_1 & 6 & 12 & 4 & 14 & 9 & 7 \end{array}$$

$$\widetilde{A_2} = \begin{array}{c|cccccc|} & x^2 & x\,y & y^2 & x\,z & y\,z & z^2 \\ f_3 & 1 & 18 & 19 & 8 & 5 & 7 \\ f_2 & & 1 & 3 & 2 & 4 & -1 \\ f_1 & & & 1 & -11 & -3 & -5 \end{array}$$

"new" polynomials $f_4 = xy + 4\,yz + 2\,xz + 3\,y^2 - z^2$ and $f_5 = y^2 - 11\,xz - 3\,yz - 5\,z^2$

F_5 the idea III

$$
\begin{aligned}
f_3 &= x^2 + 18\,xy + 19\,y^2 + 8\,xz + 5\,yz + 7\,z^2 \\
f_2 &= 3\,x^2 + 7x\,y + 22\,x\,z + 11\,yz + 22\,z^2 + 8\,y^2 \\
f_1 &= 6\,x^2 + 12\,xy + 4\,y^2 + 14\,xz + 9\,yz + 7\,z^2 \\
f_4 &= xy + 4\,yz + 2\,xz + 3\,y^2 - z^2 \\
f_5 &= y^2 - 11\,xz - 3\,yz - 5\,z^2
\end{aligned}
$$

$$
\begin{aligned}
f_2 &\longrightarrow f_4 \\
f_1 &\longrightarrow f_5
\end{aligned}
$$

Degree 3 I

$$
\begin{array}{c}
 & x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \\
zf_3 & 0 & 0 & 0 & 0 & 1 & \dots \\
yf_3 & 0 & 1 & 18 & 19 & 0 & \dots \\
xf_3 & 1 & 18 & 19 & 0 & 8 & \dots \\
zf_2 & 0 & 0 & 0 & 0 & 3 & \dots \\
yf_2 & 0 & 3 & 7 & 8 & 0 & \dots \\
xf_2 & 3 & 7 & 8 & 0 & 22 & \dots \\
zf_1 & 0 & 0 & 0 & 0 & 6 & \dots \\
yf_1 & 0 & 6 & 12 & 4 & 0 & \dots \\
xf_1 & 6 & 12 & 4 & 0 & 14 & \dots
\end{array}
$$

Degree 3 II

$$
\begin{array}{c}
 & x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \\
zf_3 & 0 & 0 & 0 & 0 & 1 & \dots \\
yf_3 & 0 & 1 & 18 & 19 & 0 & \dots \\
xf_3 & 1 & 18 & 19 & 0 & 8 & \dots \\
zf_2 & 0 & 0 & 0 & 0 & 3 & \dots \\
yf_2 & 0 & 3 & 7 & 8 & 0 & \dots \\
xf_2 & 3 & 7 & 8 & 0 & 22 & \dots \\
zf_1 & 0 & 0 & 0 & 0 & 6 & \dots \\
yf_1 & 0 & 6 & 12 & 4 & 0 & \dots \\
xf_1 & 6 & 12 & 4 & 0 & 14 & \dots
\end{array}
$$

Degree 3 III

$$A_3 = \begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_2 \\ yf_2 \\ xf_2 \\ zf_1 \\ yf_1 \\ xf_1 \end{array} \begin{array}{c} \begin{array}{cccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & \dots \\ 0 & 1 & 18 & 19 & 0 & \dots \\ 1 & 18 & 19 & 0 & 8 & \dots \\ 0 & 0 & 0 & 0 & 3 & \dots \\ 0 & 3 & 7 & 8 & 0 & \dots \\ 3 & 7 & 8 & 0 & 22 & \dots \\ 0 & 0 & 0 & 0 & 6 & \dots \\ 0 & 6 & 12 & 4 & 0 & \dots \\ 6 & 12 & 4 & 0 & 14 & \dots \end{pmatrix} \end{array}$$

Degree 3 IV

$$f_2 \longrightarrow f_4$$

$$f_1 \longrightarrow f_5$$

$$\begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_2 \\ yf_2 \\ xf_2 \\ zf_1 \\ yf_1 \\ xf_1 \end{array} \begin{array}{c} \begin{array}{ccccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & \dots \\ 0 & 1 & 18 & 19 & 0 & \dots \\ 1 & 18 & 19 & 0 & 8 & \dots \\ 0 & 0 & 0 & 0 & 3 & \dots \\ 0 & 3 & 7 & 8 & 0 & \dots \\ 3 & 7 & 8 & 0 & 22 & \dots \\ 0 & 0 & 0 & 0 & 6 & \dots \\ 0 & 6 & 12 & 4 & 0 & \dots \\ 6 & 12 & 4 & 0 & 14 & \dots \end{pmatrix} \end{array}$$

Degree 3 V

$$\widetilde{A_3} = \begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_4 \\ yf_4 \\ xf_4 \\ zf_5 \\ yf_5 \\ xf_5 \end{array} \begin{array}{c} \begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & xyz & y^2z & xz^2 & yz^2 & z^3 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 18 & 19 & 8 & 5 & 7 \\ 0 & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 \\ 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 3 & 2 & 4 & 22 \\ 0 & 0 & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 \\ 0 & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 12 & 20 & 18 \\ 0 & 0 & 0 & 1 & 0 & 12 & 20 & 0 & 18 & 0 \\ 0 & 0 & 1 & 0 & 12 & 20 & 0 & 18 & 0 & 0 \end{pmatrix} \end{array}$$

We have constructed 3 new polynomials

$$f_6 = y^3 + 8\,y^2z + xz^2 + 18\,yz^2 + 15\,z^3$$
$$f_7 = xz^2 + 11\,yz^2 + 13\,z^3$$
$$f_8 = yz^2 + 18\,z^3$$

We have the linear equivalences: $x\,f_2 \leftrightarrow x\,f_4 \leftrightarrow f_6$ and $f_4 \longrightarrow f_2$

Degree 4: reduction to 0 !

The matrix whose rows are

$$x^2 f_i, x\,y f_i, y^2 f_i, x\,z f_i, y\,z f_i, z^2 f_i, \quad i = 1, 2, 3$$

is not full rank !

Why ?

$6 \times 3 =$ 18 rows

but only $x^4, x^3\,y, \ldots, y\,z^3, z^4$ 15 columns

Simple linear algebra theorem: 3 useless row (which ones ?)

Trivial relations

$$f_2\, f_3 - f_3\, f_2 = 0$$

can be rewritten

$$\begin{aligned} &3\,x^2\, f_3 + (7 + \ b)\, xy\, f_3 + 8\, y^2\, f_3 + 22\, xz\, f_3 \\ &+11\, yz\, f_3 + 22\, z^2\, f_3 - \boxed{x^2\, f_2} - 18\, xy\, f_2 - 19\, y^2\, f_2 \\ &-8\, xz\, f_2 - 5\, yz\, f_2 - 7\, z^2\, f_2 = 0 \end{aligned}$$

We can remove the row $x^2 f_2$

same way $f_1 f_3 - f_3 f_1 = 0 \longrightarrow$ remove $x^2 f_1$

but $f_1 f_2 - f_2 f_1 = 0 \longrightarrow$ remove $x^2 f_1$! ???

Combining trivial relations

$$
\begin{aligned}
0 &= (f_2 f_1 - f_1 f_2) - 3(f_3 f_1 - f_1 f_3) \\
0 &= (f_2 - 3f_3) f_1 - f_1 f_2 + 3 f_1 f_3 \\
0 &= f_4 f_1 - f_1 f_2 + 3 f_1 f_3 \\
0 &= \left((1 - b)xy + 4\,yz + 2\,xz + 3\,y^2 - z^2\right) f_1 \\
&\quad -(6x^2 + \cdots) f_2 + 3(6x^2 + \cdots) f_3
\end{aligned}
$$

- if $b \neq 1$ remove $x\,y\ f_1$
- if $b = 1$ remove $y\,z\ f_1$

Need "some" computation

New Criterion

Any combination of the trivial relations $f_i f_j = f_j f_i$ can always be written:

$$u(f_2 f_1 - f_1 f_2) + v(f_3 f_1 - f_1 f_3) + w(f_2 f_3 - f_3 f_2)$$

where u, v, w are arbitrary polynomials.

$$(u f_2 + v f_3) f_1 - u f_1 f_2 - v f_1 f_3 + w f_2 f_3 - w f_3 f_2$$

(trivial) relation $h f_1 + \cdots = 0 \leftrightarrow \; h \in \mathrm{Id}(f_2, f_3)$

Compute a Gröbner basis of $(f_2, f_3) \longrightarrow G_{\text{prev}}$.

Remove line $h\, f_1$ iff $\mathrm{LT}(h)$ top reducible by G_{prev}

Degree 4 I

$$y^2 f_1, x\, z f_1, y\, z f_1, z^2 f_1, x\, y f_2, y^2 f_2, x\, z f_2,$$
$$y\, z f_2, z^2 f_2, x^2 f_3, x\, y f_3, y^2 f_3, x\, z f_3, y\, z f_3, z^2 f_3$$

In order to use previous computations (degree 2 and 3):

$$\begin{array}{ll} x f_2 \longrightarrow f_6 & f_2 \longrightarrow f_4 \\ x f_1 \longrightarrow f_8 & y f_1 \longrightarrow f_7 \\ f_1 \longrightarrow f_5 & \end{array}$$

$$y f_7, z f_8, z f_7, z^2 f_5, y f_6, y^2 f_4, z f_6, y\, z f_4,$$
$$z^2 f_4, x^2 f_3, x\, y f_3, y^2 f_3, x\, z f_3, y\, z f_3, z^2 f_3,$$

Degree 4 II

$$\left[\begin{array}{cccccccccccccc}
1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 \\
 & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 & & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 \\
 & & & 1 & 3 & 0 & 0 & 2 & 4 & 0 & 0 & 22 & 0 & 0 & 0 \\
 & & & & 1 & 0 & 0 & 0 & 8 & 0 & 1 & 18 & 0 & 15 & 0 \\
 & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 & 0 \\
 & & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 \\
 & & & & & & & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 \\
 & & & & & & & & 1 & 0 & 0 & 8 & 1 & 18 & 15 \\
 & & & & & & & & & 1 & 18 & 19 & 8 & 5 & 7 \\
 & & & & & & & & & & 1 & 11 & 0 & 13 & 0 \\
 & & & & & & & & & & & 1 & 12 & 20 & 18 \\
 & & & & & & & & & & & & 1 & 11 & 13 \\
 & & & & & & & & & & & & & 1 & 18 \\
 & & & & & & & & & & 1 & 3 & 2 & 4 & 22
\end{array}\right]$$

Degree 4 III

Sub matrix:

$$\begin{array}{c} \\ z^2 f_4 \\ z^2 f_5 \\ z f_7 \\ z f_8 \\ y f_7 \end{array} \begin{array}{c} \begin{array}{ccccc} xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \end{array} \\ \begin{pmatrix} 1 & 3 & 2 & 4 & 22 \\ & 1 & 12 & 20 & 18 \\ & & 1 & 11 & 13 \\ & & & 1 & 18 \\ 1 & 11 & 0 & 13 & 0 \end{pmatrix} \end{array}$$

New algorithm

- Incremental algorithm

$$(f) + G_{\text{old}}$$

- Incremental degree by degree
- Give a "unique name" to each row

Remove $h f_1 + \cdots$ if $\mathrm{LT}(h) \in \mathrm{LT}(G_{\text{old}})$

$\mathrm{LT}(h)$ signature/index of the row

F_5 matrix

Special/Simpler version of F_5 for dense/generic polynomials.
the maximal degree D is a *parameter* of the algorithm.
degree d $m = 2$, $\deg(f_i) = 2$ homogeneous quadratic polynomials, degree d:

We may assume that we have already computed:

$G_{i,d}$ Gröbner basis $[f_1, \ldots, f_i]$ up do degree d

In degree d

$$
\begin{array}{c}
 & \begin{array}{ccccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \dots \end{array} \\
\begin{array}{c} u_1 f_1 \\ u_2 f_1 \\ u_3 f_1 \\ v_1 f_2 \\ v_2 f_2 \\ w_1 f_3 \\ w_2 f_3 \\ \vdots \end{array} &
\begin{pmatrix}
1 & x & x & x & x & \dots \\
0 & 1 & x & x & x & \dots \\
0 & 0 & 1 & x & x & \dots \\
0 & 0 & 0 & 1 & x & \dots \\
0 & 0 & 0 & 0 & 1 & \dots \\
0 & 0 & 0 & 0 & 0 & \dots \\
0 & 0 & 0 & 0 & 0 & \dots \\
0 & 0 & 0 & 0 & 0 & \vdots
\end{pmatrix}
\end{array}
$$

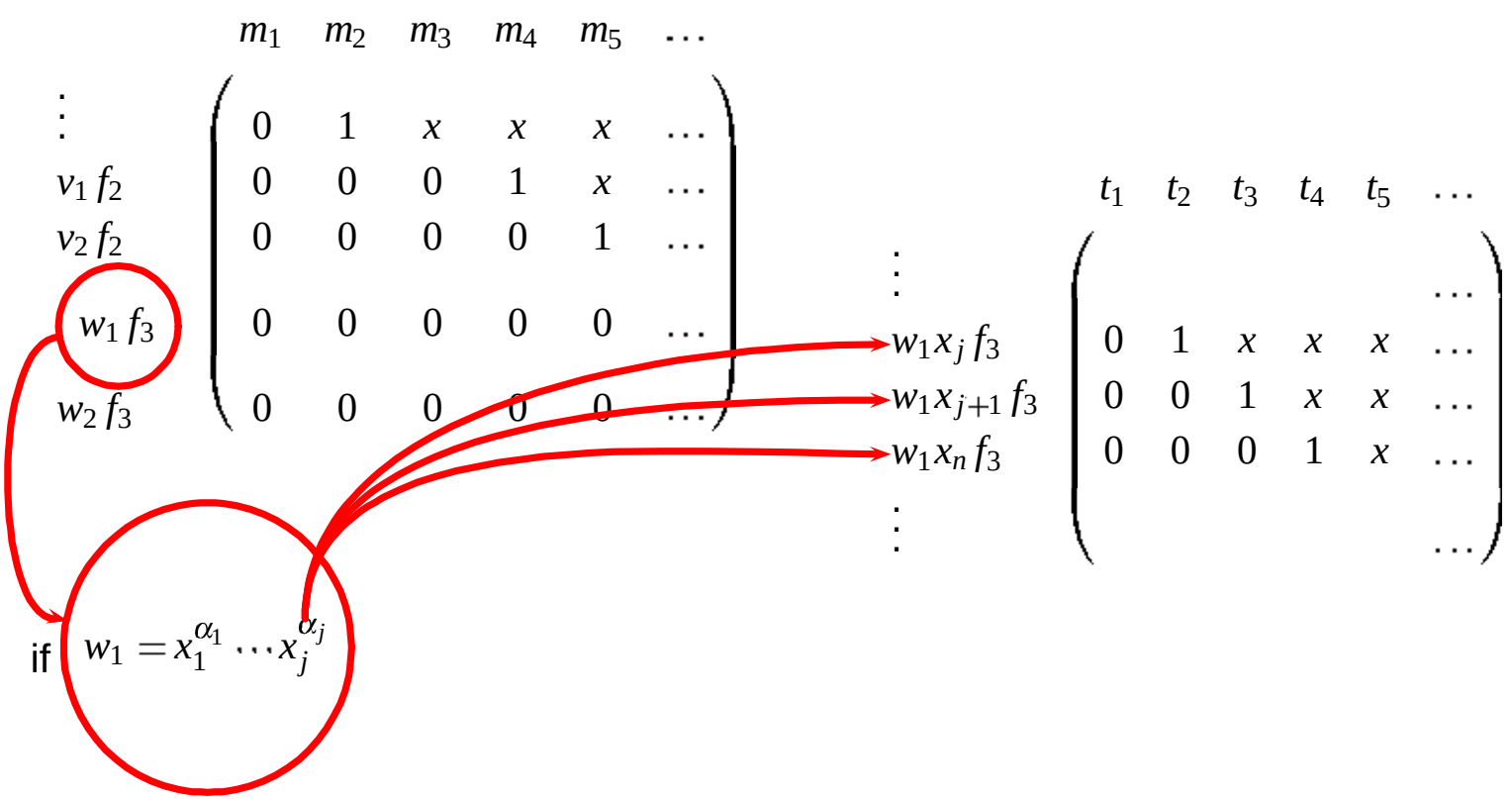
with $\deg(u_i) = \deg(v_i) = \deg(w_i) = d - 2$

From degree d to $d+1$ I

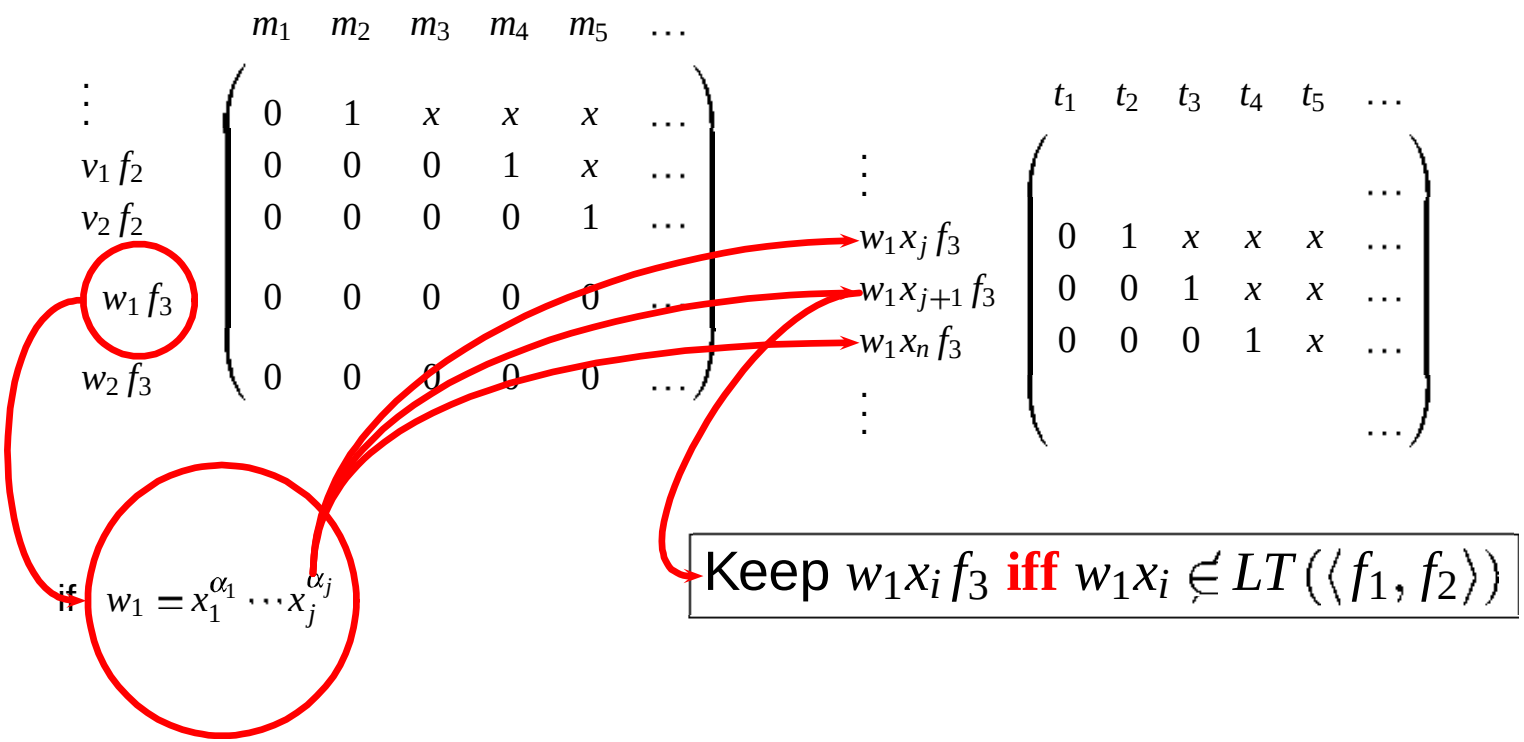
Select a row in degree d:

$$\begin{array}{c} \\ \vdots \\ v_1 f_2 \\ v_2 f_2 \\ w_1 f_3 \\ w_2 f_3 \end{array} \begin{array}{c} \begin{array}{ccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \dots \end{array} \\ \begin{pmatrix} 0 & 1 & x & x & x & \dots \\ 0 & 0 & 0 & 1 & x & \dots \\ 0 & 0 & 0 & 0 & 1 & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots \end{pmatrix} \end{array}$$

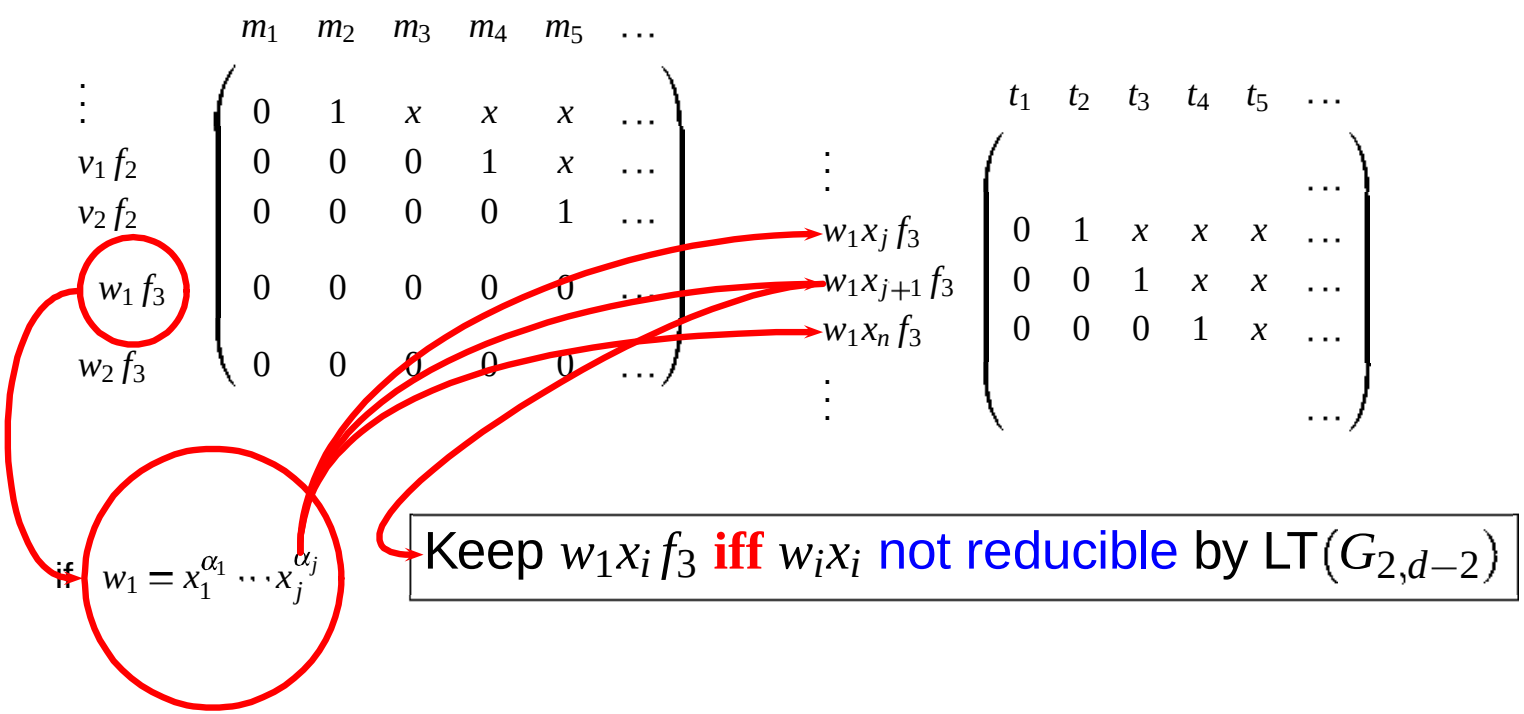
From degree d to $d+1$ II



From degree d to $d+1$ III



From degree d to $d+1$ IV



F_5 properties

Full version of F_5 : D the maximal degree is *not given*.

Theorem If $F = [f_1, \ldots, f_m]$ is a (semi) regular sequence then all the matrices are full rank.

- Easy to adapt for the special case of $\mathbb{F}_2$ (*new trivial syzygy:* $f_i^2 = f_i$).
- Incremental in degree/equations (swap 2 loops)
- Fast in general (but not always)
- F_5 matrix: easy to implement, used in applications (HFE).

Classification I

(with M. Bardet, B. Salvy)

Theorem

Classification II

Pour une suite semi-régulière $(f_1, \ldots, f_m)$*, il n'y a pas de réduction à* 0 *dans l'algorithme* F_5 *en degré inférieur à son degré de régularité* d_{reg}*; de plus* d_{reg} *est le degré en* z *du premier coefficient négatif de la série:*

$$\prod_{i=1}^{m} \left(\frac{1 - (1 - \delta_{\mathbb{K},\mathbb{F}_2})\, z^{d_i}}{1 + \delta_{\mathbb{K},\mathbb{F}_2} z^{d_i}} \right) \left(\frac{1 - \delta_{\mathbb{K},\mathbb{F}_2}\, z^2}{1 - z} \right)^n$$

où d_i *est le degré total de* f_i*. Par conséquent, le nombre total d'opérations arithmétiques dans* $\mathbb{K}$ *nécessaire à* F_5 *(voir algorithme* **??***) est borné par*

$$Cste \cdot M_{d_{reg}}(n)^{\omega} \text{ with } \omega \leq 3$$

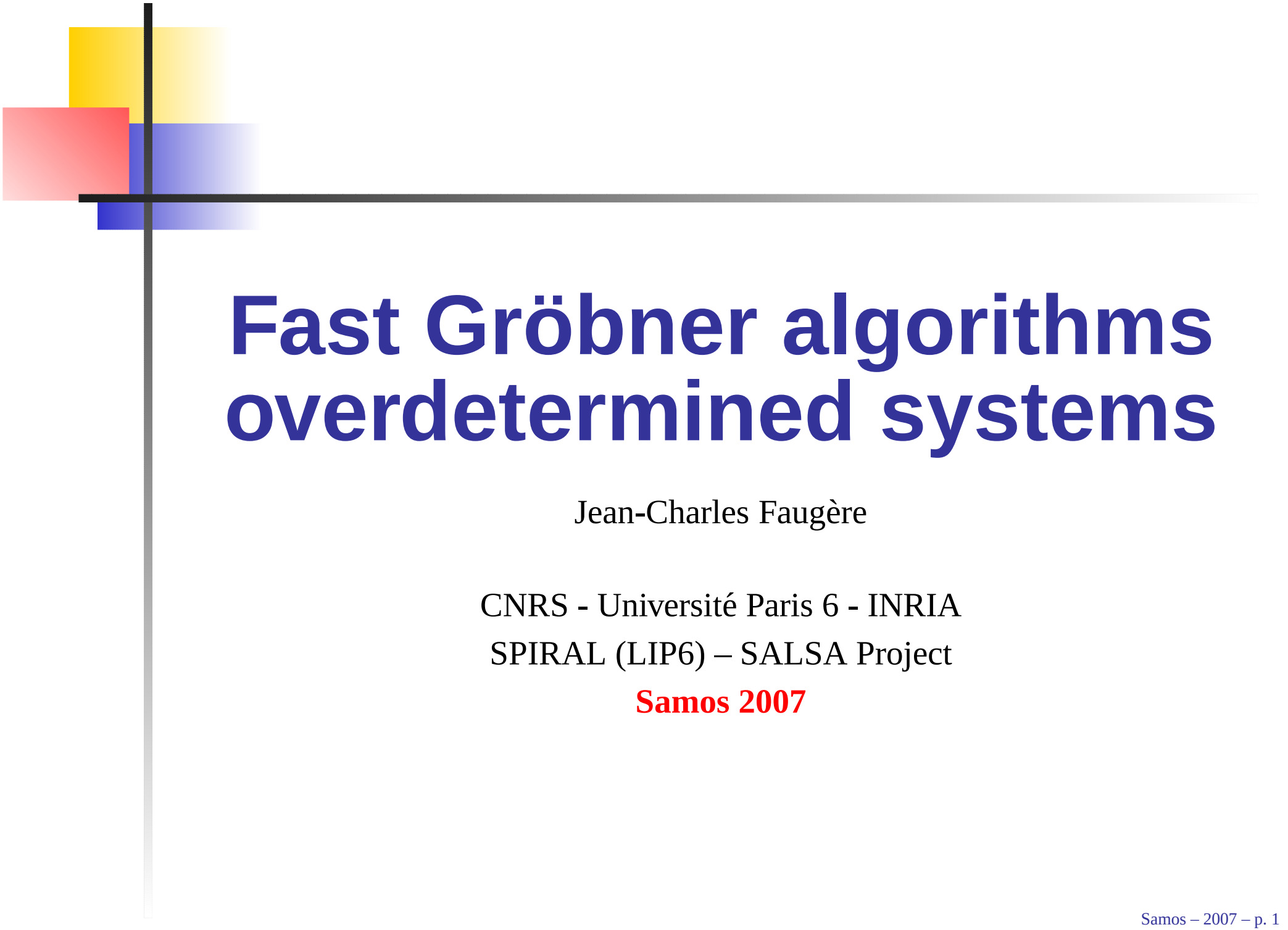
On considère une suite semi-régulière constituée d'équations $(f_1, \ldots, f_m)$. Le tableau suivant résume le résultat de

Classification III

plusieurs théorèmes donne le développement asymptotique de d_{reg} lorsque $n \longrightarrow \infty$ en fonction de la valeur du rapport entre le nombre d'équations et le nombre de variables $\frac{m}{n}$.
Légende des symboles utilisés dans le tableau:
k est une constante (qui ne dépend pas de n).
d_i est le degré total de f_i.
$H_k(X)$ est le k ème polynôme d'Hermite; $h_{k,1}$ est le plus grand zéro de H_k (tous les zéros de $H_k(X)$ sont réels).
$a_1 \approx -2.3381$ est le plus grand zéro de la fonction d'Airy (solution de $\frac{\partial^2 y}{\partial z^2} - z\,y = 0$).
$\Phi(z) = \frac{z}{n}\frac{\partial}{\partial z} \log\left((1-z)^n \prod_{i=1}^{m}(1-z^{d_i})^{-1}\right) =$
$\frac{z}{1-z} - \frac{1}{n}\sum_{i=1}^{m}\frac{d_i z^{d_i}}{1-z^{d_i}}$ et z_0 est la racine de $\Phi'(z)$ qui minimise $\Phi(z_0) > 0$.

Classification IV

m	Degré	d_{reg}
$m < n$	$\mathbb{K}, d_i = 2$	$m+1$ (Macaulay bound)
$n+1$	$\mathbb{K}$	$\sum_{i=1}^{n+1} \frac{d_i-1}{2}$ (A. Szanto)
$n+k$	$\mathbb{K}, d_i = 2$	$\frac{m}{2} - h_{k,1}\sqrt{\frac{m}{2}} + o(1)$
$n+k$	$\mathbb{K}$	$\sum_{i=1}^{n+k} \frac{d_i-1}{2} - h_{k,1}\sqrt{\sum_{i=1}^{n+k} \frac{d_i^2-1}{6}} + o(1)$
$2\,n$	$\mathbb{K}, d_i = 2$	$\frac{n}{11.6569} + 1.04\,n^{\frac{1}{3}} - 1.47 + 1.71\,n^{-\frac{1}{3}} + O\left(n^{-\frac{2}{3}}\right)$
$k\ n$	$\mathbb{K}, d_i = 2$	$(k - \frac{1}{2} - \sqrt{k(k-1)})n + \frac{-a_1}{2(k(k-1))^{\frac{1}{6}}} n^{\frac{1}{3}} + O(1)$
$k\ n$	$\mathbb{K}$	$\Phi(z_0)\,n - a_1\left(-\frac{1}{2}\Phi''(z_0)z_0^2\right)^{\frac{1}{3}} + O\left(n^{\frac{1}{3}}\right)$
n	$\mathbb{F}_2, d_i = 2$	$\frac{n}{11.1360} + 1.0034\,n^{\frac{1}{3}} - 1.58 + O(n^{-\frac{1}{3}})$
$k\ n$	$\mathbb{F}_2, d_i = 2$	$\left(-k + \frac{1}{2} + \frac{1}{2}\sqrt{2k(k-5) - 1 + 2(k+2)\sqrt{k(k+2)}\right.$



Fast Gröbner algorithms overdetermined systems

Jean-Charles Faugère

CNRS - Université Paris 6 - INRIA

SPIRAL (LIP6) – SALSA Project

Samos 2007

Why do we need efficiency ?

Users have problems that they want to solve.
Hot topic in Cryptography (L. Perret).
The goal is to evaluate the security of a cryptosystem.
Should be resistant to:

- differential cryptanalysts
- linear cryptanalysis
- Algebraic Cryptanalysis

Algebraic cryptanalysis

Convert the crypto-system $\longrightarrow$ algebraic problem.
Evaluate the difficulty of the corresponding algebraic system S.

$$V = \{z \in \mathbb{F}_2^n \ , \ f(z) = 0 \ f \in \mathscr{S}\}$$

To **solve** S:

- compute Gröbner bases.

Algebraic cryptanalysis

Convert the crypto-system $\longrightarrow$ algebraic problem.
Evaluate the difficulty of the corresponding algebraic system S.

$$V = \{z \in \mathbb{F}_2^n \ , \ f(z) = 0 \ f \in \mathscr{S}\}$$

To **solve** S:

- compute Gröbner bases.
- exaustive search !!

Complexity of exaustive $O(n2^n)$ $n > 80$

Specific problems

$$V_{\mathbb{F}_2} = \{z \in F_2^n \ , \ f_i(z) = 0, i = 1, \ldots, m\}$$

In fact we have to add the "field equations":
$x_i^2 - x_i$.

$$\text{Ideal}(\, f_i(z) = 0, i = 1, \ldots, m) + (x_i^2 - x_i, i = 1, \ldots, n)$$

Hence we have $M = m + n$ equations in n variables.
Sometimes $m >> n$.

Specific solutions

For several applications (Signal Theory, Crypto, . . .) we have to solve an overdertimed system of equations.

- Improve algorithms for overdertimed systems.
- Improve complexity bound (Macaulay bound).

Specific algorithm in Crypto

From “outside” the perception of Gröbner bases is (often) bad:

- $d^{2^{\frac{n}{10}}}$ complexity.
- Very inefficient implementation of Gröbner bases in general CAS.
- Results on Complexity are not well known.

$\longrightarrow$ develop new algorithms for solving algebraic equations.

Other algorithms: XL

In crypto: develop their own algorithms !

f_i initial equations (of degree 2) D a parameter

1. **Multiply:** Generate all the $(\prod_{j=1}^{d} x_{i_j}) f_i$ with $d \leq D-2$
2. **Linearize:** Consider each monomial in the x_{i_j} as a new variable and perform Gaussian elimination on the equations obtained in **1**.
   Ordering monomials such that all the terms containing one1 variable (say x_1) are eliminated last.
3. **Solve:** Assume that step **2**. yields at least one univariate equation in the powers of x_1. Solve this equation over the finite field.

Other algorithms: XL

Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations

N Courtois, A Klimov, J Patarin and A Shamir

Abstract. [...] Gröbner base algorithms have large exponential complexity and cannot solve in practice systems with $n >= 15$*. Kipnis and Shamir [9] have recently introduced a new algorithm called "relinearization". [...]*

This is a challenge for Computer Algebra !

Complexity

$$I = (f_1(x_1, \ldots, x_n), \cdots, f_m(x_1, \ldots, x_n))$$

$$f(x_1, \ldots, x_n) \longrightarrow f^*(x_1, \ldots, x_n, h) = h^{\deg(f)}(\frac{x_1}{h}, \ldots, \frac{x_n}{h})$$

$$I^* = (f^*{}_1(x_1, \ldots, x_n, h), \cdots, f^*{}_m(x_1, \ldots, x_n, h))$$

- n nb of variables, m nb of equations
- D maximal degree occurring
- dimension/degree
- Hilbert function/Regularity

Complexity (well known results)

$I = (f_1(x_1, \ldots), \ldots, f_m(x_1, \ldots, x_n))$ and $deg(f_i) = d$

Hypotheses none

ONE Explicit example: Mayr and Meyer

$$\text{Complexity } d^{2^n}$$

Complexity (well known results)

$I = (f_1(x_1, \ldots), \ldots, f_m(x_1, \ldots, x_n))$ and $deg(f_i) = 2$

Hypotheses "set of zeros at infinity is finite"
$dim(I^*) = 0$
Gröbner basis (DRL ordering) [La83, Giu84]

- computed in time polynomial in 2^n
- maximal degree $= n + 1$ when $m = n$ (**Macaulay**)

Lemma 1: For almost all systems: polynomial in 2^n

Complexity (well known results)

$I = (f_1(x_1, \ldots), \ldots, f_m(x_1, \ldots, x_n))$ and $deg(f_i) = 2$

Hypotheses $x_i \in GF(2)$

Lemma 2 Gröbner bases: complexity is always polynomial in 2^n.

Efficient Algorithms

Buchberger (1965)
Involutive bases (Gerdt)
F_4 (1999) linear algebra
slim Gb (2005)

$$
\begin{array}{rl}
 & \qquad\qquad\qquad \textit{momoms degree } \mathbf{d} \textit{ in } x_1,\ldots,x_n \\
A_d = \begin{array}{c} monom \times f_{i_1} \\ monom \times f_{i_2} \\ monom \times f_{i_3} \end{array} & \begin{pmatrix} \qquad\qquad \ldots \qquad\qquad \\ \ldots \\ \ldots \end{pmatrix}
\end{array}
$$

Efficient Algorithms

F_5 (2002)**full rank matrix**

$$
\begin{array}{rl}
 & \begin{array}{c} momoms\ degree\ \mathbf{d}\ in\ x_1,\ldots,x_n \end{array} \\
\begin{array}{r} \\ A_d = \\ \\ \end{array} & \begin{array}{l} monom \times f_{i_1} \\ monom \times f_{i_2} \\ monom \times f_{i_3} \end{array}
\begin{pmatrix} \ldots \\ \ldots \\ \ldots \end{pmatrix}
\end{array}
$$

F_5 matrix

Special/Simpler version of F_5 for dense/generic polynomials.
the maximal degree D is a *parameter* of the algorithm. degree d $m = 2$, $\deg(f_i) = 2$ homogeneous quadratic polynomials, degree d:

F_5 matrix

$m = 2$, $\deg(f_i) = 2$ homogeneous quadratic polynomials, degree d:

$$\begin{array}{c} \\ u_1 f_1 \\ u_2 f_1 \\ u_3 f_1 \\ v_1 f_2 \\ v_2 f_2 \end{array} \begin{array}{c} \begin{array}{ccccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \dots \end{array} \\ \begin{pmatrix} x & x & x & x & x & \dots \\ x & x & x & x & x & \dots \\ x & x & x & x & x & \dots \\ x & x & x & x & x & \dots \\ x & x & x & x & x & \dots \end{pmatrix} \end{array}$$

$$\deg(u_i) = \deg(v_i) = d - 2$$

Gauss

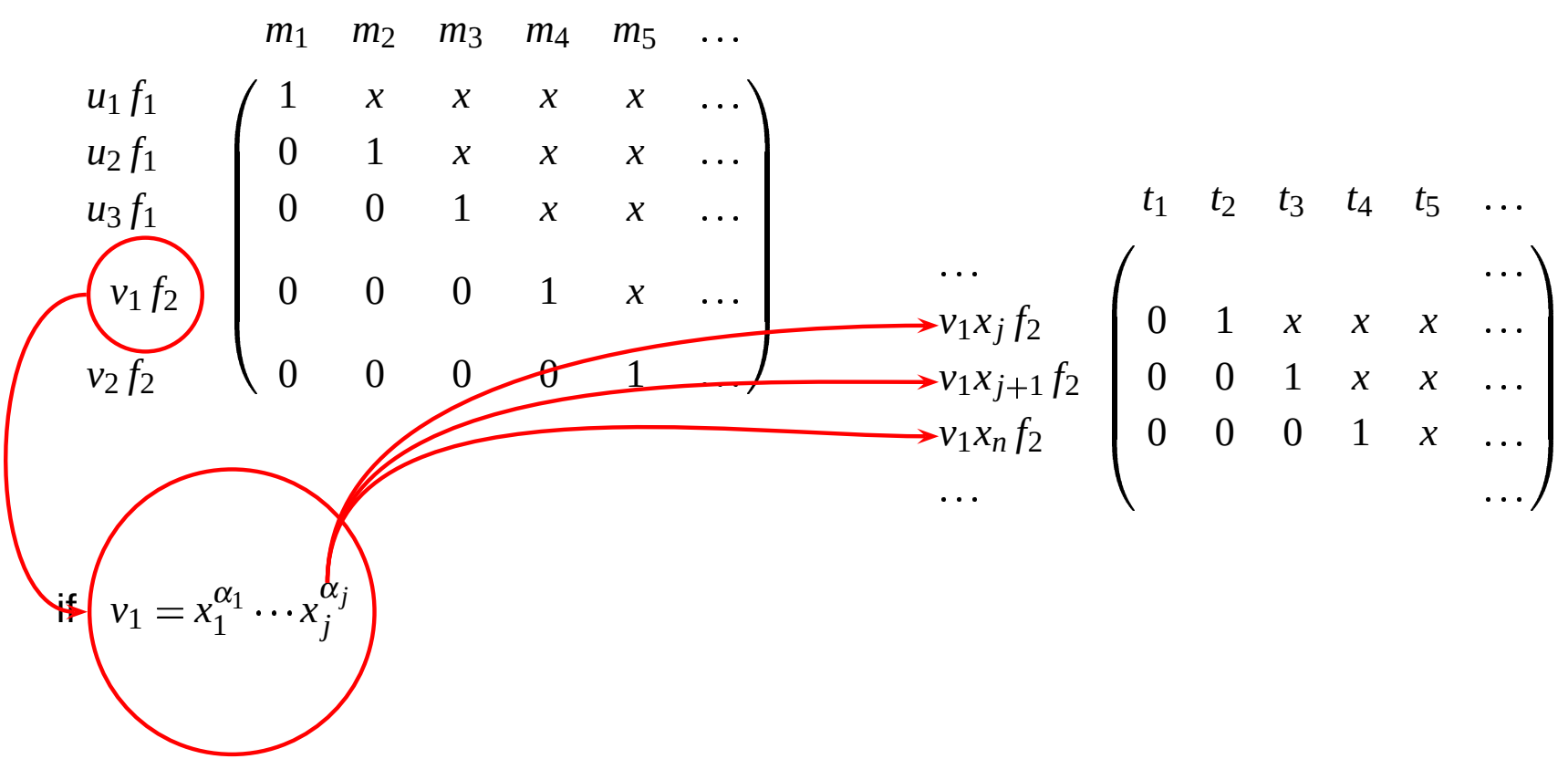
Gauss reduction:

$$
\begin{array}{c} \\ u_1 f_1 \\ u_2 f_1 \\ u_3 f_1 \\ v_1 f_2 \\ v_2 f_2 \end{array}
\begin{array}{c}
\begin{array}{ccccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \dots \end{array} \\
\left(\begin{array}{ccccccc}
1 & x & x & x & x & \dots \\
0 & 1 & x & x & x & \dots \\
0 & 0 & 1 & x & x & \dots \\
0 & 0 & 0 & 1 & x & \dots \\
0 & 0 & 0 & 0 & 1 & \dots
\end{array} \right)
\end{array}
$$

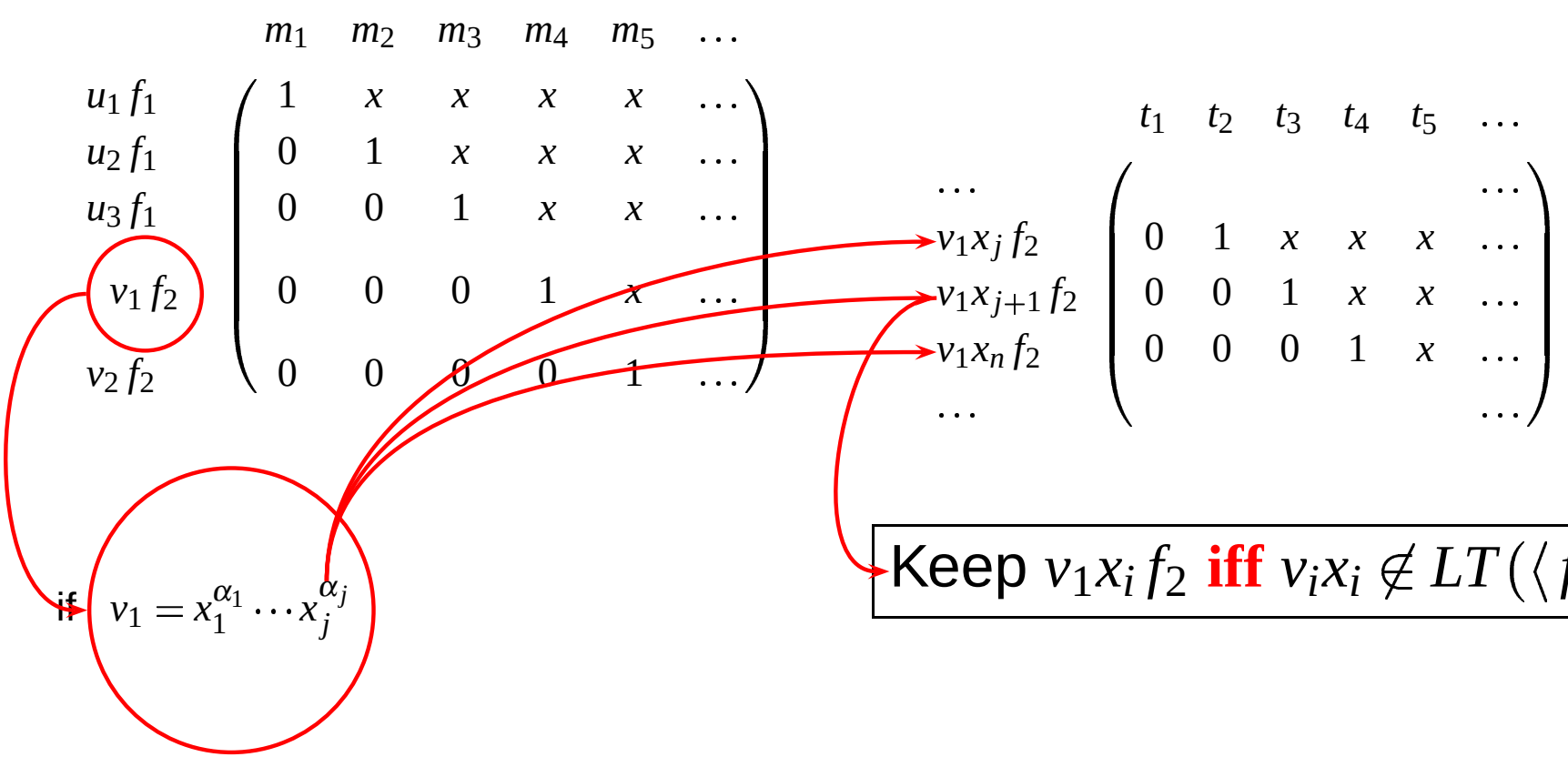
$d \longrightarrow d+1$

$$
\begin{array}{c}
 \\
u_1 f_1 \\
u_2 f_1 \\
u_3 f_1 \\
v_1 f_2 \\
v_2 f_2
\end{array}
\begin{array}{c}
\begin{array}{cccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \dots \end{array} \\
\left(\begin{array}{cccccc}
1 & x & x & x & x & \dots \\
0 & 1 & x & x & x & \dots \\
0 & 0 & 1 & x & x & \dots \\
0 & 0 & 0 & 1 & x & \dots \\
0 & 0 & 0 & 0 & 1 & \dots
\end{array} \right)
\end{array}
$$

$d \longrightarrow d+1$



$d \longrightarrow d+1$



Specific algorithms

Nothing to do !

more equations $\longrightarrow$ more efficient Gb computation

Specific algorithms

$$x_i^2 = x_i$$

"Easy" part: we can handle efficiently that all the monomials are squarefree (Boolean Gröbner bases) and to develop specific linear algebra packages (over $\mathbb{F}_2$).
Moreover, we have new trivial syzygies:

$$f_i f_j = f_j f_i \quad f^2 = f$$

$F_5/2$ (2003/2005) specific version for $\mathbb{F}_2$.

Specific Complexity

(with B. Salvy, M. Bardet, 2005)

Goal: estimate d_n maximal degree occurring Gröbner comput.

Idea: we construct A_d *following step by step* F_5 $\longrightarrow$ A_d full rank $\longrightarrow$ number of rows.

$$A_d = \begin{array}{l} \\ monom\ (\mathbf{d}-\mathbf{2}) \times f_{i_1} \\ monom\ (\mathbf{d}-\mathbf{2}) \times f_{i_2} \\ monom\ (\mathbf{d}-\mathbf{2}) \times f_{i_3} \end{array} \begin{array}{c} momoms\ degree\ \ \mathbf{d}\ in\ x_1,\ldots,x_n \\ \left(\begin{array}{c} \ldots \\ \ldots \\ \ldots \end{array} \right. \end{array}$$

F_5 criterion

Criterion: $t\,f_j$ is in the matrix if $t \notin \mathrm{Id}(LT(G_{j-1}))$, where G_{j-1} is the Gröbner basis of $\{f_1, \ldots, f_{j-1}\}$.

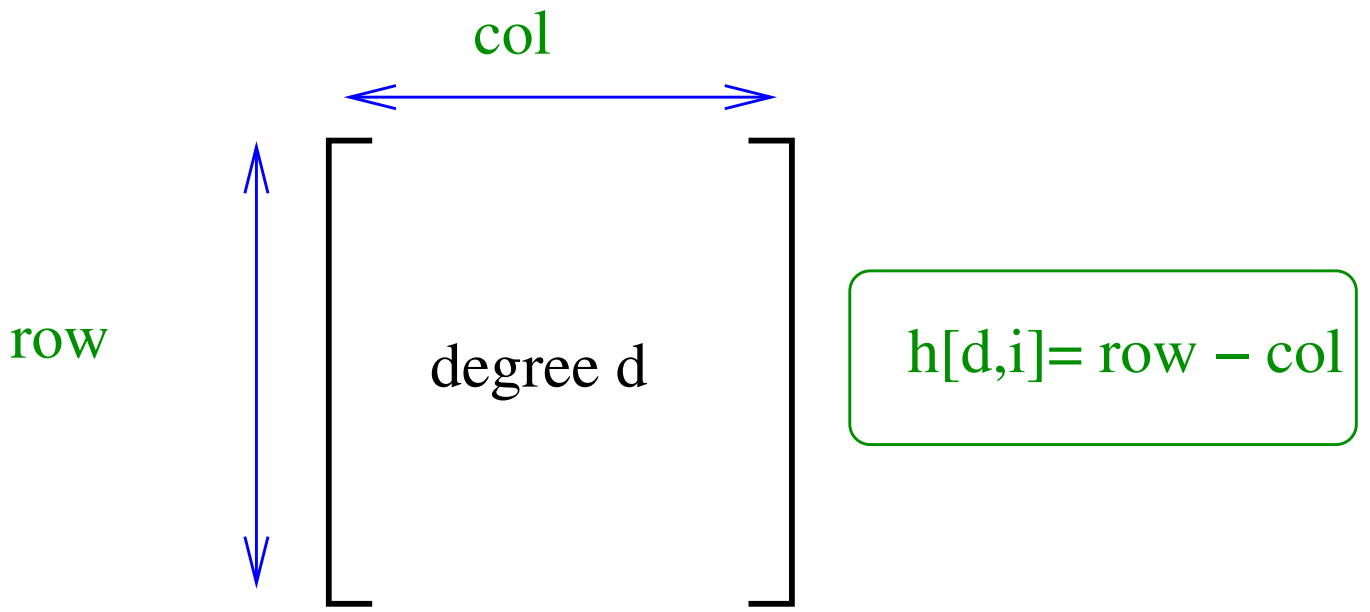
$U_{d,i}(n)$ nb of rows when computing $\{f_1, \ldots, f_i\}$ in degree d.

Recurrence relation

For $d \geq 2$:

$$U_{d,i}(n) = i \cdot \underbrace{\binom{n+d-2}{d-2}}_{\text{number of monomials of degree} \leq d-2} - \underbrace{\sum_{j=1}^{i-1} U_{d-2,j}(n)}_{\text{criterion}}$$

End of the computation



$h_{d,m}(n) < 0$ end of the Gröbner computation

Compute biggest real root N_d of $h_{d,m}(n)$.

Generating series

Theorem 1.1 *f_i degree d_i, $i = 1, \ldots, m$ finite field $\mathbb{F}_q$:*

$$H_m = \sum_{d=0}^{\infty} h_{d,m} y^d = \left(\frac{1-y^q}{1-y}\right)^n \prod_{i=1}^{m} \frac{1 - y^{d_i} + y^{d_i q - 1}}{1 + y^{d_i q - 1}}$$

particular case: $d_i = 2$, GF(2) $n = m$ eqs

$$\sum_{d=0}^{\infty} h_{d,n} y^d = \left(\frac{1+y}{1+y^2}\right)^n$$

Asymptotic expansion

biggest real root of

$$h_{d,n} = \frac{1}{2i\pi} \int_C \left(\frac{1+y}{1+y^2} \right)^n \frac{dy}{y^{d+1}}$$

Asymptotic expansion

$$d_n = \frac{1}{\lambda_0} n - \frac{\lambda_1}{\lambda_0^{\frac{4}{3}}} n^{\frac{1}{3}} + O\left(\frac{1}{n^{\frac{1}{3}}}\right)$$

$$d_n \approx \frac{\mathbf{n}}{\mathbf{11.11360}} + \mathbf{1.0034 n^{\frac{1}{3}}} + \mathbf{O}\left(\frac{\mathbf{1}}{\mathbf{n^{\frac{1}{3}}}}\right)$$

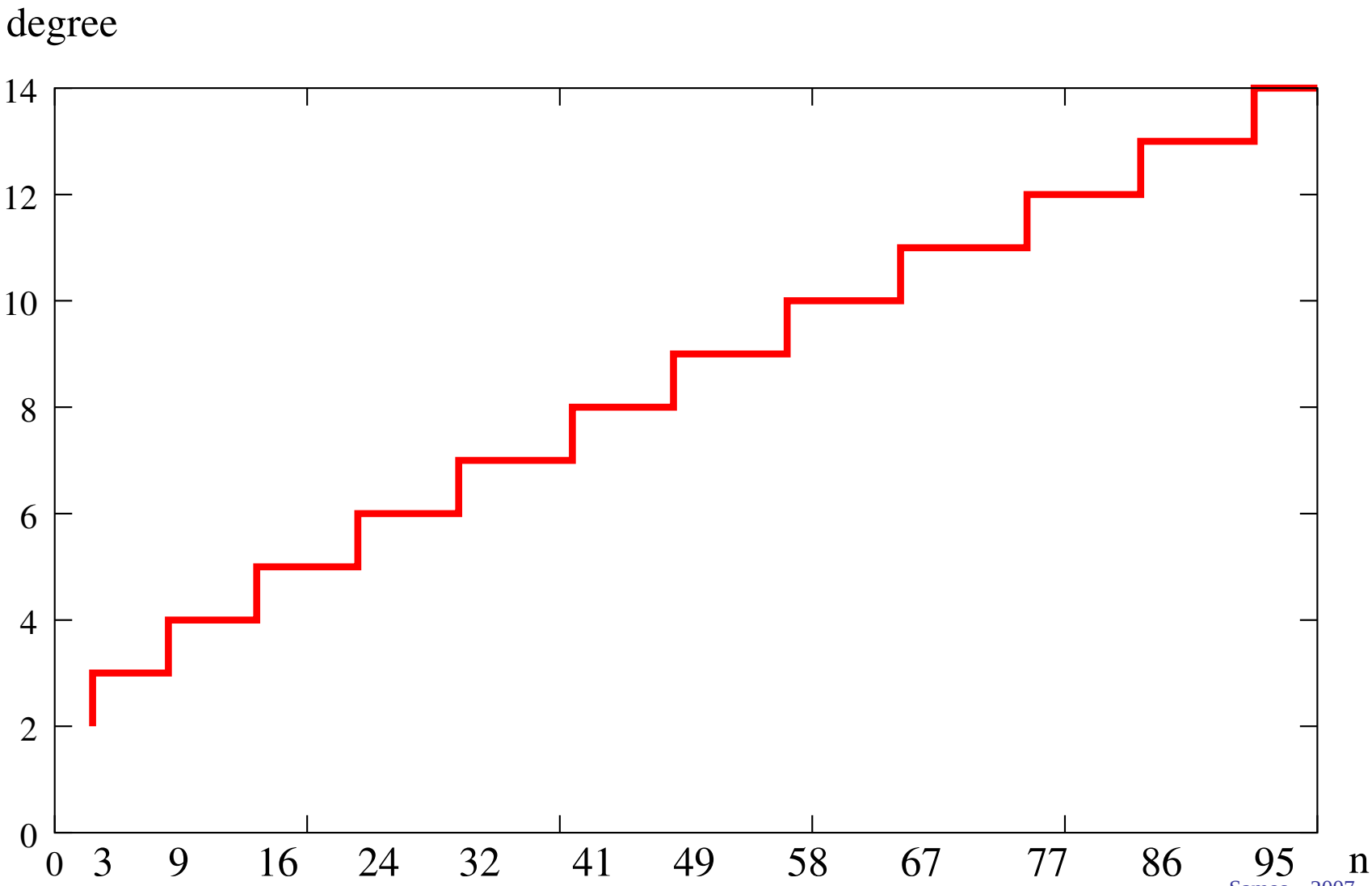
where

$\lambda_0 = 3/2\sqrt{3} + 5/2 + 1/2\sqrt{72 + 42\sqrt{3}} \approx 11.13$

and λ_1 is expressed in term of the biggest zero of the Airy function (solution $\frac{\partial^2 y}{\partial z^2} - zy = 0$)

Almost exact formula when $n \geq 3$!

Maximal Degree (F_2)



Conclusion

Classification: m number of polynomials, n variables

$m = \text{cste}\, n$	exponential complexity
$m = \text{cste}\, n\, log(n)$	sub exponential complexity
$m = \text{cste}\, n^2$	polynomial complexity

HFE

HFE = Hidden Fields Equations

- public key cryptosystem using *polynomial operations* over finite fields
- proposed by Jacques Patarin (96)
- very promising cryptosystem: signatures as short as **128, 100** and even **80 bits**.

HFE

$$\text{secret key } P(x) = \cdots x^{2^i+2^j} + \cdots + c_{17}x^{17} + c_{16}x^{16} + \cdots$$

$$\ldots, c_{16}, c_{17} \in GF(2^n), \ldots$$

univariate polynomial structure is hidden

HFE

secret key $P(x) = \cdots x^{2^i+2^j} + \cdots + c_{17}x^{17} + c_{16}x^{16} + \cdots$

$x = \sum_{i=0}^{n-1} x_i w^i \in \mathrm{GF}(2^n)$, $x_i \in GF(2)$, $w \in GF(2^n)$

$$\begin{cases} g_1(x_0, \ldots, x_{n-1}) = 0 \\ \cdots \\ g_n(x_0, \ldots, x_{n-1}) = 0 \end{cases}$$

where g_i coeff of w^i in $P(\sum_{i=0}^{n-1} x_i w^i)$ (degree 2)

HFE

secret key $P(x) = \cdots x^{2^i+2^j} + \cdots + c_{17}x^{17} + c_{16}x^{16} + \cdots$

$x = \sum_{i=0}^{n-1} x_i w^i \in \mathrm{GF}(2^n)$, $x_i \in GF(2)$, $w \in GF(2^n)$

(Random) Change of coordinates

$$x_i = \sum_{j=0}^{n-1} a_{i,j} y_j$$

(Random) Mix of equations

$$f_i = \sum_{j=1}^{n} b_{i,j} g_j$$

HFE

secret key $P(x) = \cdots x^{2^i+2^j} + \cdots + c_{17}x^{17} + c_{16}x^{16} + \cdots$

$x = \sum_{i=0}^{n-1} x_i w^i \in \mathrm{GF}(2^n)$, $x_i \in GF(2)$, $w \in GF(2^n)$

Public key:

$$\begin{cases} f_1(y_0, \ldots, y_{n-1}) \\ \ldots \\ f_n(y_0, \ldots, y_{n-1}) \end{cases}$$

HFE encryption

Initial	$(x_1, \ldots, x_n)$

HFE encryption

Initial	$(x_1, \ldots, x_n)$
Encryption	$z_i = f_i(x_1, \ldots, x_n)$

HFE encryption

Initial	$(x_1, \ldots, x_n)$
Encryption	$z_i = f_i(x_1, \ldots, x_n)$
Send	$(z_1, \ldots, z_n)$

HFE decryption

Initial	$(x_1, \ldots, x_n)$
Decryption	$z_i = f_i(x_1, \ldots, x_n)$
Send	$(z_1, \ldots, z_n)$

secret	
Initial	$(z_1, \ldots, z_n)$
Decryption	Solve $P(x) = z$

HFE decryption

Initial	$(x_1, \ldots, x_n)$
Decryption	$z_i = f_i(x_1, \ldots, x_n)$
Send	$(z_1, \ldots, z_n)$

secret	
Initial	$(z_1, \ldots, z_n)$
Decryption	Solve $P(x) = z$

Enemy	
Initial	$(z_1, \ldots, z_n)$
Decryption	$f_1 = z_1$ $f_m = z_m$

HFE decryption

Initial	$(x_1, \ldots, x_n)$
Decryption	$z_i = f_i(x_1, \ldots, x_n)$
Send	$(z_1, \ldots, z_n)$

secret	
Initial	$(z_1, \ldots, z_n)$
Decryption	Solve $P(x) = z$

Enemy	
Initial	$(z_1, \ldots, z_n)$
Decryption	$f_1 = z_1$ $f_m = z_m$

Hence, solving **algebraic system.**

Degree of univariate polynomial

Time to solve the univariate polynomial of degree d: $\mathscr{O}(\mathbf{M}(d)\log(d))$ operations in $\mathbb{F}_{2^n}$ (MCA Gathen/Gerhard)

(n,d)	(80,129)	(80,257)	(80,513)
NTL (CPU time)	0.6 sec	2.5 sec	6.4 sec
(n,d)	(128,129)	(128,257)	(128,513)
NTL (CPU time)	1.25 sec	3.1 sec	9.05 sec

(NTL/Shoup PC Pentium III 1000 Mhz)

d cannot be too big !

Experiments

	Buchberger					
	Maple	slimGb	Macaulay 2	Singular	F_4	F_5
after 10m	12	17	19	19	22	35

Experiments

	Buchberger					
	Maple	slimGb	Macaulay 2	Singular	F_4	F_5
after 10m	12	17	19	19	22	35
after 2h	14	19	23	21	28	45

Experiments

- **Challenge 1 broken**
- Recover Experimentally the complexity of HFE wrt degree of hidden polynomial

Let $D(d,n)$ be the maximum degree occuring in the Gröbner computation of HFE polynomial degree d, $\mathbb{F}_{2^n}$.

Challenge 1

Proposed by J. Patarin

- 80 equations in degree 2
- Random ? Average nb of terms: 1623.9

$$\frac{\frac{n(n-1)}{2}+n+1}{2} = 1620.5$$

Challenge 1

But after $F_5/2$: **6.4 H** can be detected that it is not random !

After 187892 sec ($\approx$ 2 days) find 4 solutions (one proc Alpha 1000 Mhz + 4 Go RAM)

Challenge 1 (solutions)

$$X = \sum_{i=1}^{80} x_i 2^{i-1}$$

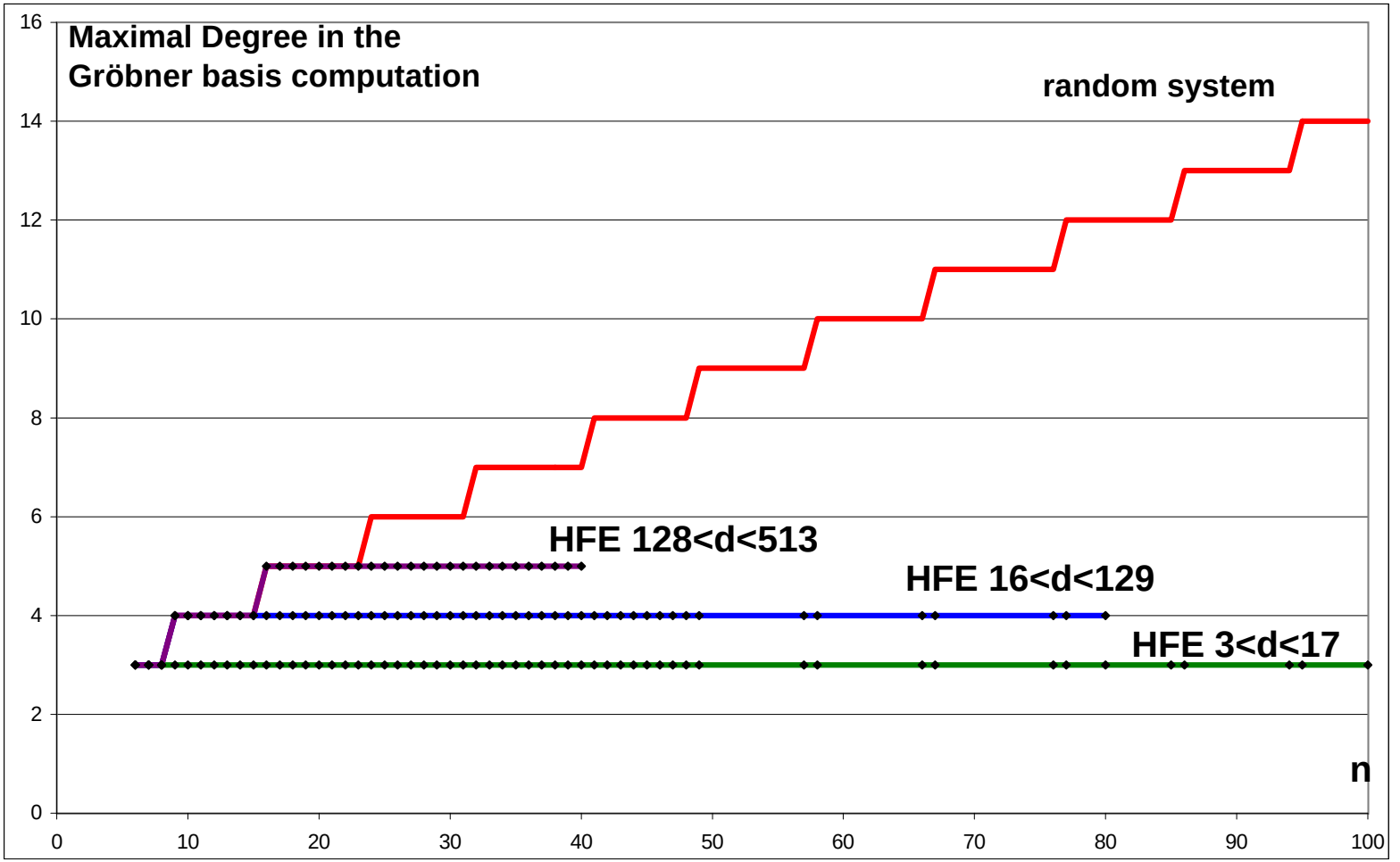
$$X = 64431800523905114055471 8$$

$$X = 93434489004594109861521 4$$

$$X = 10226777136290287612030 46$$

$$X = 10370460826518011495946 70$$

Maximal degree



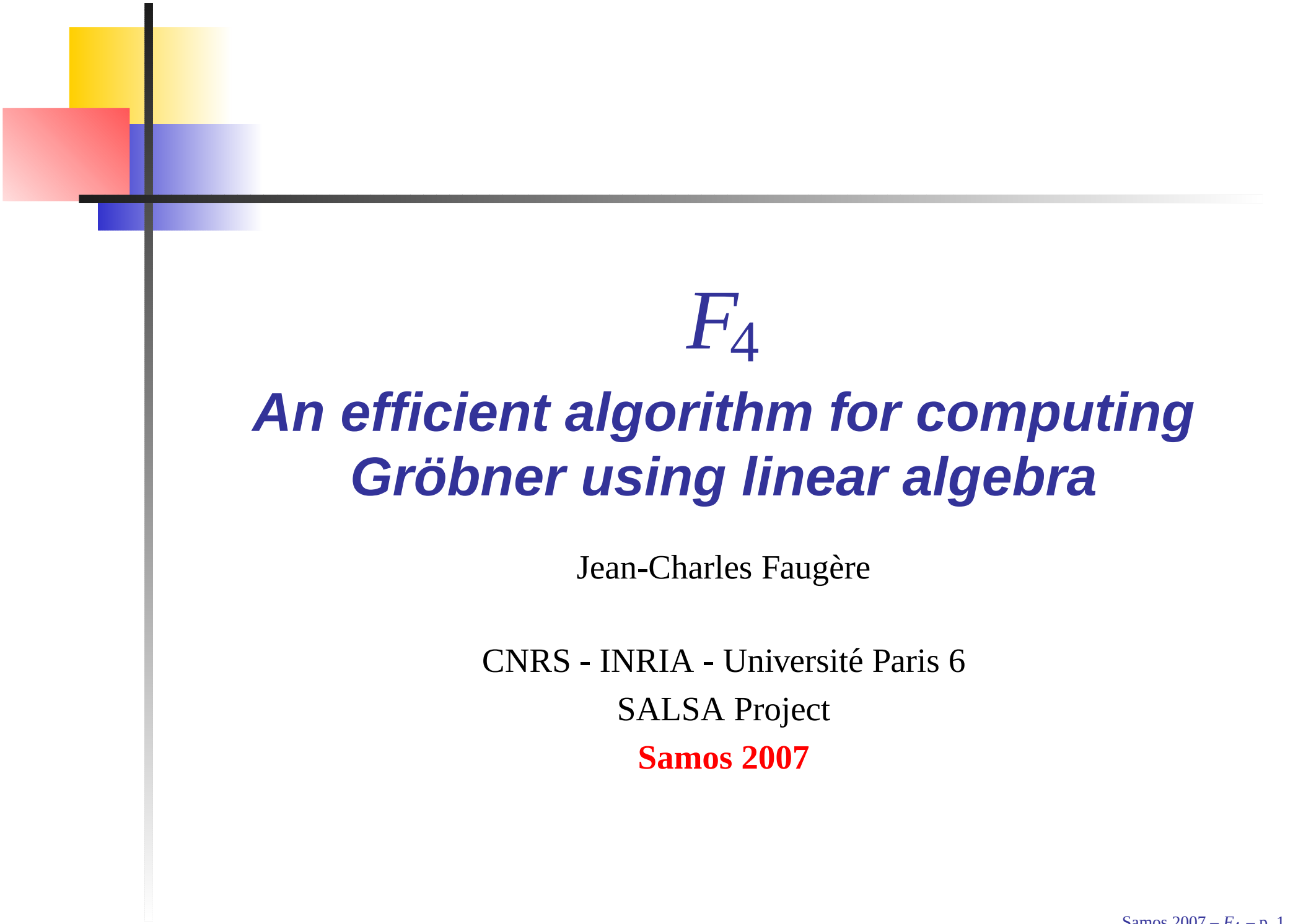
HFE Conclusion

d	D	Exp comp
$d < 17$	3	n^6
$17 \leq d < 129$	4	n^8
$129 \leq d < 513$	5	n^{10}

Complexity of HFE

Conclusion

- Applications: $\longrightarrow$ **Challenging problem** for Computer Algebra.
- Need very **powerful** algorithm/implementation.



F_4

An efficient algorithm for computing Gröbner using linear algebra

Jean-Charles Faugère

CNRS - INRIA - Université Paris 6

SALSA Project

Samos 2007

Plan of the talk

- Goal of F_4
- Description of the algorithm.
- Step by step example.

Goal of F_4

Among other things 3 big difficulties:

- A crucial issue to be faced in implementing the Buchberger algorithm is the choice of a Strategy.
- An apparent difficulty is the growth of the coefficients when computing with big integers.
- It is difficult to parallelize this algorithm: f_n depends strongly on f_{n-1}, f_{n-2}, $\ldots$ (if you remove zero !).

Goal of F_4

There are a lot of choices:

- select a critical pair in the list of critical pairs.
- choose one reductor among a list of reductors

Buchberger theorem $\longrightarrow$ not important for the correctness of the algorithm

Notations

- $\mathscr{P} = R[x_1, \ldots, x_n]$ is the polynomial ring.
- T the set of all terms.
- $F = [f_1, \ldots, f_m]$ algebraic equations
- $T(F)$ the support of F.
- a critical pair $Pair(f,g) = (\tau, t_f, f, t_g, g)$

  $(t_f, t_g) \in T^2,\ t_g.\mathrm{LT}(g) = t_f.\mathrm{LT}(f) = \tau = lcm(\mathrm{LT}(f),$
- the two projections $Left(Pair(f,g)) = (t_f, f)$, $Right(Pair(f,g)) = (t_g, g)$

Linear Algebra and Matrices

Trivial link: Linear Algebra $\leftrightarrow$ Polynomials

Definition: $F = (f_1, \ldots, f_m)$, $<$ ordering. A Matrix representation M_F of F is such that

$$\mathrm{T}F = M_F . \mathrm{T}X$$

where X the monomials (sorted for $<$) $\mathrm{T}(F)$:

$$M_F = \begin{array}{c} \\ f_1 \\ f_2 \\ f_3 \end{array} \begin{array}{c} m_1 > m_2 > m_3 \\ \begin{pmatrix} \cdots \\ \cdots \\ \cdots \end{pmatrix} \end{array}$$

Linear Algebra and Matrices

Trivial link: Linear Algebra $\leftrightarrow$ Polynomials

If Y is a vector of monomials, M a matrix then its polynomial representation is

$$^{\mathrm{T}}[f_1, \ldots, f_m] = M.{}^{\mathrm{T}}Y$$

Buchberger algorithm

Can be rewritten using linear algebra (simultating Spoly and reductions)

$$M_F = \begin{array}{c} \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_4 \end{array} \begin{array}{c} \begin{array}{cccc} m_1 & m_2 & m_3 & m_4 \end{array} \\ \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix} \end{array}$$

Macaulay method

Macaulay bound (for homogeneous polynomials):

$$D = 1 + \sum_{i=1}^{m} (deg(f_i) - 1)$$

We compute the matrix representation of $\{t\, f_i \; deg(t) \leq D - deg(f_i) \; i = 1, \ldots, m, <_{\mathrm{DRL}}$

Macaulay method

$$M_{\mathrm{Mac}} = \begin{array}{c} \\ t_1 f_1 \\ t_1' f_1 \\ t_2' f_2 \\ t_2 f_2 \\ t_3 f_3 \end{array} \begin{array}{c} m_1 > m_2 > m_3 > \cdots > m_r \\ \left(\begin{array}{c} \cdots \\ \cdots \\ \cdots \\ \cdots \\ \cdots \end{array} \right. \end{array}$$

Let $\tilde{M}_{\mathrm{Mac}}$ the result of Gaussian elimination.

Theorem: If F is regular then the polynomial representation of $\tilde{M}_{\mathrm{Mac}}$ is a Gröbner basis.

F_4: The algorithm

Algorithm $F4$

Input: $\begin{cases} F = (f_1, \ldots, f_m) \\ \mathscr{S}el\ List(Pairs) \to List(Pairs)\ \mathscr{S}el(l) \end{cases}$

$G := F$, $d := 0$, $P := \{Pair(f_i, f_j)\ i \neq j\}$

while $P \neq \emptyset$ **do**

$d := d + 1$

$P_d := \mathscr{S}el(P)$, $P := P \backslash P_d$

$\tilde{F}_d := Reduction(Left(P_d) \cup Right(P_d), G)$

for $h \in \tilde{F}_d$ **do**

$P := P \cup \{Pair(h, g) \mid g \in G\}$

$G := G \cup \{h\}$

return G

Reduction

Reduction

Input: $\begin{cases} L \text{ a finite subset of } T \times \mathscr{P} \\ G \text{ a finite subset of } \mathscr{P} \end{cases}$

Output: a finite subset of $\mathscr{P}$ (possibly an empty set).

$F := \text{Symbolic Preprocessing}(L, G)$

M the matrix representation of F.

$\tilde{M} :=$ Gaussian elimination M

$\tilde{F}$ the polynomial representation of M.

return $\left\{ f \in \tilde{F} \mid HT(f) \notin HT(F) \right\}$

Symbolic

Symbolic Preprocessing

Input: $\left\{L \subset T \times \mathscr{P}, G \subset \mathscr{P}\right.$

$F := \{t * f \mid (t, f) \in L\}$

$Done := \mathrm{LT}(F)$

while $\mathrm{T}(F) \neq Done$ **do**

m an element of $\mathrm{T}(F) \backslash Done$

$Done := Done \cup \{m\}$

if m top reducible modulo G **then**

$m = m' * \mathrm{LT}(f)$ for some $f \in G$ and some $m' \in T$

$F := F \cup \{m' * f\}$

return F

F_4: Example

$$\begin{cases} f_4 = x_1 + 2x_2 + 2x_3 + 2x_4 - 1 \\ f_3 = x_2^2 + 2x_1x_3 + 2x_2x_4 - x_3 \\ f_2 = 2x_1x_2 + 2x_2x_3 + 2x_3x_4 - x_2 \\ f_1 = x_1^2 + 2x_2^2 + 2x_3^2 + 2x_4^2 - x_1 \end{cases}$$

$G = [f_1, \ldots, f_4]$ and two critical pairs of degree 2

$$[x_1^2, 1, f_1, x_1, f_4]$$

$$[x_1x_2, 1, f_2, x_2, f_4]$$

F_4: Example

$$\begin{cases} f_4 = x_1 + 2x_2 + 2x_3 + 2x_4 - 1 \\ f_3 = x_2^2 + 2x_1x_3 + 2x_2x_4 - x_3 \\ f_2 = 2x_1x_2 + 2x_2x_3 + 2x_3x_4 - x_2 \\ f_1 = x_1^2 + 2x_2^2 + 2x_3^2 + 2x_4^2 - x_1 \end{cases}$$

$$[x_1^2, 1, f_1, x_1, f_4][x_1x_2, 1, f_2, x_2, f_4]$$

$L_2 = \{(1, f_1), (x_1, f_4), (1, f_2), (x_2, f_4)\}$
symbolic reduction: L_2 and G:

$$F = \{f_1, x_1 f_4, f_2, x_2 f_4\}$$

Cont

$Done = \{x_1^2, x_1x_2\}$

T(F)= $\{x_1^2, x_2^2, x_3^2, \boxed{x_4^2}, x_1, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_3x_4, x_2,$

Select $\boxed{x_4^2}$: cannot be reduced by G

Cont

$Done = \{x_1^2, x_1x_2\}$

T(F)= $\{x_1^2, x_2^2, x_3^2, \boxed{x_4^2}, x_1, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_3x_4, x_2,$

Select $\boxed{x_4^2}$: cannot be reduced by G

T(F)= $\{x_1^2, x_2^2, \boxed{x_3^2}, x_4^2, x_1, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_3x_4, x_2,$

Select $\boxed{x_3^2}$: cannot be reduced by G

Cont

$Done = \{x_1^2, x_1x_2\}$

T(F)= $\{x_1^2, x_2^2, x_3^2, \boxed{x_4^2}, x_1, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_3x_4, x_2,$

Select $\boxed{x_4^2}$: cannot be reduced by G

T(F)= $\{x_1^2, x_2^2, \boxed{x_3^2}, x_4^2, x_1, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_3x_4, x_2,$

Select $\boxed{x_3^2}$: cannot be reduced by G . . .

T(F)= $\{x_1^2, x_2^2, x_3^2, x_4^2, x_1, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_3x_4, x_2, x$

Select $\boxed{1}$: cannot be reduced by G

Cont

$Done = \{x_1^2, x_1x_2\}$

T(F)= $\{x_1^2, x_2^2, x_3^2, \boxed{x_4^2}, x_1, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_3x_4, x_2,$

Select $\boxed{x_4^2}$: cannot be reduced by G

T(F)= $\{x_1^2, x_2^2, \boxed{x_3^2}, x_4^2, x_1, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_3x_4, x_2,$

Select $\boxed{x_3^2}$: cannot be reduced by G . . .

T(F)= $\{x_1^2, x_2^2, x_3^2, x_4^2, x_1, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_3x_4, x_2, x$

Select $\boxed{1}$: cannot be reduced by G

T(F)= $\{x_1^2, \boxed{x_2^2}, x_3^2, x_4^2, x_1, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_3x_4, x_2,$

Select $\boxed{x_2^2}$: reducible by $1 \times f_3$

Cont

T(F)= $\{x_1^2, x_2^2, x_3^2, x_4^2, x_1, x_1x_2, \boxed{x_1x_3}, x_1x_4, x_2x_3, x_3x_4, x_2,$

Select $\boxed{x_1x_3}$: reducible by $x_3 \times f_4$

$$F = \{f_1, x_1 f_4, f_2, x_2 f_4, f_3, x_3 f_4\}$$

Cont

T(F)= $\{x_1^2, x_2^2, x_3^2, x_4^2, x_1, x_1x_2, \boxed{x_1x_3}, x_1x_4, x_2x_3, x_3x_4, x_2,$

Select $\boxed{x_1x_3}$: reducible by $x_3 \times f_4$

$$F = \{f_1, x_1 f_4, f_2, x_2 f_4, f_3, x_3 f_4\}$$

. . .

T(F)= $\{x_1^2, x_2^2, x_3^2, x_4^2, x_1, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_3x_4, x_2, x$
$1, x_3, x_4\}$

$$F = \{f_1, x_1 f_4, f_2, x_2 f_4, f_3, x_3 f_4, x_4 f_4, f_4\}$$

Matrice

The symbolic reduction returns:

	x_1^2	x_1x_2	x_2^2	x_1x_3	x_2x_3	x_3^2	x_1x_4	x_2x_4	x_3x_4	x_4^2	x_1	x_2	x_3	x_4	1
f_4	0	0	0	0	0	0	0	0	0	0	1	2	2	2	-1
$x_4 f_4$	0	0	0	0	0	0	1	2	2	2	0	0	0	-1	0
$x_3 f_4$	0	0	0	1	2	2	0	0	2	0	0	0	-1	0	0
f_3	0	0	1	2	0	0	0	2	0	0	0	0	-1	0	0
f_2	0	1	0	0	1	0	0	0	1	0	0	$-1/2$	0	0	0
$x_2 f_4$	0	1	2	0	2	0	0	2	0	0	0	-1	0	0	0
f_1	1	0	2	0	0	2	0	0	0	2	-1	0	0	0	0
$x_1 f_4$	1	2	0	2	0	0	2	0	0	0	-1	0	0	0	0

Matrice

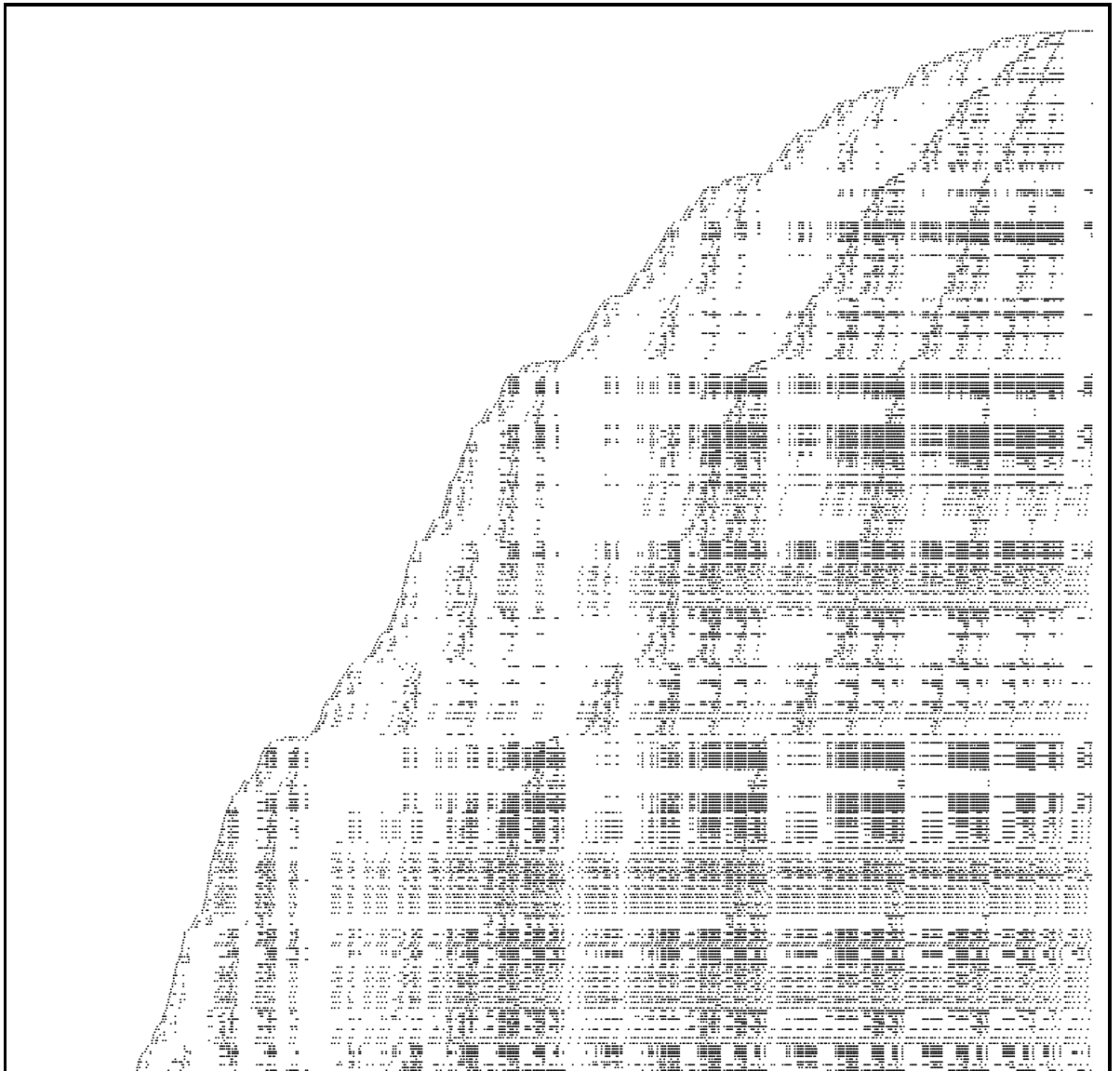
then the matrix is reduced to *row echelon form*:

	x_1^2	x_1x_2	x_2^2	x_1x_3	x_2x_3	x_3^2	x_1x_4	x_1	x_2x_4	x_3x_4	x_4^2	x_2	x_3	x_4	1
f_4	0	0	0	0	0	0	0	1	0	0	0	2	2	2	-1
$x_4 f_4$	0	0	0	0	0	0	1	0	2	2	2	0	0	-1	0
$x_1 f_4$	0	0	0	0	0	1	0	0	2	$\frac{32}{7}$	$\frac{27}{7}$	$\frac{-1}{7}$	$\frac{-4}{7}$	$\frac{-9}{7}$	0
$x_2 f_4$	0	0	0	0	1	0	0	0	-2	$-\frac{23}{7}$	$-\frac{24}{7}$	$\frac{1}{14}$	$\frac{2}{7}$	$\frac{8}{7}$	0
$x_3 f_4$	0	0	0	1	0	0	0	0	0	$\frac{-4}{7}$	$\frac{-6}{7}$	$\frac{1}{7}$	$\frac{-3}{7}$	$\frac{2}{7}$	0
f_3	0	0	1	0	0	0	0	0	2	$\frac{8}{7}$	$\frac{12}{7}$	$\frac{-2}{7}$	$\frac{-1}{7}$	$\frac{-4}{7}$	0
f_2	0	1	0	0	0	0	0	0	2	$\frac{30}{7}$	$\frac{24}{7}$	$\frac{-4}{7}$	$\frac{-2}{7}$	$-\frac{8}{7}$	0
f_1	1	0	0	0	0	0	0	0	-8	$-\frac{80}{7}$	$-\frac{64}{7}$	$\frac{20}{7}$	$\frac{24}{7}$	$\frac{40}{7}$	-1

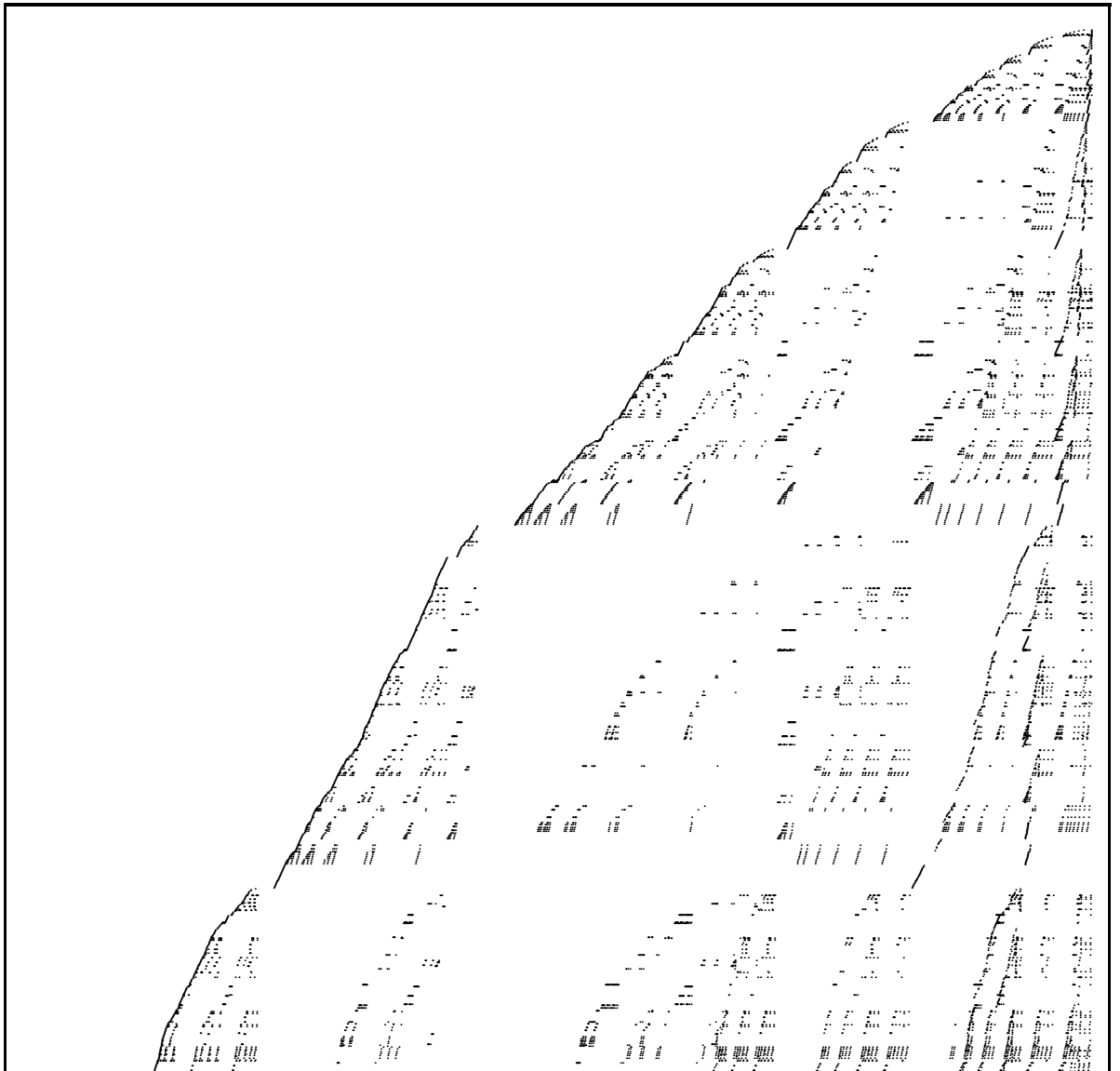
Degree 3

Let f_{i+3} be the polynomial corresponding to the i th row of this matrix ($i = 2, 3, \ldots, 8$). (for instance $f_5 = x_1x_4 + 2x_2x_4 + \cdots$).
The next degree is $d = 3$ and $L_3 = \{(x_2, f_2), (x_1, f_3), (x_3, f_3), (x_2, f_6), (x_2, f_5), (x_3, f_6)\}$

F_4: some matrices



Matrix



F_4: some remarks

Theorem 1 *The algorithm F_4 computes a Gröbner basis G in $\mathscr{P}$ such that $F \subseteq G$ and $Id(G) = Id(F)$.*

- The algorithm computes *successive truncated* Gröbner bases.
- Designed for degree ordering.
- Replaces the classical Buchberger reduction by *the simultaneous reduction* of several polynomials.

F_4: some remarks

- The new reduction mechanism is achieved by means of a *symbolic precomputation* and by extensive used of *sparse linear algebra methods*.
- Even though the new algorithm does not improve the worst case complexity it is *several times faster* than the other algorithms/mplementations (both for integers and modulo p computations).
- symbolic reduction $\longrightarrow$ *efficient* complexity depends on the #*the support* $\neq$ the number of (non zero) elements in the final matrix A.

Conclusion

- We have transformed the *degree of freedom* in the Buchberger algorithm into strategies for *efficiently solving linear algebra* systems.
- This is easier because we have constructed the matrix A and we can decide to begin the reduction of one row before another with a *"good reason"*.
- For integer coefficients it is a major advantage to be able to apply an iterative algorithm on the whole matrix.

Conclusion

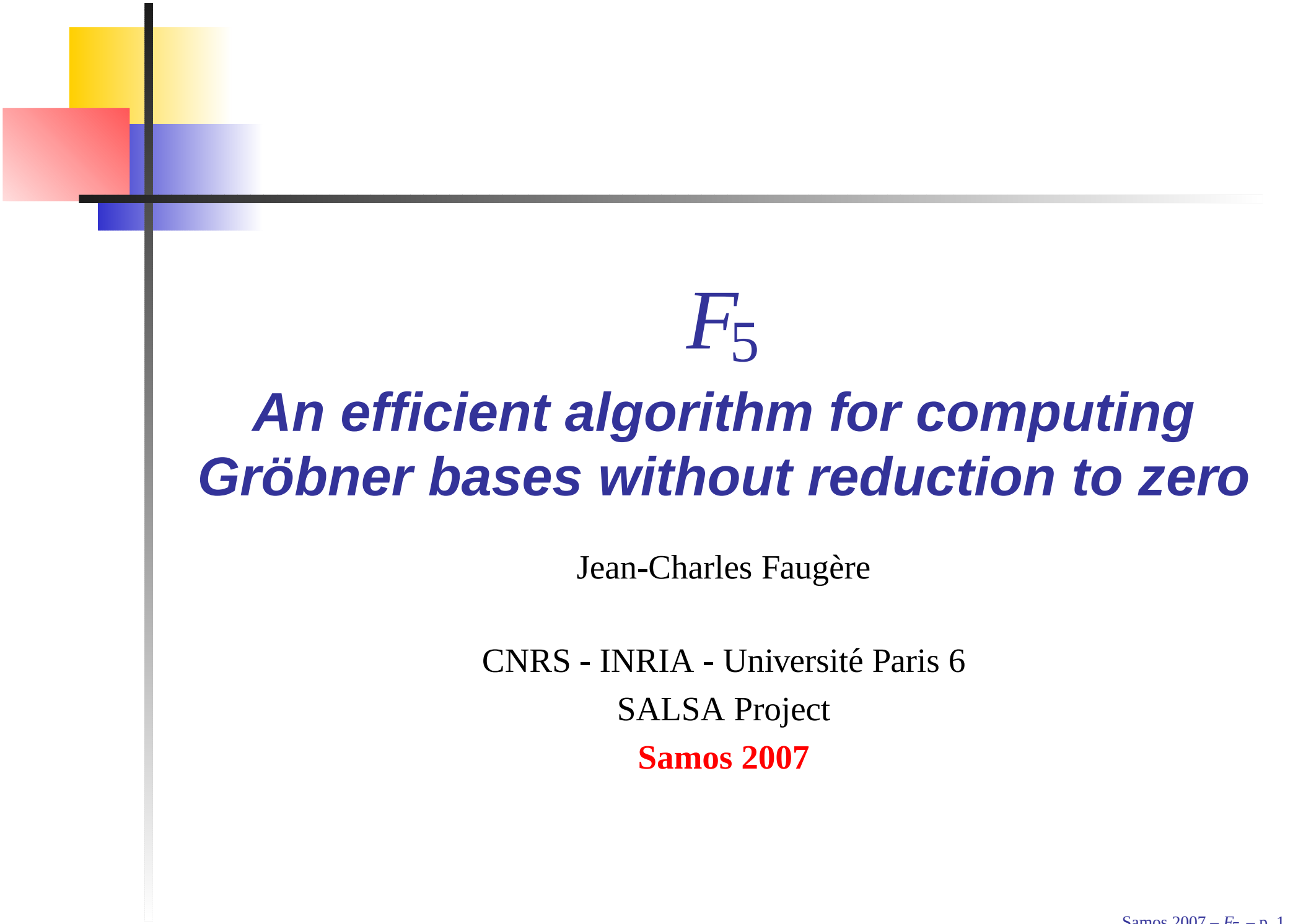
- Bad point: the matrix A is *singular*

$\longrightarrow$ see F_5

- Bad point: A is often *huge*.

$\longrightarrow$ compression divide the size of A by > 10

- Not efficient for monomials or binomials (Mayr/Meyer example).
- Difficult to implement (but . . .)



F_5

An efficient algorithm for computing Gröbner bases without reduction to zero

Jean-Charles Faugère

CNRS - INRIA - Université Paris 6

SALSA Project

Samos 2007

Plan of the talk

- Goal
- The idea
- Theorem
- Description of the algorithm
- Simple description for dense polynomials
- Experimental efficiency
  - Number of useless critical pairs

Goal of F_5

Computing Gröbner bases: Buchberger algorithm or F_4

with Buchberger Criteria 90% of the time is spent in **computing zero**

Open issue remove useless computations.

$\longrightarrow$ a more powerful criterion to remove useless critical pairs.

Goal of F_5: **theoretical and practical answer.**

Goal of F_5

Goal of F_5: **theoretical and practical answer.**

Gröbner basis of $(f_1, \ldots, f_m)$

what is a reduction to zero ?

$$\sum_{i=1}^{m} g_i f_i = 0$$

$(g_1, \ldots, g_m)$ is a **syzygy**.

Previous Work

Buchberger 1979: *A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Basis.*
(two criteria remove 90% of useless critical pairs.)
Gebauer and Moller 1986: *Buchberger's Algorithm and Staggered Linear Bases.*
Möller, Mora and Traverso 1992 : *Gröbner Bases Computation Using Syzygies*
Gerdt Blinkov 1998 *Involutive Bases of Polynomial Ideals* some reductions are forbidden

Previous Work

Buchberger 1979: *A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Basis.*

The efficiency of those algorithms is not yet satisfactory in theory and practice because a lot of useless critical pairs are not removed.

The Idea

$$\mathscr{S}_b \begin{cases} f_3 = x^2 + 18xy + 19y^2 + 8xz + 5yz + 7z^2 \\ f_2 = 3x^2 + (7+b)xy + 22xz + 11yz + 22z^2 + 8y^2 \\ f_1 = 6x^2 + 12xy + 4y^2 + 14xz + 9yz + 7z^2 \end{cases}$$

The Idea

$$\mathscr{S}_0 \begin{cases} f_3 = x^2 + 18xy + 19y^2 + 8xz + 5yz + 7z^2 \\ f_2 = 3x^2 + 7xy + 22xz + 11yz + 22z^2 + 8y^2 \\ f_1 = 6x^2 + 12xy + 4y^2 + 14xz + 9yz + 7z^2 \end{cases}$$

With Buchberger $x > y > z$:

- 5 useless reductions
- 5 useful pairs

We proceed degree by degree.

The Idea

$$\mathscr{S}_0 \begin{cases} f_3 = x^2 + 18xy + 19y^2 + 8xz + 5yz + 7z^2 \\ f_2 = 3x^2 + 7xy + 22xz + 11yz + 22z^2 + 8y^2 \\ f_1 = 6x^2 + 12xy + 4y^2 + 14xz + 9yz + 7z^2 \end{cases}$$

$$A_2 = \begin{array}{c} \\ f_3 \\ f_2 \\ f_1 \end{array} \begin{array}{c} \begin{array}{cccccc} x^2 & xy & y^2 & xz & yz & z^2 \end{array} \\ \begin{pmatrix} 1 & 18 & 19 & 8 & 5 & 7 \\ 3 & 7 & 8 & 22 & 11 & 22 \\ 6 & 12 & 4 & 14 & 9 & 7 \end{pmatrix} \end{array}$$

The Idea

$$\mathscr{S}_0 \begin{cases} f_3 = x^2 + 18xy + 19y^2 + 8xz + 5yz + 7z^2 \\ f_2 = 3x^2 + 7xy + 22xz + 11yz + 22z^2 + 8y^2 \\ f_1 = 6x^2 + 12xy + 4y^2 + 14xz + 9yz + 7z^2 \end{cases}$$

$$B_2 = \begin{array}{c} \\ f_3 \\ f_2 \\ f_1 \end{array} \begin{array}{c} \begin{array}{cccccc} x^2 & xy & y^2 & xz & yz & z^2 \end{array} \\ \begin{pmatrix} 1 & 18 & 19 & 8 & 5 & 7 \\ 0 & 1 & 3 & 2 & 4 & -1 \\ 0 & 0 & 1 & -11 & -3 & -5 \end{pmatrix} \end{array}$$

The Idea

$$\mathscr{S}_0 \begin{cases} f_3 = x^2 + 18xy + 19y^2 + 8xz + 5yz + 7z^2 \\ f_2 = 3x^2 + 7xy + 22xz + 11yz + 22z^2 + 8y^2 \\ f_1 = 6x^2 + 12xy + 4y^2 + 14xz + 9yz + 7z^2 \end{cases}$$

$$B_2 = \begin{array}{c} \\ f_3 \\ f_2 \\ f_1 \end{array} \begin{array}{c} \begin{array}{cccccc} x^2 & xy & y^2 & xz & yz & z^2 \end{array} \\ \begin{pmatrix} 1 & 18 & 19 & 8 & 5 & 7 \\ 0 & 1 & 3 & 2 & 4 & -1 \\ 0 & 0 & 1 & -11 & -3 & -5 \end{pmatrix} \end{array}$$

"new" polynomials $f_4 = xy + 4yz + 2xz + 3y^2 - z^2$
and $f_5 = y^2 - 11xz - 3yz - 5z^2$

Degree 3

$$f_3 = x^2 + 18xy + 19y^2 + 8xz + 5yz + 7z^2$$
$$f_2 = 3x^2 + 7xy + 22xz + 11yz + 22z^2 + 8y^2$$
$$f_1 = 6x^2 + 12xy + 4y^2 + 14xz + 9yz + 7z^2$$
$$f_4 = xy + 4yz + 2xz + 3y^2 - z^2$$
$$f_5 = y^2 - 11xz - 3yz - 5z^2$$

and

$$f_2 \longrightarrow f_4$$
$$f_1 \longrightarrow f_5$$

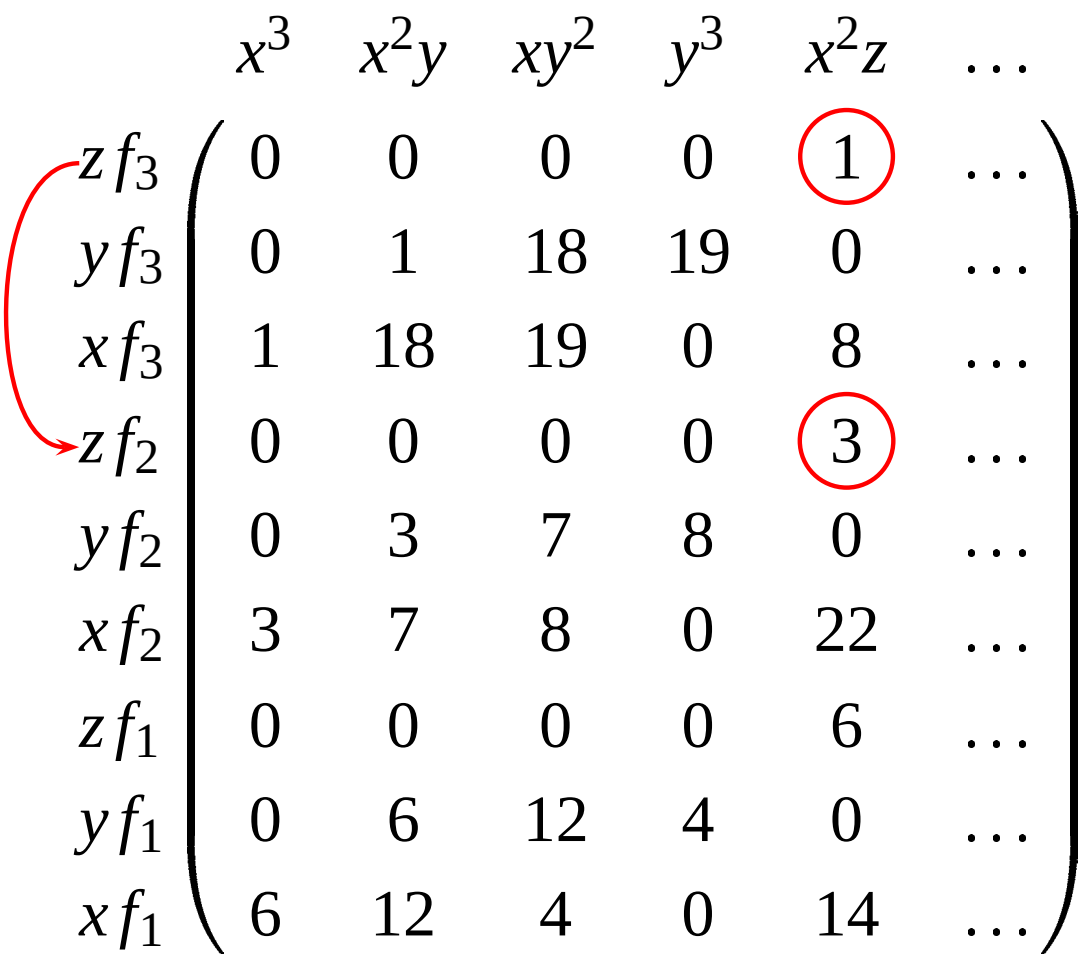
Degree 3

$$
\begin{array}{c}
 \\
zf_3 \\
yf_3 \\
xf_3 \\
zf_2 \\
yf_2 \\
xf_2 \\
zf_1 \\
yf_1 \\
xf_1
\end{array}
\begin{array}{c}
\begin{array}{ccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \end{array} \\
\begin{pmatrix}
0 & 0 & 0 & 0 & 1 & \dots \\
0 & 1 & 18 & 19 & 0 & \dots \\
1 & 18 & 19 & 0 & 8 & \dots \\
0 & 0 & 0 & 0 & 3 & \dots \\
0 & 3 & 7 & 8 & 0 & \dots \\
3 & 7 & 8 & 0 & 22 & \dots \\
0 & 0 & 0 & 0 & 6 & \dots \\
0 & 6 & 12 & 4 & 0 & \dots \\
6 & 12 & 4 & 0 & 14 & \dots
\end{pmatrix}
\end{array}
$$

Degree 3

	x^3	x^2y	xy^2	y^3	x^2z	$\ldots$
zf_3	0	0	0	0	1	$\ldots$
yf_3	0	1	18	19	0	$\ldots$
xf_3	1	18	19	0	8	$\ldots$
zf_2	0	0	0	0	3	$\ldots$
yf_2	0	3	7	8	0	$\ldots$
xf_2	3	7	8	0	22	$\ldots$
zf_1	0	0	0	0	6	$\ldots$
yf_1	0	6	12	4	0	$\ldots$
xf_1	6	12	4	0	14	$\ldots$

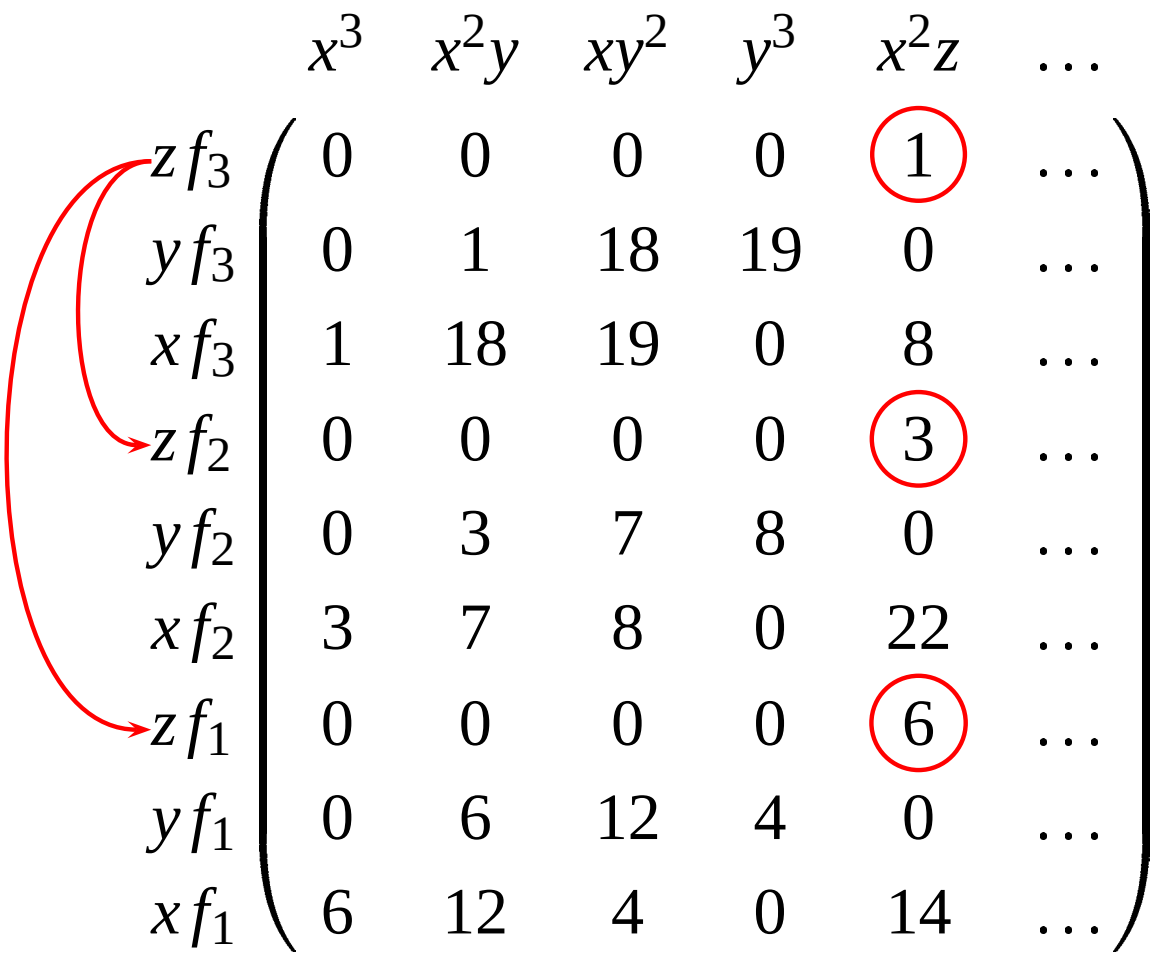
Degree 3


x^3 x^2y xy^2 y^3 x^2z …
zf_3 0 0 0 0 1 …
yf_3 0 1 18 19 0 …
xf_3 1 18 19 0 8 …
zf_2 0 0 0 0 3 …
yf_2 0 3 7 8 0 …
xf_2 3 7 8 0 22 …
zf_1 0 0 0 0 6 …
yf_1 0 6 12 4 0 …
xf_1 6 12 4 0 14 …

Degree 3

$f_2 \longrightarrow f_4$

$f_1 \longrightarrow f_5$



Degree 3

	x^3	x^2y	xy^2	y^3	x^2z	xyz	y^2z	xz^2	yz^2	z^3
zf_3	0	0	0	0	1	18	19	8	5	7
yf_3	0	1	18	19	0	8	5	0	7	0
xf_3	1	18	19	0	8	5	0	7	0	0
zf_4	0	0	0	0	0	1	3	2	4	22
yf_4	0	0	1	3	0	2	4	0	22	0
xf_4	0	1	3	0	2	4	0	22	0	0
zf_5	0	0	0	0	0	0	1	12	20	18
yf_5	0	0	0	1	0	12	20	0	18	0
xf_5	0	0	1	0	12	20	0	18	0	0

Degree 3

	x^3	x^2y	xy^2	y^3	x^2z	xyz	y^2z	xz^2	yz^2	z^3
xf_3	1	18	19	0	8	5	0	7	0	0
yf_3		1	18	19	0	8	5	0	7	0
yf_2			1	3	0	2	4	0	22	0
$\mathbf{xf_2}$				1	0	0	8	1	18	15
zf_3					1	18	19	8	5	7
zf_2						1	3	2	4	22
zf_1							1	12	20	18
$\mathbf{yf_1}$								1	11	13
$\mathbf{xf_1}$									1	18

Degree 3

We have constructed 3 new polynomials

$$f_6 = y^3 + 8y^2z + xz^2 + 18yz^2 + 15z^3$$
$$f_7 = xz^2 + 11yz^2 + 13z^3$$
$$f_8 = yz^2 + 18z^3$$

We have the linear equivalences:

$$x\,f_2 \leftrightarrow x\,f_4 \leftrightarrow f_6$$
$$f_4 \longrightarrow f_2$$

Degree 4

The matrix whose rows are

$$x^2 f_i, xy f_i, y^2 f_i, xz f_i, yz f_i, z^2 f_i, \ i = 1,2,3$$

is not full rank !

Why ? (1)

$6 \times 3 =$ 18 rows

$x^4, x^3 y, \ldots, y z^3, z^4$ 15 columns

Why ? (1)

$6 \times 3 =$ 18 rows

$x^4, x^3 y, \ldots, y z^3, z^4$ 15 columns

Simple linear algebra theorem: 3 useless row (which ones ?)

Why (2)

$$f_2 f_3 - f_3 f_2 = 0$$

can be rewritten

$$3x^2 f_3 + (7+b) xy f_3 + 8y^2 f_3 + 22 xz f_3$$

$$+11 yz f_3 + 22 z^2 f_3 - x^2 f_2 - 18 xy f_2 - 19 y^2 f_2$$

$$-8 xz f_2 - 5 yz f_2 - 7 z^2 f_2 = 0$$

Why (2)

$$f_2 f_3 - f_3 f_2 = 0$$

can be rewritten

$$3x^2 f_3 + (7+b) xy f_3 + 8y^2 f_3 + 22 xz f_3$$
$$+11 yz f_3 + 22 z^2 f_3 - x^2 f_2 - 18 xy f_2 - 19 y^2 f_2$$
$$-8 xz f_2 - 5 yz f_2 - 7 z^2 f_2 = 0$$

We can remove the row $x^2 f_2$

Why (2)

same way $f_1 f_3 - f_3 f_1 = 0 \longrightarrow$ remove $x^2 f_1$

but $f_1 f_2 - f_2 f_1 = 0 \longrightarrow$ remove $x^2 f_1$!

Why (2)

$$
\begin{aligned}
0 &= (f_2 f_1 - f_1 f_2) - 3(f_3 f_1 - f_1 f_3) \\
0 &= (f_2 - 3 f_3) f_1 - f_1 f_2 + 3 f_1 f_3 \\
0 &= f_4 f_1 - f_1 f_2 + 3 f_1 f_3 \\
0 &= \left((1-b)xy + 4yz + 2xz + 3y^2 - z^2\right) f_1 \\
&\quad -(6x^2 + \cdots) f_2 + 3(6x^2 + \cdots) f_3
\end{aligned}
$$

- if $b \neq 1$ remove $xy\, f_1$
- if $b = 1$ remove $yz\, f_1$

Need “some” computation

Criterion

Any combination of the trivial relations $f_i f_j = f_j f_i$ can always be written:

$$u(f_2 f_1 - f_1 f_2) + v(f_3 f_1 - f_1 f_3) + w(f_2 f_3 - f_3 f_2)$$

where u, v, w are arbitrary polynomials.

Criterion

Any combination of the trivial relations $f_i f_j = f_j f_i$ can always be written:

$$(u f_2 + v f_3)\ f_1 - u f_1 f_2 - v f_1 f_3 + w f_2 f_3 - w f_3 f_2$$

Criterion

Any combination of the trivial relations $f_i f_j = f_j f_i$ can always be written:

$$\boxed{(u f_2 + v f_3)} f_1 - u f_1 f_2 - v f_1 f_3 + w f_2 f_3 - w f_3 f_2$$

(trivial) relation $h f_1 + \cdots = 0 \leftrightarrow h \in Id(f_2, f_3)$

Compute a Gröbner basis of $(f_2, f_3) \longrightarrow G_{\text{prev}}$.

Remove line $h f_1$ iff $LT(h)$ top reducible by G_{prev}

Degree 4

$$y^2 f_1, xz f_1, yz f_1, z^2 f_1$$
$$xy f_2, y^2 f_2, xz f_2, yz f_2, z^2 f_2$$
$$x^2 f_3, xy f_3, y^2 f_3, xz f_3, yz f_3, z^2 f_3$$

Degree 4

$$y^2 f_1, xz f_1, yz f_1, z^2 f_1$$
$$xy f_2, y^2 f_2, xz f_2, yz f_2, z^2 f_2$$
$$x^2 f_3, xy f_3, y^2 f_3, xz f_3, yz f_3, z^2 f_3$$

In order to use previous computations (degree 2 and 3):

$$x f_2 \to f_6 \quad f_2 \to f_4$$
$$x f_1 \to f_8 \quad y f_1 \to f_7$$
$$f_1 \to f_5$$

Degree 4

$$y f_7, z f_8, z f_7, z^2 f_5, y f_6, y^2 f_4, z f_6, y z f_4,$$
$$z^2 f_4, x^2 f_3, x y f_3, y^2 f_3, x z f_3, y z f_3, z^2 f_3,$$

Degree 4

$$
\begin{bmatrix}
1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 \\
 & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 & & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 \\
 & & & 1 & 3 & 0 & 0 & 2 & 4 & 0 & 0 & 22 & 0 & 0 & 0 \\
 & & & & 1 & 0 & 0 & 0 & 8 & 0 & 1 & 18 & 0 & 15 & 0 \\
 & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 & 0 \\
 & & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 \\
 & & & & & & & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 \\
 & & & & & & & & 1 & 0 & 0 & 8 & 1 & 18 & 15 \\
 & & & & & & & & & 1 & 18 & 19 & 8 & 5 & 7 \\
 & & & & & & & & & & 1 & 11 & 0 & 13 & 0 \\
 & & & & & & & & & & & 1 & 12 & 20 & 18 \\
 & & & & & & & & & & & & 1 & 11 & 13 \\
 & & & & & & & & & & & & & 1 & 18 \\
 & & & & & & & & & & 1 & 3 & 2 & 4 & 22
\end{bmatrix}
$$

Degree 4

$$
\begin{array}{c}
 & \begin{array}{ccccc} xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \end{array} \\
\begin{array}{c} z^2 f_4 \\ z^2 f_5 \\ z f_7 \\ z f_8 \\ y f_7 \end{array} &
\begin{pmatrix}
1 & 3 & 2 & 4 & 22 \\
 & 1 & 12 & 20 & 18 \\
 & & 1 & 11 & 13 \\
 & & & 1 & 18 \\
1 & 11 & 0 & 13 & 0
\end{pmatrix}
\end{array}
$$

Partial conclusion

- Incremental algorithm

$$(f) + G_{\text{old}}$$

- Give a “unique name” to each row.

  Remove $h f_1 + \cdots$ if $LT(h) \in LT(G_{\text{old}})$

  $LT(h)$ signature of the row

- Implementation of the rewritten rules.

Signature of a polynomial

- $\mathscr{P}$ ring of polynomials $k[x_1, \ldots, x_n]$

Signature of a polynomial

- $\mathscr{P}$ ring of polynomials $k[x_1, \ldots, x_n]$

$$I = (f_1) + I_{\text{old}}$$

Signature of a polynomial

$\mathscr{P}$ ring of polynomials $k[x_1, \ldots, x_n]$

$$I = (f_1) + I_{\text{old}}$$

Objects actually used in the algorithm:

$$(u, f) \in T \times \mathscr{P}, \exists g_1 \in \mathscr{P}, f' \in I_{\text{old}}$$

s.t. $f = g_1 f_1 + f'$ where $LT(g_1) = u$

Signature (2)

$$r = (u, f) \in T \times \mathscr{P}, \exists g_1 \in \mathscr{P}, f' \in I_{\text{old}}$$
s.t. $f = g_1 f_1 + f'$ where $LT(g_1) = u$

We say that it is **admissible**

Signature (2)

$$r = (u, f) \in T \times \mathscr{P}, \exists g_1 \in \mathscr{P}, f' \in I_{\text{old}}$$
s.t. $f = g_1 f_1 + f'$ where $LT(g_1) = u$

We say that it is **admissible**

$$\text{poly}(r) = f \in \mathscr{P}$$
$$\mathscr{S}(r) = u \in T$$

Signature (2)

$$r = (u, f) \in T \times \mathscr{P}, \exists g_1 \in \mathscr{P}, f' \in I_{\text{old}}$$
s.t. $f = g_1 f_1 + f'$ where $LT(g_1) = u$

We say that it is **admissible**

$$\text{poly}(r) = f \in \mathscr{P}$$
$$\mathscr{S}(r) = u \in T$$

Example: $(f_2) + Id(f_3)$

$$r_2 = (1, 3x^2 + 7xy + 22xz + 11yz + 22z^2 + 8y^2)$$
$$r_6 = (x, y^3 + 8y^2z + xz^2 + \cdots) = (x + \cdots) f_2 + (\cdots) f_3$$

Signature (2)

$$r = (u, f) \in T \times \mathscr{P}, \exists g_1 \in \mathscr{P}, f' \in I_{\text{old}}$$
s.t. $f = g_1 f_1 + f'$ where $LT(g_1) = u$

We say that it is **admissible**

$$\text{poly}(r) = f \in \mathscr{P}$$
$$\mathscr{S}(r) = u \in T$$

$$LT(r) = LT(\text{poly}(r)).$$
$$LC(r) = LC(\text{poly}(r)).$$
$$G \subset \mathscr{P}, \text{NF}(r, G) = (\mathscr{S}(r), NF(\text{poly}(r), G)).$$

New criterion

We say that r is normalised if

$$\mathscr{S}(r) \notin LT(I_{\text{old}})$$

New criterion

We say that r is normalised if

$$\mathscr{S}(r) = u \text{ and } \varphi(u) = u$$
$$\text{where } \varphi = NF(.,Groebner(I_{\text{old}}))$$

New criterion

We say that r is normalised if

$$\mathscr{S}(r) = u \text{ and } \varphi(u) = u$$
$$\text{where } \varphi = NF(.,Groebner(I_{\text{old}}))$$

A critical pair $(r_i, r_j) = u_i r_i - u_j r_j$ is *normalised* if

- $u_j \mathscr{S}(r_j) \prec u_i \mathscr{S}(r_i)$
- $u_j r_j$ and $u_i r_i$ normalised

$$u_i = \frac{lcm(LT(r_i),LT(r_j))}{LT(r_i)}, \; u_j = \frac{lcm(LT(r_i),LT(r_j))}{LT(r_j)}.$$

Theorem

If $F = [f_1, \ldots, f_m]$ and $G = [r_1, \ldots, r_k]$ such that

(i) $F \subset \text{poly}(G)$. Let g_i be $\text{poly}(r_i)$ and $G_1 = [g_1, \ldots, g_k]$.

(ii) r_i admissible $(i = 1, \ldots, k)$.

(iii) for all $(i, j) \in \{1, \ldots, k\}$, such that the critical pair (r_i, r_j) is normalised then $\text{spol}(g_i, g_j) \longrightarrow 0$

Then G_1 is Gröbner basis of I.

Theorem

If $F = [f_1, \ldots, f_m]$ and $G = [r_1, \ldots, r_k]$ such that

(i) $F \subset \text{poly}(G)$. Let g_i be $\text{poly}(r_i)$ and $G_1 = [g_1, \ldots, g_k]$.

(ii) r_i admissible $(i = 1, \ldots, k)$.

(iii) for all $(i, j) \in \{1, \ldots, k\}$, such that the critical pair (r_i, r_j) is normalised then $\text{spol}(g_i, g_j)$ has a t representation for $t < u_i r_i$ with $u_i = \frac{lcm(LT(g_i), LT(g_j))}{LT(r_i)}$.

Then G_1 is Gröbner basis of I.

F_5 Algorithm

Input: $f, G_{\text{old}}, \varphi = \text{NF}(.,G_{\text{old}})$

$G := G_{\text{old}} \cup \{r = (1, f)\}$

$P := \left(\left[CritPair(r,r',\varphi) \,|\, r' \in G_{\text{old}}\right]\right)$

while $P \neq \emptyset$ **do**

$P_d := \{p \in P \,|\, deg(p) = \text{min degree of} P\}$

$R_d := Reduction(Spol(P_d)), G, \varphi)$

for $r \in R_d$ **do**

$P := (P \cup \{CritPair(r,r',\varphi) \,|\, r' \in G])$

$G := G \cup \{r\}$

return G

Critpair

$$\text{Critpair}(r,r') = \begin{cases} \emptyset \ \textit{if} \ (r,r') \ \textit{not normalised} \\ [t,u_1,r_1,u_2,r_2] \ \textit{else} \end{cases}$$

where

$$t = lcm(LT(r_1),LT(r_2))$$
$$u_1 = \frac{t}{LT(r_1)}$$
$$u_2 = \frac{t}{LT(r_2)}$$

S-polynomials

$$\mathrm{Spol}([t, u_1, r_1, u_2, r_2]) =$$

$$\begin{cases} \emptyset \quad \textit{if } u_i r_i \text{ can be rewritten} \\ \textit{else} \\ r_{N+1} := (u_1 \mathscr{S}(r_1), u_1 \,\mathrm{poly}(r_1) - u_2 \,\mathrm{poly}(r_2)) \\ \qquad N := N + 1 \\ \qquad \text{Add the new rule } \mathscr{S}(r_N) \to r_N \end{cases}$$

Is Reducible ?

r top reducible by r' = if

$$\begin{cases} u = \dfrac{LT(r)}{LT(r')} \text{ is a monomial} \\ \textit{and} \quad ur' \text{ normalised} (\varphi(u\mathscr{S}(r_{i_j})) = u\mathscr{S}(r_{i_j})) \\ \textit{and} \quad ur' \text{ cannot be rewritten} \end{cases}$$

Top Reduction

if r is top reducible by r' ($u = \frac{LT(r)}{LT(r')}$)

r top reducible by r' =

$$\begin{cases} \{(\mathscr{S}(r), \mathrm{poly}(r) - u\,\mathrm{poly}(r'))\} \\ \qquad \text{if } u\mathscr{S}(r') \prec \mathscr{S}(r) \\ \hline \{r, r_{N+1}\} \\ \quad r_{N+1} = (u\mathscr{S}(r'), u\,\mathrm{poly}(r') - \mathrm{poly}(r)) \\ \quad N := N + 1 \\ \quad \text{Add a new rule} \mathscr{S}(r_N) \longrightarrow r_N) \\ \qquad \text{else } \mathscr{S}(r) \prec u\mathscr{S}(r') \end{cases}$$

Theoretical results

Theorem 1 *Termination of the algorithm.*

Theorem 2 *The result of the algorithm* F_5 *is a (non reduced) Gröbner basis.*

Theorem 3 *If the algorithm finds a reduction to zero,* $r_{i_k} \to 0$ *then there exists* $\mathbf{s} \in \mathrm{Syz} \backslash \mathrm{PSyz}$ *with* $LT(\mathbf{s}) = \mathscr{S}(r_{i_k})$.

Corollary 4 *If the input system is a* regular sequence *there is no reduction to zero.*

Corollary 5 *For* almost all systems *there is no reduction to zero.*

F_5 matrix

Special/Simpler version of F_5 for dense/generic polynomials.
the maximal degree D is a *parameter* of the algorithm. degree d $m = 2$, $\deg(f_i) = 2$ homogeneous quadratic polynomials, degree d:

F_5 matrix

$m = 2$, $\deg(f_i) = 2$ homogeneous quadratic polynomials, degree d:

$$\begin{array}{c} \\ u_1 f_1 \\ u_2 f_1 \\ u_3 f_1 \\ v_1 f_2 \\ v_2 f_2 \end{array} \begin{array}{c} \begin{array}{ccccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \dots \end{array} \\ \begin{pmatrix} x & x & x & x & x & \dots \\ x & x & x & x & x & \dots \\ x & x & x & x & x & \dots \\ x & x & x & x & x & \dots \\ x & x & x & x & x & \dots \end{pmatrix} \end{array}$$

$$\deg(u_i) = \deg(v_i) = d - 2$$

Gauss

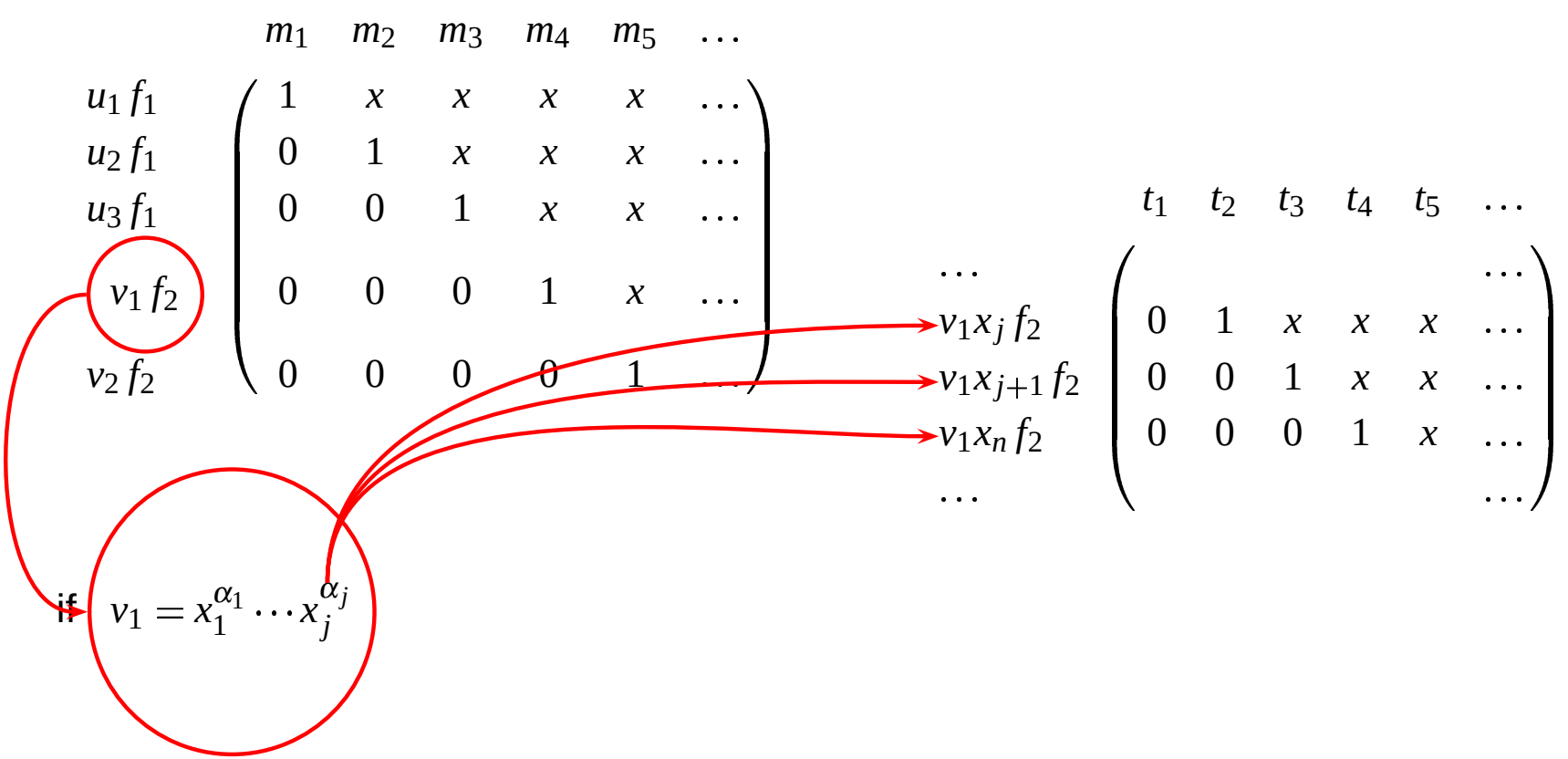
Gauss reduction:

$$
\begin{array}{c} \\ u_1 f_1 \\ u_2 f_1 \\ u_3 f_1 \\ v_1 f_2 \\ v_2 f_2 \end{array}
\begin{array}{c}
\begin{array}{ccccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \dots \end{array} \\
\begin{pmatrix}
1 & x & x & x & x & \dots \\
0 & 1 & x & x & x & \dots \\
0 & 0 & 1 & x & x & \dots \\
0 & 0 & 0 & 1 & x & \dots \\
0 & 0 & 0 & 0 & 1 & \dots
\end{pmatrix}
\end{array}
$$

$d \longrightarrow d+1$

$$
\begin{array}{c}
 \\
u_1\, f_1 \\
u_2\, f_1 \\
u_3\, f_1 \\
v_1\, f_2 \\
v_2\, f_2
\end{array}
\begin{array}{c}
\begin{array}{cccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \dots \end{array} \\
\left(\begin{array}{cccccc}
1 & x & x & x & x & \dots \\
0 & 1 & x & x & x & \dots \\
0 & 0 & 1 & x & x & \dots \\
0 & 0 & 0 & 1 & x & \dots \\
0 & 0 & 0 & 0 & 1 & \dots
\end{array} \right)
\end{array}
$$

$d \longrightarrow d+1$



$d \longrightarrow d+1$