Lecture 2-13-1 - Polynomial systems, computer algebra and applications

Jean-Charles Faugère

Regular Sequence
Algebraic Cryptanalysis of HFE (first part)
Link betwen Critical Pairs and Linear Algebra
Characterizations of Gröbner Bases
F_4
F_5

2022 - 2023 – MPRI

HFE Problem

Matsumoto, T., Imai, H.
"Public quadratic polynomial-tuples for efficient signature-verification and message-encryption".
EUROCRYPT '88.

J. Patarin.
"Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms".
EUROCRYPT '96.

Secrets:

- two $n \times n$ invertible matrices S and T with coefficients in $\mathbb{F}_2$
- sparse univariate polynomial of degree D

$$H(X) = \sum_{s \in \mathcal{S}} c_s X^s$$

where $c_s \in \mathbb{F}_{2^n}$
and $\mathcal{S} = \{2^i \mid 0 \leqslant i \text{ and } i \leqslant D\} \cup \{2^i + 2^j \mid 0 \leqslant i < j \text{ and } i + j \leqslant D\}$
Particular case: $\mathcal{S} = \{2^i + 2^j\}$ then $H(X)$ is a monomial.

Finite Field Extension

Definition (Finite Field Extension)

The field $\mathbb{F}_{p^n}$ where p prime and $n \geqslant 1$ may be explicitly constructed in the following way. One first chooses an irreducible polynomial P in $F_p[X]$ of degree n (such an irreducible polynomial always exists). Then the quotient ring $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$ of the polynomial ring $\mathbb{F}_p[X]$ by the ideal generated by P is a field of order p^n.

In our case: $p = 2$, P is of degree n any $x \in \mathbb{F}_{2^n}$ can be written $\sum_{i=0}^{n-1} x_i \omega^i$ where $x_i \in \mathbb{F}_2$ (where ω is the class of X in $\mathbb{F}_p[X]/(P)$).

Example

$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$.

HFE Problem: Public Key

We define the polynomial ring $R = \mathbb{F}_2[X_1, \ldots, X_n]$ and we substitute X by $\sum_{i=0}^{n-1} X_i \omega^i$ into the HFE polynomial $H(X)$:

$$H(\sum_{i=0}^{n-1} X_i \omega^i) = \sum_{i=0}^{n-1} H_i(X_1, \ldots, X_n) \omega^i$$

where each $H_i \in R$ is a polynomial of degree 2.
The next step is to mix the variables:

$$\begin{pmatrix} X_1 \\ \cdots \\ X_n \end{pmatrix} = T \times \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}$$

and the equations:

$$\begin{pmatrix} P_1 \\ \cdots \\ P_n \end{pmatrix} = S \times \begin{pmatrix} H_1 \\ \cdots \\ H_n \end{pmatrix}$$

HFE Public Key

$(P_1, \ldots, P_n) \in R^n$ is the Public Key.

HFE Problem: Public Key

$$\begin{pmatrix} X_1 \\ \cdots \\ X_n \end{pmatrix} = T \times \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}$$

and the equations:

$$\begin{pmatrix} P_1 \\ \cdots \\ P_n \end{pmatrix} = S \times \begin{pmatrix} H_1 \\ \cdots \\ H_n \end{pmatrix}$$

In other words, we compose S, H and T:

$$S(H(T(X))) = (P_1(x_1, \ldots, x_n), \cdots, P_n(x_1, \ldots, x_n))$$

HFE Encrypt/Verify

Encrypt

Assume that $M = (M_1, \ldots, M_n) \in \mathbb{F}_2^n$ is then message. Then

$$\begin{pmatrix} C_1 \\ \cdots \\ C_n \end{pmatrix} = \begin{pmatrix} P_1(M_1, \ldots, M_n) \\ \cdots \\ P_n(M_1, \ldots, M_n) \end{pmatrix}$$

is the ciphertext.

This operation is very fast since it is just the evaluation of quadratic polynomials.

Exercice

This operation can be done with linear algebra. Why ?

HFE Decrypt/Sign

Decrypt

Assume that $C = (C_1, \ldots, C_n) \in \mathbb{F}_2^n$ is then ciphertext.
To decrypt the ciphertext C, we first find all solutions Z to the univariate equation

$$H(Z) = S^{-1}C,$$

next we compute $T^{-1}Z$ to recover the original message.

Hence we have to solve a degree D univariate equation.
Find the roots of a polynomial of degree F with coefficients in $\mathbb{F}_{2^n}$ can be done (see [5] for instance) in $\mathcal{O}(\mathbf{M}(d)\log(d))$ operations in $\mathbb{F}_{2^n}$ where $\mathbf{M}(d)$ is the cost of polynomial multiplication.
In practice, we cannot take arbitrarily big value for the degree of the univariate polynomial (say $d \leqslant 1024$).

HFE Challenge

For instance: $n = 80$, $d = 96$ for the first HFE Challenge.

Algebraic Attack

The direct attack is obvious: given $(M_1, \ldots, M_n)$ we have to solve the following polynomials system:

$$\begin{cases} P_1(x_1, \ldots, x_n) = M_1 \\ \qquad\qquad \ldots \\ P_n(x_1, \ldots, x_n) = M_n \end{cases}$$

Algebraic Attack

$(M_1, \ldots, M_n)$ is given.
More precisely since the solutions are to be found in $\mathbb{F}_2$ we have to solve the following system:

$$\begin{cases} P_1(x_1, \ldots, x_n) = M_1 \\ \qquad \ldots \\ P_n(x_1, \ldots, x_n) = M_n \\ x_1^2 - x_1 \\ \quad \ldots \\ x_n^2 - x_n \end{cases}$$

Question

What is the complexity of solving the algebraic system?
What is the complexity of computing the Gröbner basis.

Simple Estimation of the Complexity

From a complexity point of view the two important parameters are: d the maximal degree occurring in the computation and the size N_d of the Macaulay matrix in degree d.
Then the whole complexity is simply N_d^ω where $2 \leqslant \omega \leqslant 3$ is the cost of linear algebra.
Since we add the field equations $x_i^2 - x_i$ it means that all the monomials are squarefree, so that

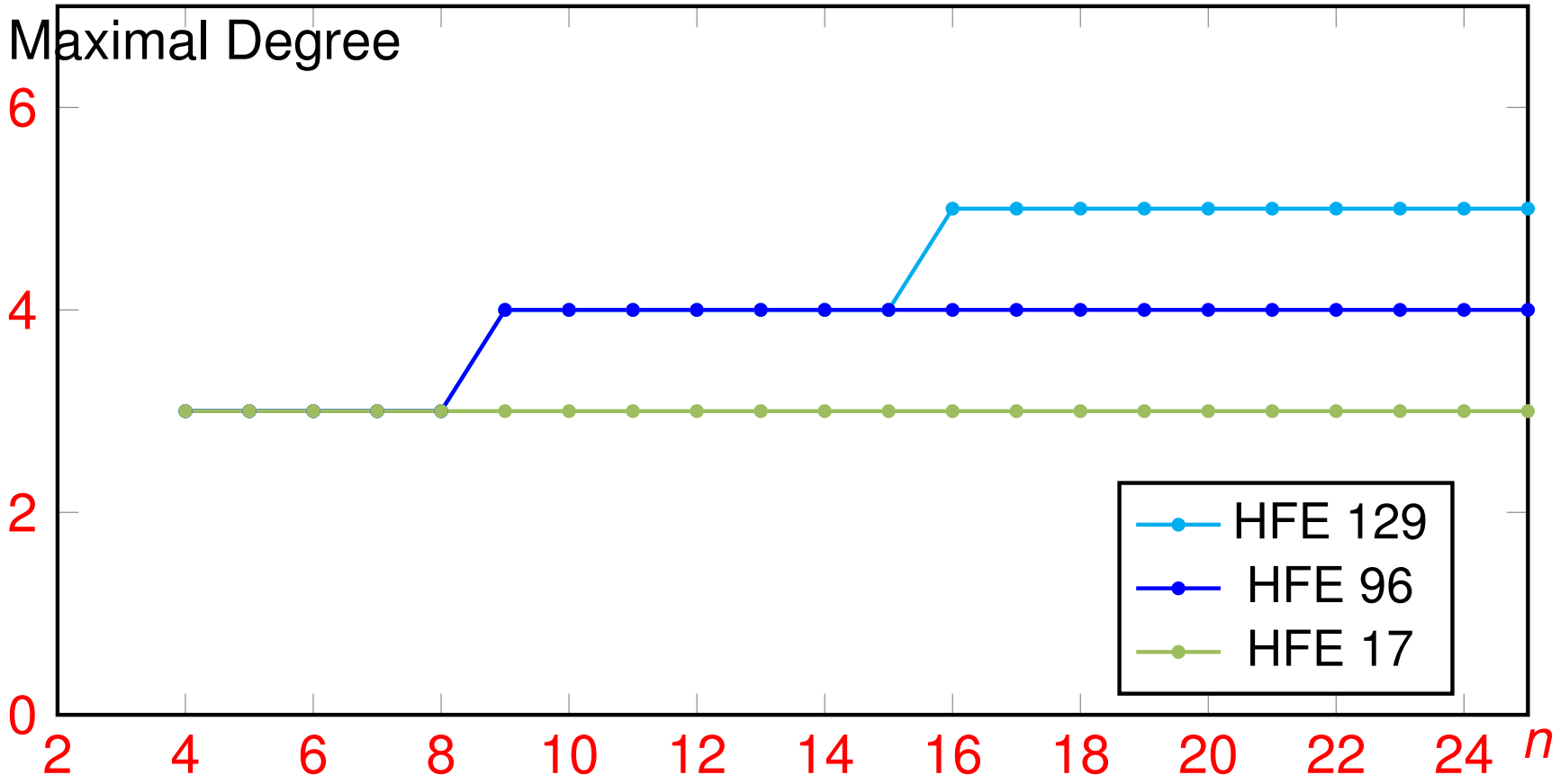
$$N_d = \binom{n}{d}$$

Hence, the main goal is to estimate d.
We begin by running some experiments.

Experimental Complexity

D	16	17	33	96	128	129	257	384	512	513
Max degree	3	4	4	4	4	5	5	5	5	6

Relation between *D* and the maximal degree.

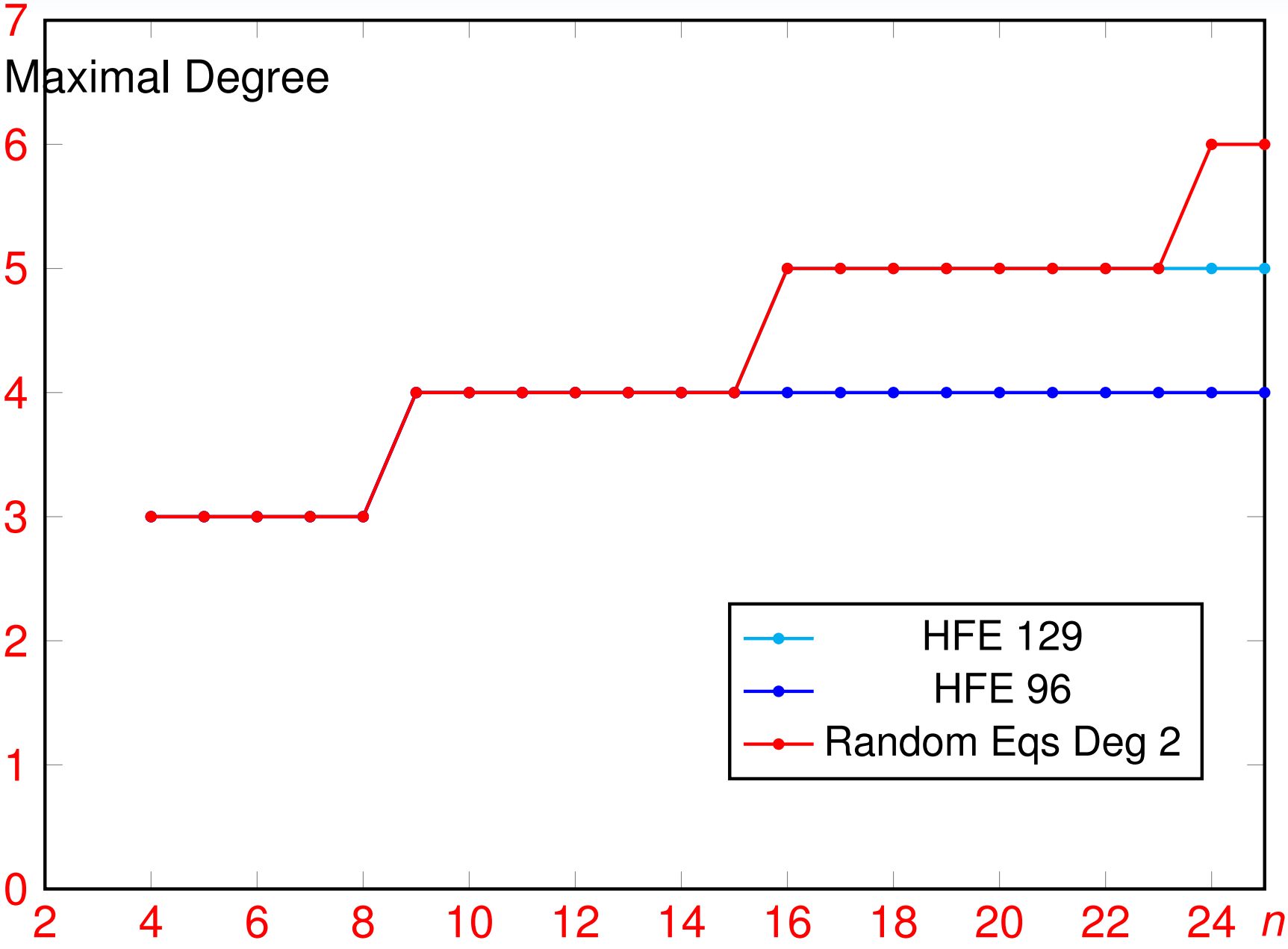


Experimental Complexity

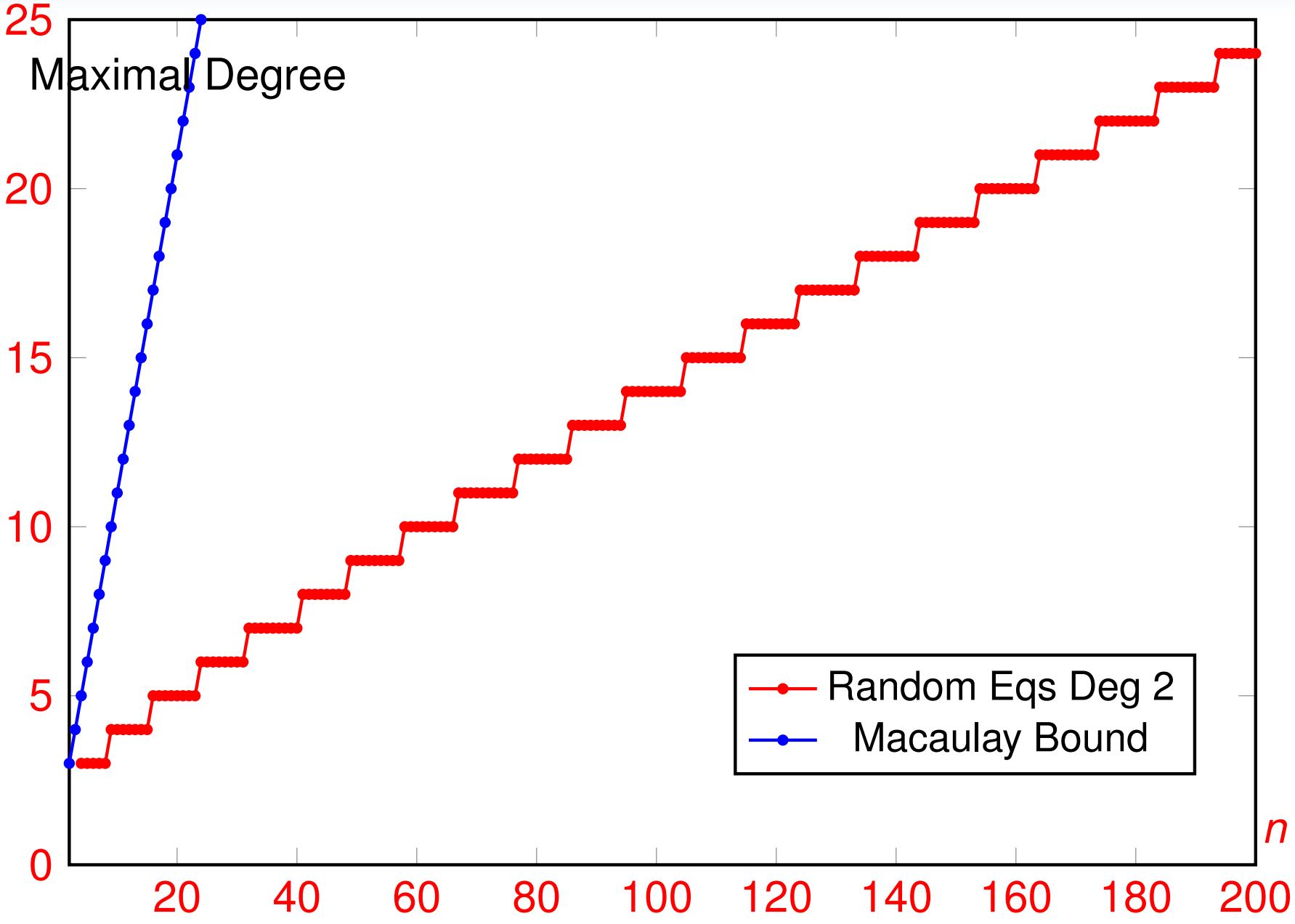
n	14	15	16	17	23	24	25
degree	4	4	5	5	5	6	6
nb of rows	1695	1379	8840	11424	40480	223124	278875

Maximal degree occurring in Gröbner for *random* systems.

Experimental Complexity



Complexity


25
20
15
10
5
0
Maximal Degree
Random Eqs Deg 2
Macaulay Bound
20
40
60
80
100
120
140
160
180
200
n

F_4

F_4

Matrix representation of polynomials

Definition

If $F = [f_1, \ldots, f_m]$ is a vector of m polynomials and $<$ an admissible ordering, $\mathrm{T}_<(F) = [t_1, \ldots, t_l]$ the monomials in the support of F sorted for $<$. The matrix representation of $M_{T_<(F)}(F)$ wrt F is:

$$M(F) = \begin{array}{c|ccc} & t_1 & t_2 & t_3 \\ f_1 & \cdots & \cdots & \cdots \\ f_2 & \cdots & \cdots & \cdots \\ f_3 & \cdots & \cdots & \cdots \end{array}$$

$$M(F)_{f_i,t_j} = \mathrm{coeff}\left(f_i, t_j\right)$$

Moreover, $M(F)$ satisfies the following equation:

$$F = M(F) \cdot T_<(F)$$

Polynomial representation of a matrix

Definition

If M is a matrix of size $l \times m$ with coefficients in $\mathbb{K}$ and $X = [t_1, \ldots, t_m]$ is a vector of terms, then the polynomial representation of M wrt X is the vector of l polynomials given by:

$$F = M \cdot X$$

Example (Cyclic 4 Problem)

The monomial ordering is DRL

$$F = \left[\begin{array}{c} f_1 = abcd - 1, f_2 = abc + abd + acd + bcd, \\ f_3 = ab + bc + ad + cd, f_4 = a + b + c + d \end{array} \right]$$

The matrix representation of $F_1 = [f_3, bf_4, df_4]$ is:

$$A_1 = M(F_1) = \begin{array}{c|ccccccc} & ab & b^2 & bc & ad & bd & cd & d^2 \\ df_4 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ f_3 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ bf_4 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array}$$

Example (Cyclic 4 Problem)

The monomial ordering is DRL

$$F = \left[\begin{array}{c} f_1 = abcd - 1, f_2 = abc + abd + acd + bcd, \\ f_3 = ab + bc + ad + cd, f_4 = a + b + c + d \end{array} \right]$$

The matrix representation of $F_1 = [f_3, bf_4, df_4]$ is:

$$A_1 = M(F_1) = \begin{array}{c|ccccccc|} & ab & b^2 & bc & ad & bd & cd & d^2 \\ df_4 & & & & 1 & 1 & 1 & 1 \\ f_3 & 1 & & 1 & 1 & & 1 & \\ bf_4 & 1 & 1 & 1 & & 1 & & \end{array}$$

Macaulay matrix

Definition (Macaulay matrix [?])

Let $F = [f_1, \ldots, f_m]$ a vector of m polynomials and d a non negative integer then the Macaulay matrix in degree d of F $\mathcal{M}_d^{\text{acaulay}}(F)$, is the matrix representation of

$$F^{(d)} = \left[t_j \cdot f_i \mid 1 \leqslant i \leqslant m \text{ and } t_j \in T \text{ with } \deg(t_j) \leqslant d - \deg(f_i) \right]$$

$$\mathcal{M}_d^{\text{acaulay}}(F) = M(F^{(d)}) = \begin{array}{c|ccc} & m_1 & m_2 & m_3 \\ t_1 f_1 & \cdots & \cdots & \cdots \\ t_2 f_2 & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{array}$$

Echelon form of a matrix

The basis operation is to compute a row echelon form of matrix; this will be the most costly operation.

Definition

If $M(F)$ is the matrix representation of a vector of polynomials F we denote by $\widetilde{M(F)}$ the Gaussian elimination of $M(F)$ (without pivoting the columns of the matrix).

We extend this definition to polynomials:

Definition

Let $F \subset \mathbb{K}[x_1, \ldots, x_n]$ and $<$ a monomial ordering. We denote by $\tilde{F}$ the polynomial representation of $\widetilde{M(F)}$. We say that $\tilde{F}$ is the echelon form of F (or a Gaussiant elimination) wrt $<$.

Example

The matrix representation of $F_1 = [f_3, bf_4, df_4]$ is:

$$A_1 = M(F_1) = \begin{array}{c|ccccccc} & ab & b^2 & bc & ad & bd & cd & d^2 \\ df_4 & & & & 1 & 1 & 1 & 1 \\ f_3 & 1 & & 1 & 1 & & 1 & \\ bf_4 & 1 & 1 & 1 & & 1 & & \end{array}$$

Example

The matrix representation of $F_1 = [f_3, bf_4, df_4]$ is:

$$\tilde{A}_1 = \begin{array}{c|ccccccc} & ab & b^2 & bc & ad & bd & cd & d^2 \\ df_4 & & & & 1 & 1 & 1 & 1 \\ f_3 & 1 & & 1 & & -1 & & -1 \\ bf_4 & & 1 & & & 2 & & 1 \end{array}$$

Example

The polynomial representation of:

$$\tilde{A}_1 = \begin{array}{c} \\ df_4 \\ f_3 \\ bf_4 \end{array} \begin{array}{c} \begin{array}{ccccccc} ab & b^2 & bc & ad & bd & cd & d^2 \end{array} \\ \left| \begin{array}{ccccccc} & & & 1 & 1 & 1 & 1 \\ 1 & & 1 & & -1 & & -1 \\ & 1 & & & 2 & & 1 \end{array} \right| \end{array}$$

$$\tilde{F}_1 = \begin{bmatrix} f_5 = ad + bd + cd + d^2, \\ f_6 = ab + bc - bd - d^2, \\ f_7 = b^2 + 2\,bd + d^2 \end{bmatrix}$$

Macaulay method

The idea of using linear algebra to solve polynomial systems date back to Macaulay.
Macaulay matrix is a generalization of the Sylvester matrix [**?**] (the matrix involved in the computation of the resultant of 2 polynomials).

The link between the computation of a truncated d-Gröbner basis is given by the following theorem of Lazard:

Theorem (Lazard)

If $\widetilde{F = \{f_1, \ldots, f_m\}}$ *is a set of homogeneous polynomials then* $\mathcal{M}_d^{\widetilde{\text{acaulay}}}(F)$ *is a (non reducible)* d*-Gröbner basis of* F*.*
If $\widetilde{F = \{f_1, \ldots, f_m\}}$ *is a set of polynomials, then there exists* $d > 0$ *such that* $\mathcal{M}_d^{\widetilde{\text{acaulay}}}(F)$ *is a Gröbner basis of* F*.*

Macaulay bound

Theorem (Macaulay bound)

Let $F = \{f_1, \ldots, f_m\}$ is a set of homogeneous polynomials which is a regular sequence. We define

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

then $\widetilde{\mathcal{M}_D^{\text{acaulay}}(F)}$ is a (non reduced) Gröbner basis of F.

Regular sequence I

We consider the Macaulay matrix of $F = [f_1, \ldots, f_m]$.
If the Macaulay matrix is singular $\longleftrightarrow$ the rows of the matrix are not independent.
Moreover, each row of the matrix is a product $t \times f$ where t is a term and $f \in F$; the linear dependence can be expressed by $\sum_{f \in F, t \in T} \lambda_{t,f}\ t\, f = 0$ or equivalently by grouping terms:

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

where g_i are polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. We say that $(g_1, \ldots, g_m)$ is a syzygy. The relation (5) can be rewritten:

$$g_1 f_1 = 0 \text{ modulo } \mathrm{Id}(f_2, \ldots, f_m) \tag{2}$$

in other words it is a **zero divisor** $(\textit{if}\ g_1 \neq 0)$.

Regular sequence II

A linear system is non singular if one cannot find a non zero linear combination:

$$\sum_{i=1}^{m} \lambda_i f_i = 0 \text{ with } \lambda_i \in \mathbb{K} \tag{3}$$

For algebraic systems: it is not possible to avoid non zero relations (5) :

$$f_i f_j - f_j f_i = 0 \tag{4}$$

We say that it is a trivial syzygy.

Regular sequence I

We consider the Macaulay matrix of $F = [f_1, \ldots, f_m]$.
If the Macaulay matrix is singular $\longleftrightarrow$ lthe rows of the matrix are not independent.
Moreover, each row of the matrix is a product $t \times f$ where t is a term and $f \in F$; the linear dependence can be expressed by $\sum_{f \in F, t \in T} \lambda_{t,f}\ t\, f = 0$ or equivalently by grouping terms:

$$\sum_{i=1}^{m} g_i f_i = 0 \tag{5}$$

where g_i are polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. We say that $(g_1, \ldots, g_m)$ is a syzygy. The relation (5) can be rewritten:

$$g_1 f_1 = 0 \text{ modulo } \mathrm{Id}(f_2, \ldots, f_m) \tag{6}$$

in other words it is a **zero divisor** $(\textit{if}\ g_1 \neq 0)$.

Regular sequence II

A linear system is non singular if one cannot find a non zero linear combination:

$$\sum_{i=1}^{m} \lambda_i f_i = 0 \text{ with } \lambda_i \in \mathbb{K} \tag{7}$$

For algebraic systems: it is not possible to avoid non zero relations (5) :

$$f_i f_j - f_j f_i = 0 \tag{8}$$

We say that it is a trivial syzygy.

Regular sequence III

Definition (Regular Sequence

Algebraic definition: the system $(f_1, \ldots, f_m)$ of homogeneous polynomials is **regular** if for all $i = 1, \ldots, m$ and g such that

$$g \cdot f_i \in \langle f_1, \ldots, f_{i-1} \rangle$$

then g is also in $\langle f_1, \ldots, f_{i-1} \rangle$.

Geometric definition: the system$(f_1, \ldots, f_m)$ of homogeneous polynomials is **regular** if for all $i \in \{1, \ldots, m\}$, the dimension of $\langle f_1, \ldots, f_i \rangle$ is $n - i$.
We say that the sequence $(f_1, \ldots, f_m)$ is regular.
The sequence $(f_1, \ldots, f_m)$ of affine polynomials is regular if the sequence $(f_1^h, \ldots, f_m^h)$ is regular (f_i^h is the highest homogeneous par of f_i).

Regular sequence IV

Remark

Another characterization of regular sequences: there is no relation

$$\sum_i g_i \cdot f_i = 0 \text{ with } g_i \in \mathbb{K}[x_1, \ldots, x_n]$$

except the relations induced by the trivial syzygies $f_i f_j = f_j f_i$.

Remark

From the geometric definition: there is no regular sequence when $m > n$.

Link betwen Critical Pairs and Linear Algebra Characterizations of Gröbner Bases

Characterizations of Gröbner Bases

Useful characterizations of Gröbner bases.

Definition (t-representation)

Let $P = [p_1, \ldots, p_k]$ be a finite subset of $\mathbb{K}[x_1, \ldots, x_n]$, $0 \neq f \in \mathbb{K}[x_1, \ldots, x_n]$, and $t \in T$. Assume that there exists $(g_1, \ldots, g_k) \in \mathbb{K}[x_1, \ldots, x_n]^k$ such that:

$$f = \sum_{i=1}^{k} g_i \, p_i$$

We say that it is a $t-$*representation* of f wrt P if $t \geqslant \mathrm{LT}(g_i p_i)$ for all $1 \leqslant i \leqslant k$. We denote by $f = O_P(t)$ this property.
We note $f = o_P(t)$ when there exists $t' \in T$ such that $t' < t$ and $f = O_P(t')$.

Characterizations of Gröbner Bases

Proposition

If f, g are polynomials and , t is a term, P a finite subset of polynomials, then

$$\begin{array}{llll} f = O_P(t) & g = O_P(t) & \text{implies} & f + g = O_P(t) \\ f = o_P(t) & g = o_P(t) & \text{implies} & f + g = o_P(t) \\ f = O_P(t) & u \in T & \text{implies} & u\ f = O_P(u\,t) \\ f = o_P(t) & u \in T & \text{implies} & u\,f = o_P(u\,t) \end{array}$$

Proposition (R)

If $\textsc{Reduction}(p, P) = 0$ *or* $p \xrightarrow[P]{*} 0$ *then* $p = O_P(\mathrm{LT}(p))$.

Proof.

Easy exercise. □

Characterizations of Gröbner Bases

When $f = O_G(\mathrm{LT}(f))$ we say that f has a standard representation wrt G.

Theorem

G is a Gröbner basis if and only if $\forall 0 \neq f \in \mathrm{Id}(G)$, $f = O_G(\mathrm{LT}(f))$.

Proof.

Exercice. □

and what happen when

$$f \neq O_G(\mathrm{LT}(f)) \ ?$$

Cancellation

$$f \in I = \mathrm{Id}\,(f_1, \cdots, f_m)$$

By definition:

$$f = g_1 f_1 + \cdots + g_m f_m$$

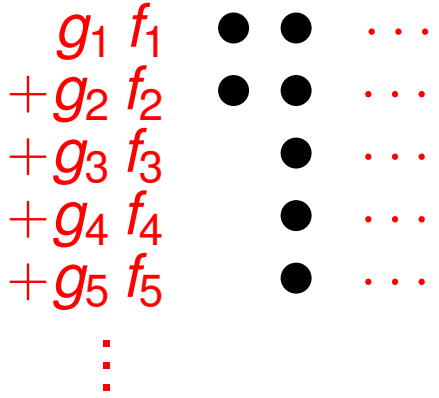
Cancellation

$$f \in I = \mathrm{Id}\,(f_1, \cdots, f_m)$$

By definition:

$$f = g_1 f_1 + \cdots + g_m f_m$$

Not a unique representation !



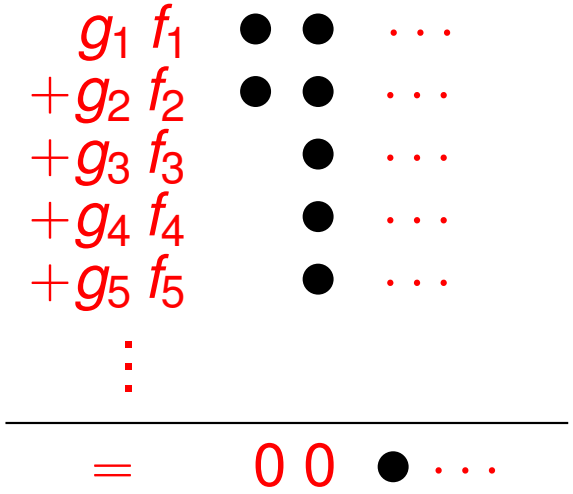
Cancellation

$$f \in I = \mathrm{Id}\,(f_1, \cdots, f_m)$$

By definition:

$$f = g_1 f_1 + \cdots + g_m f_m$$

Not a unique representation !



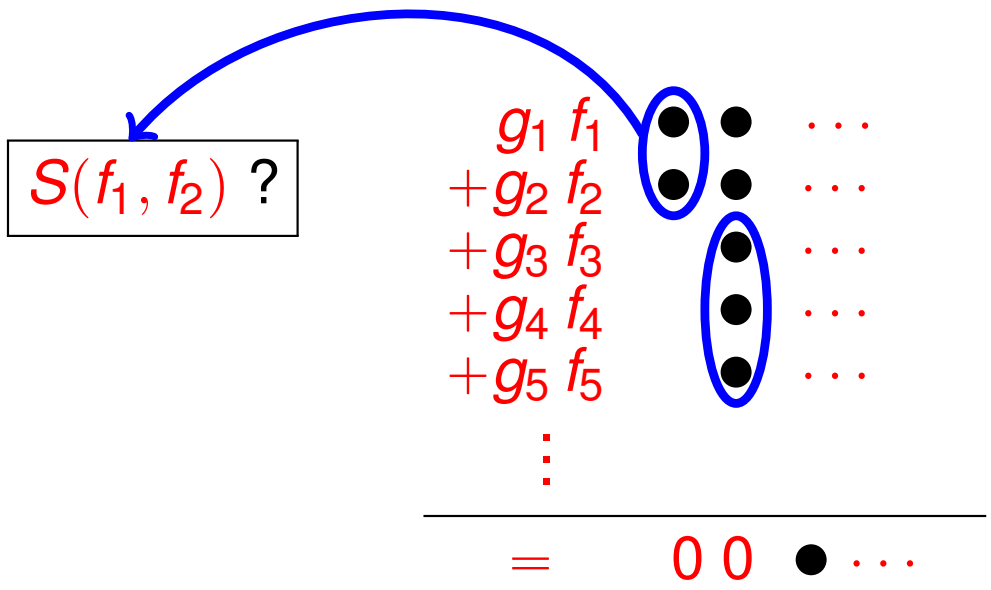
Cancellation

$$f \in I = \mathrm{Id}\,(f_1, \cdots, f_m)$$

By definition:

$$f = g_1 f_1 + \cdots + g_m f_m$$

Not a unique representation !



Characterizations of Gröbner Bases

Theorem

G is a Gröbner basis if and only if $\forall 0 \neq f \in \mathrm{Id}(G)$, $f = O_G(\mathrm{LT}(f))$.

Theorem

Let G be a finite subset of polynomials. If for all g_1, g_2 in G, we have $\mathrm{Spol}(g_1, g_2) = 0$ or $\mathrm{Spol}(g_1, g_2) = o_G(\mathrm{lcm}(g_1, g_2))$, then G is a Gröbner basis.

Proof.

We need to proof a lemma first . . . □

Proof of the theorem: lemma

Lemma

Let $f_1, \ldots, f_k$ *be nonzero polynomials in* $\mathbb{K}[x_1, \ldots, x_n]$ *and* $t \in T$. *Consider* $f = O_P(t) = \Sigma_{i=1}^{k} c_i \mathbf{x}^{\alpha_i} f_i$, *where* $c_i \in \mathbb{K}^*$ *such that*

$$t = \mathbf{x}^{\alpha_1} LT(f_1) = \cdots = \mathbf{x}^{\alpha_k} LT(f_k).$$

If $LT(f) < t$, *then* $k > 1$ *and* f *can be rewritten:*

$$f = \sum_{i=1}^{k-1} b_i \frac{t}{\tau_i} \operatorname{Spol}(f_i, f_{i+1}) \text{ with } b_i \in \mathbb{K}, \tag{9}$$

where $\tau_i = lcm(f_i, f_{i+1})$. *Furthermore*

$$\frac{t}{\tau_i} LT(\operatorname{Spol}(f_i, f_{i+1})) < t, \text{ for all } i = 1, \ldots, k-1.$$

Characterizations of Gröbner Bases

Corollary (Buchberger)

Let G be a finite subset of polynomials . G is a Gröbner basis if and only if $\mathrm{Spol}(f,g) \xrightarrow{*} 0$ for all $(f,g) \in G^2$.

Corollary (Buchberger)

Let G be a finite subset of polynomials . G is a Gröbner basis if and only if REDUCTION$(\mathrm{Spol}(f,g), G) = 0$ *for all $(f,g) \in G^2$.*

Proof.

Let $(f,g) \in G^2$, $f \neq g$. Put $t = \mathrm{LT}(\mathrm{Spol}(f,g)) < \mathrm{lcm}(f,g)$
If REDUCTION$(\mathrm{Spol}(f,g), G) = 0$ then from proposition (R) :
$\mathrm{Spol}(f,g) = O_G(\mathrm{LT}(\mathrm{Spol}(f,g))) = O_G(t) = o_G(\mathrm{lcm}(f,g))$and we can apply the theorem. □

Buchberger Algorithm

Very simple version of the **Buchberger** algorithm:

Algorithm (Buchberger)

Input: $\begin{cases} F = [f_1, \ldots, f_s] \text{ a list of polynomials} \\ < \text{ admissible ordering} \end{cases}$

Output: G a finite subset of $\mathbb{K}[x_1, \ldots, x_n]$.

$G := F$ and $m := s$

$P := \{(f_i, f_j) \mid 1 \leqslant i < j \leqslant m\}$ *the list of critical pairs*

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

  Select and remove from P a critical pair (f, g)

  $f_{m+1} := \mathrm{Spol}(f, g)$

  $f_{m+1} :=$ REDUCTION(f_{m+1}, G)

  if $f_{m+1} \neq 0$ **then**

    $m := m + 1$

    $P := P \cup \{(f_i, f_m) \mid 1 \leqslant i < m\}$

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

return G

F_4

F_4

The F_4 algorithm

Definition

A critical pairs of (f_i, f_j) is a member of $T^2 \times \mathbb{K}[x_1, \ldots, x_n] \times T \times \mathbb{K}[x_1, \ldots, x_n]$,

$$\mathrm{Pair}(f_i, f_j) := (\mathrm{lcm}_{ij}, t_i, f_i, t_j, f_j)$$

such that

$$\mathrm{lcm}(\mathrm{Pair}(f_i, f_j)) = \mathrm{lcm}_{ij} = \mathrm{LT}(t_i f_i) = \mathrm{LT}(t_j f_j) = \mathrm{lcm}(f_i, f_j)$$

Definition

We define the degree of the critical pair $p_{i,j} = \mathrm{Pair}(f_i, f_j)$, $\deg(p_{i,j})$, to be $\deg(lcm_{i,j})$. We define the following operators:

$$\mathrm{Left}(p_{i,j}) := t_i \cdot f_i \;\; et \;\; \mathrm{Right}(p_{i,j}) := t_j \cdot f_j$$

Algorithm F_4 [?] (simplified version)

Input: $\begin{cases} F \text{ is a finite subset of } \mathbb{K}[x_1, \ldots, x_n] \\ \mathcal{S}el \text{ is a function } List(Pairs) \to List(Pairs) \\ \qquad \text{such that } \mathcal{S}el(l) \neq \emptyset \text{ if } l \neq \emptyset \end{cases}$

Output: un sous ensemble fini de $\mathbb{K}[x_1, \ldots, x_n]$.

$G := F$, $\tilde{F_0^+} := F$, $d := 0$ and $P := \{\mathrm{Pair}(f, g) \mid (f, g) \in G^2 \text{ with } f \neq g\}$

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

$d := d + 1$

$P_d := \mathcal{S}el(P)$

$P := P \backslash P_d$

$L_d := \mathrm{Left}(P_d) \cup \mathrm{Right}(P_d)$

$\tilde{F_d^+} :=$ REDUCTION(L_d, G)

for $h \in \tilde{F_d^+}$ **do**

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

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

return G

We can now extend the definition of reduction of a polynomial modulo a subset of$\mathbb{K}[x_1, \ldots, x_n]$, to the reduction of a subset of $\mathbb{K}[x_1, \ldots, x_n]$ modulo another subset of $\mathbb{K}[x_1, \ldots, x_n]$:

Algorithm REDUCTION

Input: L, G finite subsets of $\mathbb{K}[x_1, \ldots, x_n]$
Output: a finite subset of $\mathbb{K}[x_1, \ldots, x_n]$ (could be empty).
$F :=$SYMBOLICPREPROCESSING(L, G)
$\tilde{F} :=$ Gaussian reduction of F wrt $<$
$\tilde{F}^+ := \left\{ f \in \tilde{F} \mid \mathrm{LT}(f) \notin \mathrm{LT}(F) \right\}$ // *the "useful" part of* $\tilde{F}$
return $\tilde{F}^+$

No arithmetic operation is used: it is a symbolic preprocessing.

Algorithm SymbolicPreprocessing

Input: L, G finite subsets of $\mathbb{K}[x_1, \ldots, x_n]$
Output: a finite subset of $\mathbb{K}[x_1, \ldots, x_n]$
$F := L$
$Done := \mathrm{LT}(F)$
while $\mathrm{T}(F) \neq Done$ **do**
    choose m an element of $\mathrm{T}(F) \backslash Done$
    $Done := Done \cup \{m\}$
    if m top réductible modulo G **then**
        exists $g \in G$ and $m' \in T$ such that $m = m' \cdot \mathrm{LT}(g)$
        $F := F \cup \{m' \cdot g\}$
return F

The SymbolicPreprocessing function is very efficient: its complexity is proportional to the size of the output (if $\#G$ is smaller than the final size of $T(F)$) [parallel implementation].

Lemma (1)

For all polynomials $p \in L_d$,we have $p \xrightarrow{G \cup \tilde{F^+}} 0$

Theorem

The F_4 algorithm computes a Gröbner basis of G in $\mathbb{K}[x_1, \ldots, x_n]$ such that $F \subseteq G$ and $Id(G) = Id(F)$.

Proof.

. . . □

Remark

If $\#Sel(l) = 1$ for all $l \neq \emptyset$ then the F_4 algorithm reduces to the Buchberger algorithm. In this case the function Sel is the equivalent of the selection strategy for the Buchberger algorithm.

Selection function

Algorithm Selection

Input: P a list of critical pairs
Output: a list of critical pairs.
$d := \min\{\deg(\mathrm{lcm}(p)) \mid p \in P\}$
$P_d := \{p \in P \mid \deg(\mathrm{lcm}(p)) = d\}$
return P_d

We call this strategy *the normal strategy for* F_4.
Hence, if the input polynomials are homogeneous, we obtain in degree d, a d Gröbner basis; $\mathcal{S}el$ selects, in the next step, all the critical pairs which are needed to compute the Gröbner basis in degree $d+1$.

Optimisations

- including Buchberger Criteria (or F_5 criterion).
- reuse **all** the rows in the reduced matrices.

Algorithm Buchberger Criteria - Implementation

$(G_{new}, P_{new}) :=$ UPDATE(G_{old}, P_{old}, h)

Input:
- a finite subset G_{old} of $\mathbb{K}[x_1, \ldots, x_n]$
- a finite subset P_{old} of critical pairs in $\mathbb{K}[x_1, \ldots, x_n]$
- $0 \neq h \in \mathbb{K}[x_1, \ldots, x_n]$

Output: a finite subset in $\mathbb{K}[x_1, \ldots, x_n]$ an updated list of critical pairs.

Algorithm F_4 algorithm (with Criteria)

Input: $\begin{cases} F \subset \mathbb{K}[x_1, \ldots, x_n] \\ \mathcal{S}el \text{ a function } \mathrm{List}(Pairs) \to \mathrm{List}(Pairs) \end{cases}$

Output: a finite subset of $\mathbb{K}[x_1, \ldots, x_n]$.

$G := \emptyset$ and$P := \emptyset$ and $d := 0$

while $F \neq \emptyset$ **do**

$f := \mathrm{first}(F)$; $F := F \backslash \{f\}$

$(G, P) :=$UPDATE(G, P, f)

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

$d := d + 1$

$P_d := \mathcal{S}el(P)$; $P := P \backslash P_d$

$L_d := \mathrm{Left}(P_d) \cup \mathrm{Right}(P_d)$

$(\tilde{F_d^+}, F_d) :=$REDUCTION$(L_d, G, (F_i)_{d=1,\ldots,(d-1)})$

for $h \in \tilde{F_d^+}$ **do**

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

$(G, P) :=$UPDATE(G, P, h)

return G

F4: step by step

Example (3 quadratic equation in $\mathbb{F}_{101}$)

Monomial ordering is DRL and the normal strategy

$$F = \left[\begin{array}{l} f_1 = {x_1}^2 + 66\,x_1\,x_2 + 4\,x_1\,x_3 + 25\,{x_2}^2 + 41\,x_2\,x_3 + 54\,{x_3}^2 + 42\,x_1 \\ \quad +87\,x_2 + 22\,x_3 + 86, \\ f_2 = {x_1}^2 + 22\,x_1\,x_2 + 38\,x_1\,x_3 + 9\,{x_2}^2 + 53\,x_2\,x_3 + 6\,{x_3}^2 + 92\,x_1 \\ \quad +61\,x_2 + 74\,x_3 + 49, \\ f_3 = {x_1}^2 + 13\,x_1\,x_2 + 86\,x_1\,x_3 + 29\,{x_2}^2 + 11\,x_2\,x_3 + 81\,{x_3}^2 + 98\,x_1 \\ \quad +67\,x_2 + 7\,x_3 + 40 \end{array} \right.$$

At the beginning $G = \{f_1\}$ and $P_1 = \{\mathrm{Pair}(f_2, f_3), \mathrm{Pair}(f_1, f_2)\}$ such that $L_1 = \{(1, f_3), (1, f_2), (1, f_1)\}$.

SymbolicPreprocessing$(L_1, G, \varnothing)$:

$F_1 = \{f_3, f_2, f_1\}$ $\quad T(F_1) = \{\boxed{x_1^2}, x_1x_2, x_1x_3, x_2^2, x_2x_3, x_3^2, x_1, x_2, x_3, 1\}$

$\boxed{x_1^2}$ is already done. All the other monomials are not reducible.

F4: step by step

Example (3 quadratic equation in $\mathbb{F}_{101}$)

At the beginning $G = \{f_1\}$ and $P_2 = \{\mathrm{Pair}(f_2, f_3), \mathrm{Pair}(f_1, f_2)\}$ such that $L_2 = \{(1, f_3), (1, f_2), (1, f_1)\}$.

SymbolicPreprocessing$(L_2, G, \varnothing)$:

$$F_2 = \{f_3, f_2, f_1\} \quad T(F_2) = \{\boxed{x_1^2}, x_1x_2, x_1x_3, x_2^2, x_2x_3, x_3^2, x_1, x_2, x_3, 1\}$$

$\boxed{x_1^2}$ is already done. All the other monomials are not reducible.

Matrix representation of $F_1 = [f_3, f_2, f_1]$ is:

$$A_1 = M(F_1) = \begin{array}{c|cccccc|c} & x_1^2 & x_1x_2 & x_2^2 & x_1x_3 & x_2x_3 & x_3^2 & \cdots \\ f_3 & 1 & 13 & 29 & 86 & 11 & 81 & \cdots \\ f_2 & 1 & 22 & 26 & 38 & 53 & 6 & \cdots \\ f_1 & 1 & 66 & 25 & 4 & 41 & 54 & \cdots \end{array}$$

F4: step by step

Example (3 quadratic equation in $\mathbb{F}_{101}$)

At the beginning $G = \{f_1\}$ and $P_2 = \{\mathrm{Pair}(f_2, f_3), \mathrm{Pair}(f_1, f_2)\}$ such that $L_2 = \{(1, f_3), (1, f_2), (1, f_1)\}$.

SymbolicPreprocessing$(L_2, G, \varnothing)$:

$$F_2 = \{f_3, f_2, f_1\} \quad T(F_2) = \{\boxed{x_1^2}, x_1x_2, x_1x_3, x_2^2, x_2x_3, x_3^2, x_1, x_2, x_3, 1\}$$

$\boxed{x_1^2}$ is already done. All the other monomials are not reducible.

$$\widetilde{A_2} = \begin{array}{c|cccccc|c} & x_1^2 & x_1x_2 & x_2^2 & x_1x_3 & x_2x_3 & x_3^2 & \cdots \\ f_6 & 0 & 0 & 1 & 28 & 19 & 79 & \cdots \\ f_5 & 0 & 1 & 0 & 12 & 2 & 5 & \cdots \\ f_1 & 1 & 66 & 4 & 25 & 41 & 54 & \cdots \end{array}$$

F4: step by step

Example (3 quadratic equation in $\mathbb{F}_{101}$)

At the beginning $G = \{f_1\}$ and $P_2 = \{\mathrm{Pair}(f_2, f_3), \mathrm{Pair}(f_1, f_2)\}$ such that $L_2 = \{(1, f_3), (1, f_2), (1, f_1)\}$.

SymbolicPreprocessing$(L_2, G, \varnothing)$:

$$F_2 = \{f_3, f_2, f_1\} \quad T(F_2) = \{\boxed{x_1^2}, x_1x_2, x_1x_3, x_2^2, x_2x_3, x_3^2, x_1, x_2, x_3, 1\}$$

$\boxed{x_1^2}$ is already done. All the other monomials are not reducible.

$$\widetilde{A_2} = \begin{array}{c|cccccc|c} & x_1^2 & x_1x_2 & x_2^2 & x_1x_3 & x_2x_3 & x_3^2 & \cdots \\ f_6 & 0 & 0 & 1 & 28 & 19 & 79 & \cdots \\ f_5 & 0 & 1 & 0 & 12 & 2 & 5 & \cdots \\ f_1 & 1 & 66 & 4 & 25 & 41 & 54 & \cdots \end{array}$$

Polynomial representation of $\widetilde{A_2}$:

F4: step by step

Example (3 quadratic equation in $\mathbb{F}_{101}$)

At the beginning $G = \{f_1\}$ and $P_2 = \{\mathrm{Pair}(f_2, f_3), \mathrm{Pair}(f_1, f_2)\}$ such that $L_2 = \{(1, f_3), (1, f_2), (1, f_1)\}$.

SymbolicPreprocessing$(L_2, G, \varnothing)$:

$F_2 = \{f_3, f_2, f_1\} \quad T(F_2) = \{\boxed{x_1^2}, x_1x_2, x_1x_3, x_2^2, x_2x_3, x_3^2, x_1, x_2, x_3, 1\}$

$\boxed{x_1^2}$ is already done. All the other monomials are not reducible.

$$\widetilde{A_2} = \begin{array}{c|cccccc|c} & x_1^2 & x_1x_2 & x_2^2 & x_1x_3 & x_2x_3 & x_3^2 & \cdots \\ f_6 & 0 & 0 & 1 & 28 & 19 & 79 & \cdots \\ f_5 & 0 & 1 & 0 & 12 & 2 & 5 & \cdots \\ f_1 & 1 & 66 & 4 & 25 & 41 & 54 & \cdots \end{array}$$

Polynomial representation of $\widetilde{A_2}$:

$f_5 = x_1\,x_2 + 12\,x_1\,x_3 + 2\,x_2\,x_3 + 55\,{x_3}^2 + 66\,x_1 + 88\,x_2 + 60\,x_3 + 92,$
$f_6 = {x_2}^2 + 28\,x_1\,x_3 + 19\,x_2\,x_3 + 79\,{x_3}^2 + 30\,x_1 + 50\,x_2 + 59\,x_3 + 46$

F4: step by step

Example (3 quadratic equation in $\mathbb{F}_{101}$)

In degree 3: $P_3 = \{\mathrm{Pair}(f_1, f_5), \mathrm{Pair}(f_5, f_6)\}$ such that
$L_3 = \{(x_2, f_1), (x_1, f_5), (x_2, f_5), (x_1, f_6)\}$.

SymbolicPreprocessing$(L_3, G, \varnothing)$:
$F_3 = \{x_2 f_1, x_1 f_5, x_2 f_5, x_1 f_6\}$
$T(F_3) = \{\boxed{x_1^2 x_2}, \boxed{x_1 x_2^2}, x_2^3, x_1 x_2 x_3, x_1 x_3^2, x_1 x_3, \ldots\}$

F4: step by step

Example (3 quadratic equation in $\mathbb{F}_{101}$)

In degree 3: $P_3 = \{\mathrm{Pair}(f_1, f_5), \mathrm{Pair}(f_5, f_6)\}$ such that
$L_3 = \{(x_2, f_1), (x_1, f_5), (x_2, f_5), (x_1, f_6)\}$.

SymbolicPreprocessing$(L_3, G, \varnothing)$:
$F_3 = \{x_2 f_1, x_1 f_5, x_2 f_5, x_1 f_6\}$
$T(F_3) = \{\boxed{x_1^2 x_2}, \boxed{x_1 x_2^2}, x_2^3, x_1 x_2 x_3, x_1 x_3^2, x_1 x_3, \ldots\}$
x_2^3 is divisible by $x_2 f_6 \longrightarrow F_3 = F_3 \cup \{x_2 f_6\}$
$x_1 x_2 x_3$ is divisible by $x_3 f_5 \longrightarrow F_3 = F_3 \cup \{x_3 f_5\}$
$\ldots$

F4: step by step

Example (3 quadratic equation in $\mathbb{F}_{101}$)

In degree 3: $P_3 = \{\mathrm{Pair}(f_1, f_5), \mathrm{Pair}(f_5, f_6)\}$ such that
$L_3 = \{(x_2, f_1), (x_1, f_5), (x_2, f_5), (x_1, f_6)\}$.

SymbolicPreprocessing$(L_3, G, \varnothing)$:
$F_3 = \{x_2 f_1, x_1 f_5, x_2 f_5, x_1 f_6\}$
$T(F_3) = \{\boxed{x_1^2 x_2}, \boxed{x_1 x_2^2}, x_2^3, x_1 x_2 x_3, x_1 x_3^2, x_1 x_3, \ldots\}$
x_2^3 is divisible by $x_2 f_6 \longrightarrow F_3 = F_3 \cup \{x_2 f_6\}$
$x_1 x_2 x_3$ is divisible by $x_3 f_5 \longrightarrow F_3 = F_3 \cup \{x_3 f_5\}$
$\ldots$
$F_3 = [x_2\, f_1, x_1\, f_5, x_2\, f_5, x_1\, f_6, x_2\, f_6, x_3\, f_5, x_3\, f_6, f_5, f_6, x_3\, f_1, f_1]$

F4: step by step

Example (3 quadratic equation in $\mathbb{F}_{101}$)

x_2^3 is divisible by $x_2 f_6 \longrightarrow F_3 = F_3 \cup \{x_2 f_6\}$
$x_1 x_2 x_3$ is divisible by $x_3 f_5 \longrightarrow F_3 = F_3 \cup \{x_3 f_5\}$
...

$$F_3 = [x_2\, f_1, x_1\, f_5, x_2\, f_5, x_1\, f_6, x_2\, f_6, x_3\, f_5, x_3\, f_6, f_5, f_6, x_3\, f_1, f_1]$$

$$A_3 = \begin{array}{r|cccccccccccccccc}
f_6 & & & & & & & & & & & 1 & 28 & 19 & 79 & 30 & 50 \\
f_5 & & & & & & & & & & 1 & 0 & 12 & 2 & 55 & 66 & 88 \\
. & & & & & & & & & 1 & 66 & 25 & 4 & 41 & 54 & 42 & 87 \\
. & & & & & 1 & 28 & 19 & 79 & 0 & 0 & 0 & 30 & 50 & 59 & 0 & 0 \\
. & & & & 1 & 0 & 12 & 2 & 55 & 0 & 0 & 0 & 66 & 88 & 60 & 0 & 0 \\
. & & & 1 & 66 & 25 & 4 & 41 & 54 & 0 & 0 & 0 & 42 & 87 & 22 & 0 & 0 \\
. & & 1 & 0 & 28 & 19 & 0 & 79 & 0 & 0 & 30 & 50 & 0 & 59 & 0 & 0 & 46 \\
x_2 f_5 & 1 & 0 & 0 & 12 & 2 & 0 & 55 & 0 & 0 & 66 & 88 & 0 & 60 & 0 & 0 & 92 \\
f_{10} & 1 & 0 & 28 & 19 & 0 & 79 & 0 & 0 & 30 & 50 & 0 & 59 & 0 & 0 & 46 & 0 \\
x_2 f_1 & 1 & 66 & 25 & 0 & 4 & 41 & 0 & 54 & 0 & 0 & 42 & 87 & 0 & 22 & 0 & 0 & 86 \\
f_8 & 1 & 0 & 0 & 12 & 2 & 0 & 55 & 0 & 0 & 66 & 88 & 0 & 60 & 0 & 0 & 92 & 0
\end{array}$$

$$f_{10} = x_1\, {x_3}^2 + 23\, {x_3}^3 + 77\, x_1\, x_3 + 66\, x_2\, x_3 + 84\, {x_3}^2 + 48\, x_1 + 38\, x_2 + 44\, x_3 + 68$$
$$f_8 = x_2\, {x_3}^2 + 98\, {x_3}^3 + 60\, x_1\, x_3 + 34\, x_2\, x_3 + 85\, {x_3}^2 + 65\, x_1 + 9\, x_2 + 74\, x_3 + 28$$

F4: step by step

Example (Cyclic 4)

Monomial ordering is DRL and the normal strategy

$$F = \left[\begin{array}{c} f_1 = abcd - 1, f_2 = abc + abd + acd + bcd, \\ f_3 = ab + bc + ad + cd, f_4 = a + b + c + d \end{array} \right]$$

At the beginning $G = \{f_4\}$ and $P_1 = \{\mathrm{Pair}(f_3, f_4)\}$ such that $L_1 = \{(1, f_3), (b, f_4)\}$.

Example (Cyclic 4)

Monomial ordering is DRL and the normal strategy

$$F = \left[\begin{array}{c} f_1 = abcd - 1, f_2 = abc + abd + acd + bcd, \\ f_3 = ab + bc + ad + cd, f_4 = a + b + c + d \end{array} \right]$$

At the beginning $G = \{f_4\}$ and $P_1 = \{\mathrm{Pair}(f_3, f_4)\}$ such that $L_1 = \{(1, f_3), (b, f_4)\}$.

SymbolicPreprocessing$(L_1, G, \emptyset)$:

$F_1 = \{f_3, b\, f_4\}$ $\quad T(F_1) = \{\boxed{ab}, ad, b^2, bc, bd, cd\}$

$\boxed{ab}$ is already done.

Example (Cyclic 4)

Monomial ordering is DRL and the normal strategy

$$F = \left[\begin{array}{c} f_1 = abcd - 1, f_2 = abc + abd + acd + bcd, \\ f_3 = ab + bc + ad + cd, f_4 = a + b + c + d \end{array} \right]$$

At the beginning $G = \{f_4\}$ and $P_1 = \{\mathrm{Pair}(f_3, f_4)\}$ such that $L_1 = \{(1, f_3), (b, f_4)\}$.

SymbolicPreprocessing$(L_1, G, \varnothing)$:

$F_1 = \{f_3, b\, f_4\}$ $\quad T(F_1) = \{\boxed{ab}, \boxed{ad}, b^2, bc, bd, cd\}$

Example (Cyclic 4)

Monomial ordering is DRL and the normal strategy

$$F = \left[\begin{array}{c} f_1 = abcd - 1, f_2 = abc + abd + acd + bcd, \\ f_3 = ab + bc + ad + cd, f_4 = a + b + c + d \end{array} \right]$$

At the beginning $G = \{f_4\}$ and $P_1 = \{\mathrm{Pair}(f_3, f_4)\}$ such that $L_1 = \{(1, f_3), (b, f_4)\}$.

SymbolicPreprocessing$(L_1, G, \varnothing)$:

$F_1 = \{f_3, b\, f_4\}$ $\quad T(F_1) = \{\boxed{ab}, \boxed{ad}, b^2, bc, bd, cd\}$

ad is top reducible by $f_4 \in G$!

Example (Cyclic 4)

Monomial ordering is DRL and the normal strategy

$$F = \left[\begin{array}{c} f_1 = abcd - 1, f_2 = abc + abd + acd + bcd, \\ f_3 = ab + bc + ad + cd, f_4 = a + b + c + d \end{array} \right]$$

At the beginning $G = \{f_4\}$ and $P_1 = \{\mathrm{Pair}(f_3, f_4)\}$ such that $L_1 = \{(1, f_3), (b, f_4)\}$.

SymbolicPreprocessing$(L_1, G, \varnothing)$:

$F_1 = \{f_3, b\,f_4, df_4\}$ $\quad T(F_1) = \{\boxed{ab}, \boxed{ad}, b^2, bc, bd, cd, d^2\}$

Example (Cyclic 4)

Monomial ordering is DRL and the normal strategy

$$F = \left[\begin{array}{c} f_1 = abcd - 1, f_2 = abc + abd + acd + bcd, \\ f_3 = ab + bc + ad + cd, f_4 = a + b + c + d \end{array} \right]$$

At the beginning $G = \{f_4\}$ and $P_1 = \{\mathrm{Pair}(f_3, f_4)\}$ such that $L_1 = \{(1, f_3), (b, f_4)\}$.

SymbolicPreprocessing$(L_1, G, \varnothing)$:

$F_1 = \{f_3, b\,f_4, df_4\}$ $\quad T(F_1) = \{\boxed{ab}, \boxed{ad}, \boxed{b^2}, bc, bd, cd, d^2\}$

Example (Cyclic 4)

Monomial ordering is DRL and the normal strategy

$$F = \left[\begin{array}{c} f_1 = abcd - 1, f_2 = abc + abd + acd + bcd, \\ f_3 = ab + bc + ad + cd, f_4 = a + b + c + d \end{array} \right]$$

At the beginning $G = \{f_4\}$ and $P_1 = \{\mathrm{Pair}(f_3, f_4)\}$ such that $L_1 = \{(1, f_3), (b, f_4)\}$.

SymbolicPreprocessing$(L_1, G, \emptyset)$:

$F_1 = \{f_3, b\,f_4, df_4\}$ $\quad T(F_1) = \{\boxed{ab}, \boxed{ad}, \boxed{b^2}, bc, bd, cd, d^2\}$

b^2 is not reducible by G

Example (Cyclic 4)

Monomial ordering is DRL and the normal strategy

$$F = \left[\begin{array}{c} f_1 = abcd - 1, f_2 = abc + abd + acd + bcd, \\ f_3 = ab + bc + ad + cd, f_4 = a + b + c + d \end{array} \right]$$

At the beginning $G = \{f_4\}$ and $P_1 = \{\mathrm{Pair}(f_3, f_4)\}$ such that $L_1 = \{(1, f_3), (b, f_4)\}$.

SymbolicPreprocessing$(L_1, G, \varnothing)$:

$F_1 = \{f_3, b\,f_4, df_4\}$ $\quad T(F_1) = \{\boxed{ab}, \boxed{ad}, \boxed{b^2}, \boxed{bc}, \boxed{bd}, \boxed{cd}, \boxed{d^2}\}$

Example (Cyclic 4)

Monomial ordering is DRL and the normal strategy

$$F = \left[\begin{array}{c} f_1 = abcd - 1, f_2 = abc + abd + acd + bcd, \\ f_3 = ab + bc + ad + cd, f_4 = a + b + c + d \end{array} \right]$$

At the beginning $G = \{f_4\}$ and $P_1 = \{\mathrm{Pair}(f_3, f_4)\}$ such that $L_1 = \{(1, f_3), (b, f_4)\}$.

SymbolicPreprocessing $(L_1, G, \varnothing)$ returns

$$F_1 = [f_3, bf_4, df_4].$$

Example (Cyclic 4)

Matrix representation of $F_1 = [f_3, bf_4, df_4]$ is:

$$A_1 = M(F_1) = \begin{array}{c|ccccccc} & ab & b^2 & bc & ad & bd & cd & d^2 \\ df_4 & & & & 1 & 1 & 1 & 1 \\ f_3 & 1 & & 1 & 1 & & 1 & \\ bf_4 & 1 & 1 & 1 & & 1 & & \end{array}$$

Example (Cyclic 4)

Gaussian reduction of A_1 is:

$$\widetilde{A_1} = \begin{array}{c|ccccccc} & ab & b^2 & bc & ad & bd & cd & d^2 \\ df_4 & & & & 1 & 1 & 1 & 1 \\ f_3 & 1 & & 1 & & -1 & & -1 \\ bf_4 & & 1 & & & 2 & & 1 \end{array}$$

Example (Cyclic 4)

$$\widetilde{A_1} = \begin{array}{c|ccccccc} & ab & b^2 & bc & ad & bd & cd & d^2 \\ df_4 & & & & 1 & 1 & 1 & 1 \\ f_3 & 1 & & 1 & & -1 & & -1 \\ bf_4 & & 1 & & & 2 & & 1 \end{array}$$

$$\tilde{F}_1 = \begin{bmatrix} f_5 = ad + bd + cd + d^2, \\ f_6 = ab + bc - bd - d^2, \\ f_7 = b^2 + 2\,bd + d^2 \end{bmatrix}$$

Example (Cyclic 4)

$\tilde{F_1} = [f_5 = ad + bd + cd + d^2,$
$f_6 = ab + bc - bd - d^2,$
$f_7 = b^2 + 2\,bd + d^2]$

and since $ab, ad \in \mathrm{LT}(F_1)$ we have
$\tilde{F_1}_+ = [f_7]$
and now $G = \{f_4, f_7\}$.

Example (Cyclic 4)

For the next step we have to consider $P_2 = \{\mathrm{Pair}(f_2, f_4)\}$
hence $L_2 = \{(1, f_2), (bc, f_4)\}$ and $\mathcal{F} = \{F_1\}$.

Example (Cyclic 4)

$L_2 = \{(1, f_2), (bc, f_4)\}$ et $\mathcal{F} = \{F_1\}$.
In SymbolicPreprocessing we can try to simplify the products $1 \cdot f_2$ and $bc \cdot f_4$ using the previous computations:

For instance $\mathrm{LT}(bc\, f_4) = abc = \mathrm{LT}(c\, f_6)$ and so instead of $bc \cdot f_4$ we can consider $c \cdot f_6$.

Example (Cyclic 4)

For the next step we have to consider $P_2 = \{\mathrm{Pair}(f_2, f_4)\}$
hence $L_2 = \{(1, f_2), (bc, f_4)\}$ and $\mathcal{F} = \{F_1\}$.
SymbolicPreprocessing

$F_2 = \{f_2, c\,f_6\}$ $\quad T(F_2) = \{\boxed{abc}, bc^2, abd, acd, bcd, cd^2\}$

Example (Cyclic 4)

For the next step we have to consider $P_2 = \{\mathrm{Pair}(f_2, f_4)\}$
hence $L_2 = \{(1, f_2), (bc, f_4)\}$ and $\mathcal{F} = \{F_1\}$.
SymbolicPreprocessing

$F_2 = \{f_2, cf_6\}$ $\quad T(F_2) = \{\boxed{abc}, bc^2, \boxed{abd}, acd, bcd, cd^2\}$

Example (Cyclic 4)

$\tilde{F_1} = [f_5 = ad + bd + cd + d^2, f_6 = ab + bc - bd - d^2, f_7 = b^2 + 2\,bd + d^2]$

For the next step we have to consider $P_2 = \{\mathrm{Pair}(f_2, f_4)\}$
hence $L_2 = \{(1, f_2), (bc, f_4)\}$ and $\mathcal{F} = \{F_1\}$.
SymbolicPreprocessing

$F_2 = \{f_2, cf_6\} \quad T(F_2) = \{\boxed{abc}, bc^2, \boxed{abd}, acd, bcd, cd^2\}$

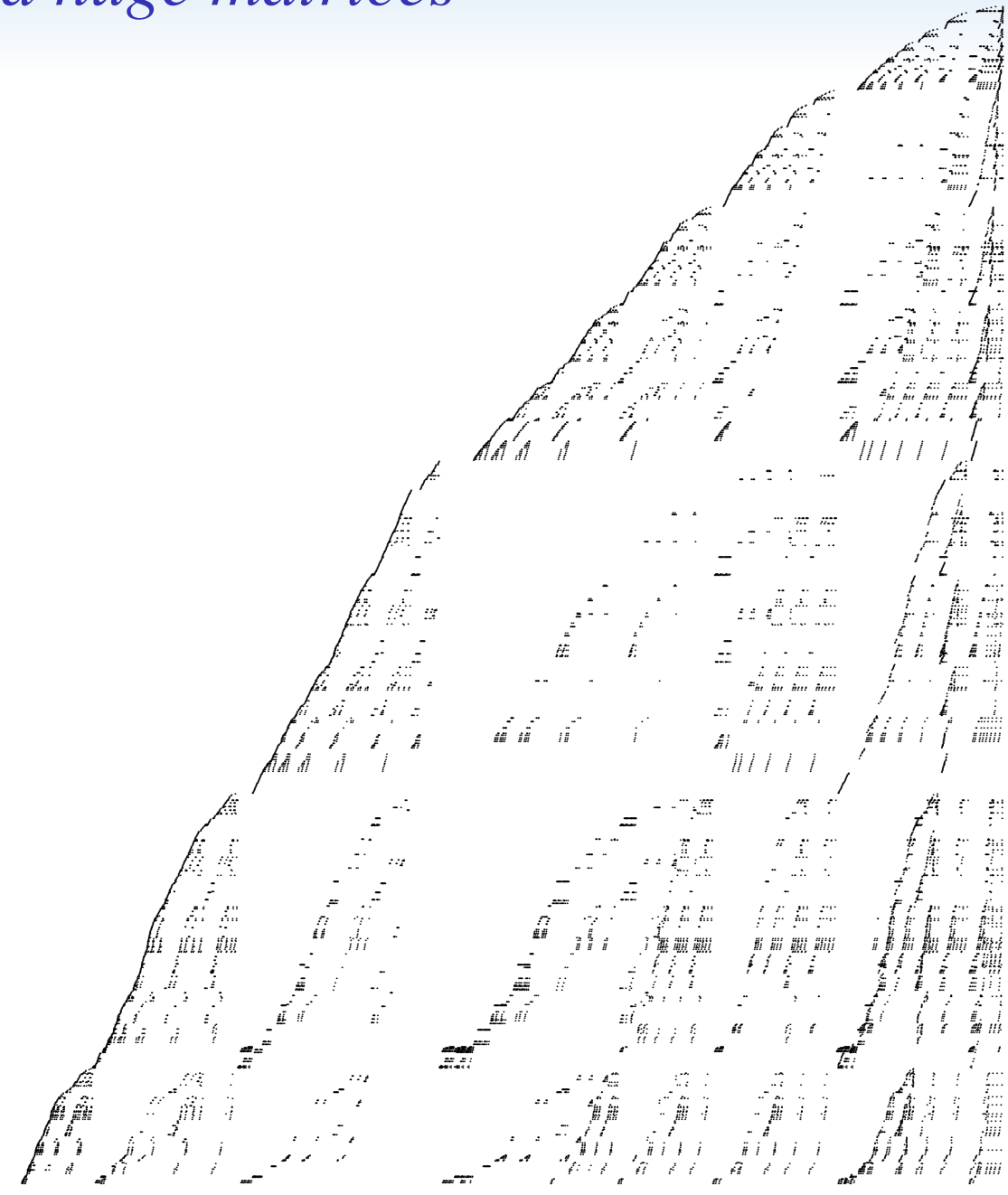
abd is reducible by $bd\,f_4$ but also by $b\,f_5$!

Optimisations

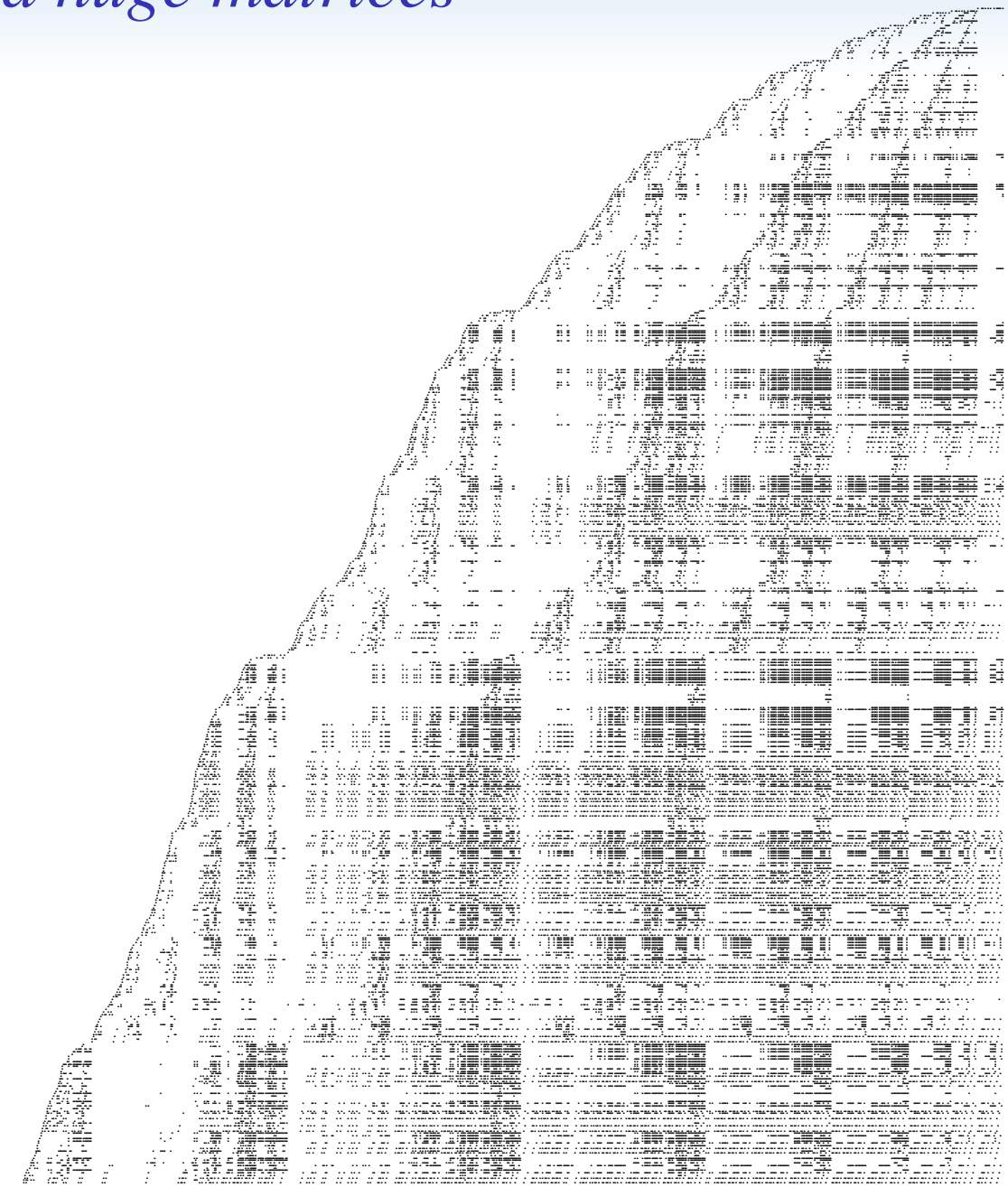
- including Buchberger Criteria (or F_5 criterion).

- reuse **all** the rows in the reduced matrices.
- Improve the linear algebra step (dedicated algorithms, matrix compression, . . .)

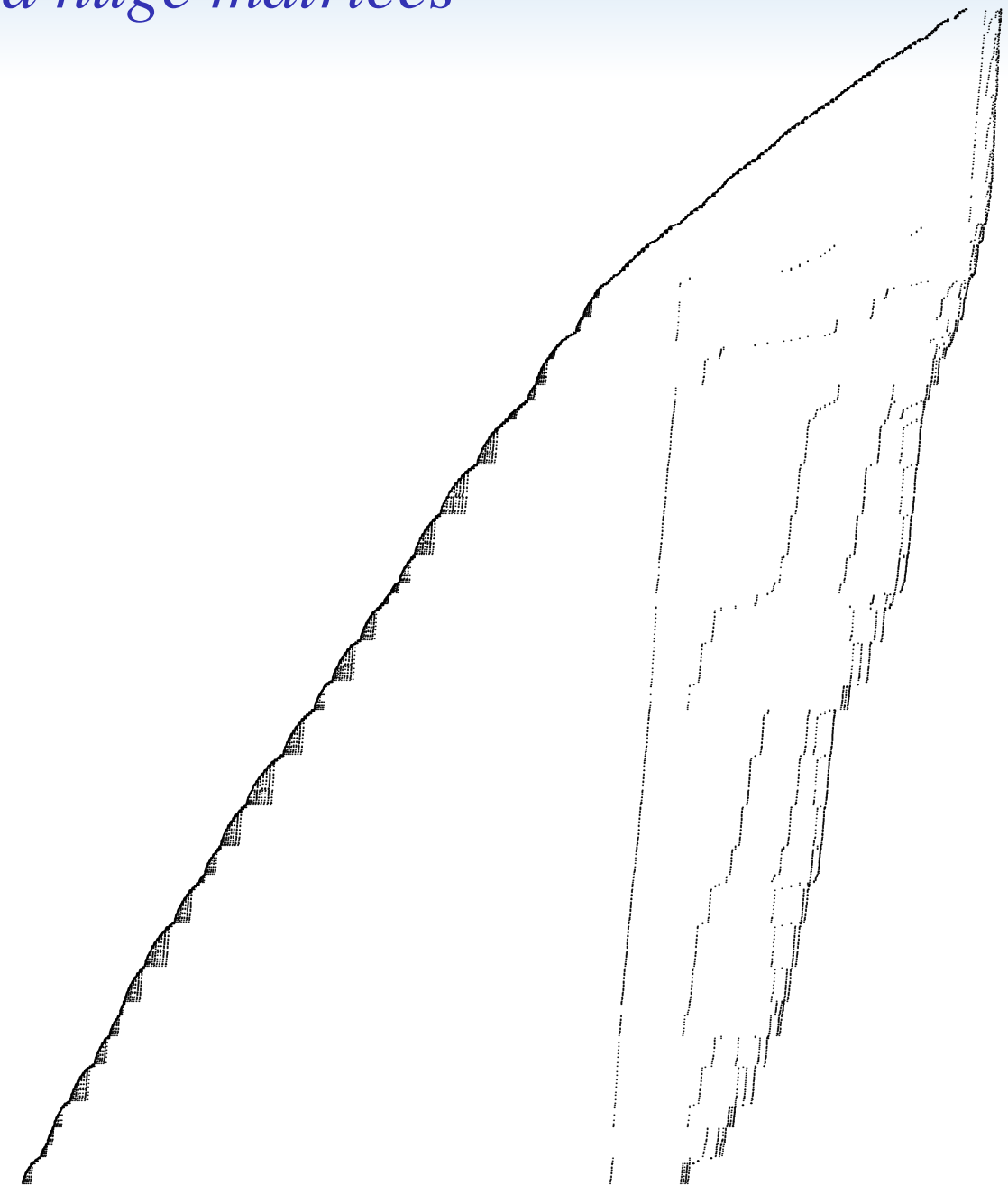
F_4 generated huge matrices



F_4 generated huge matrices



F_4 *generated huge matrices*



Need to compress the matrices !

(i) Compression bitmap: denote by

$$j_1, j_2, j_3, \ldots$$

the position of the non zero elements in the matrix, then

$$\sum_k 2^{j_k - 1}$$

is the corresponding bitmap.
This efficient but the reduction factor is not big (constant factor).

Compress the matrices

(ii) Another idea is to consider the differences (Lempel-Ziv coding):

$$\boxed{j_1}\boxed{j_2 - j_1}\boxed{j_3 - j_2}\cdots$$

when the difference $j_k - j_{k-1}$ is small (< 128), $\longrightarrow$ we can use one byte to store the result.
This method is is more efficient wrt the memory usage and only slightly slower (10%).

Algorithms

Algorithms: for *computing* Gröbner bases.

- Buchberger (1965,1979,1985)
  - ☞ First and Second Criteria
- F_4 using linear algebra (1999) (strategies)
- F_5 no reduction to zero (2002)
  - Today $\longrightarrow$ simple matrix F_5 algorithm
- Signature-based Gröbner computations (2008-. . .)

F_5 *algorithm*

- Goal: avoid useless reduction to 0
  generate full rank matrices
- Incremental algorithm

$$(f_1) + G_{\text{prev}}$$

- We have to explain: new F_5 criterion

F_5 *an example I*

We consider the following example: (b is a parameter):

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

For now we assume that $b = 0$
With Buchberger $x > y > z$:

- 5 useless reductions
- 5 useful pairs

F_5 *an example 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 *an example 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 (first try)

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

and

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

Degree 3 (first try)

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

Degree 3 (first try)

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

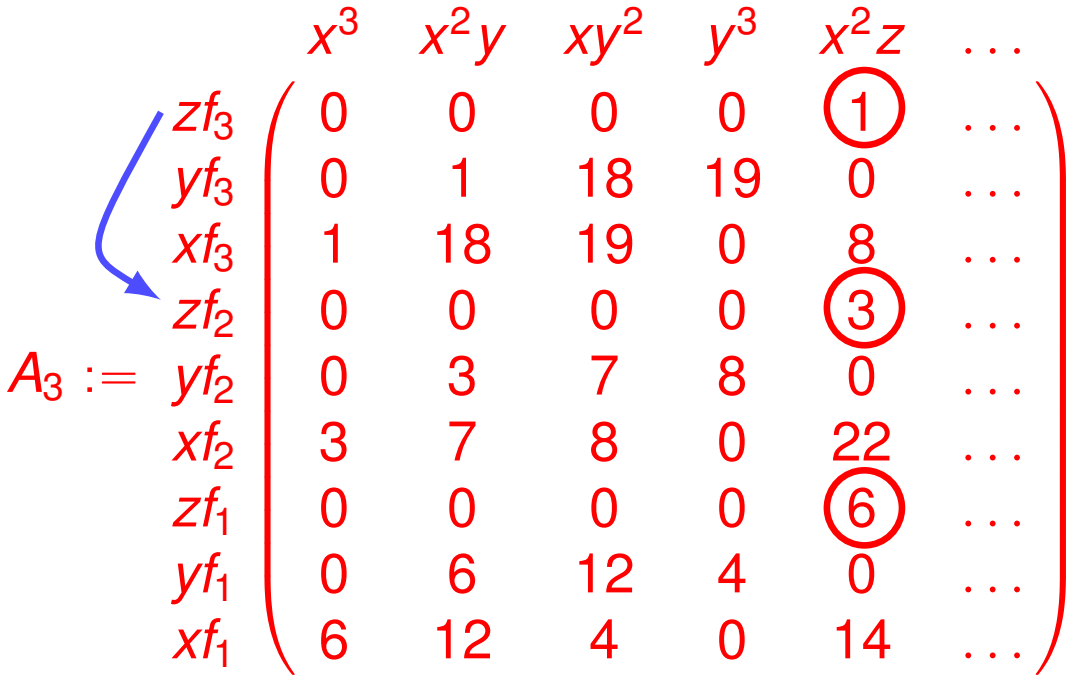
Degree 3 (first try)

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

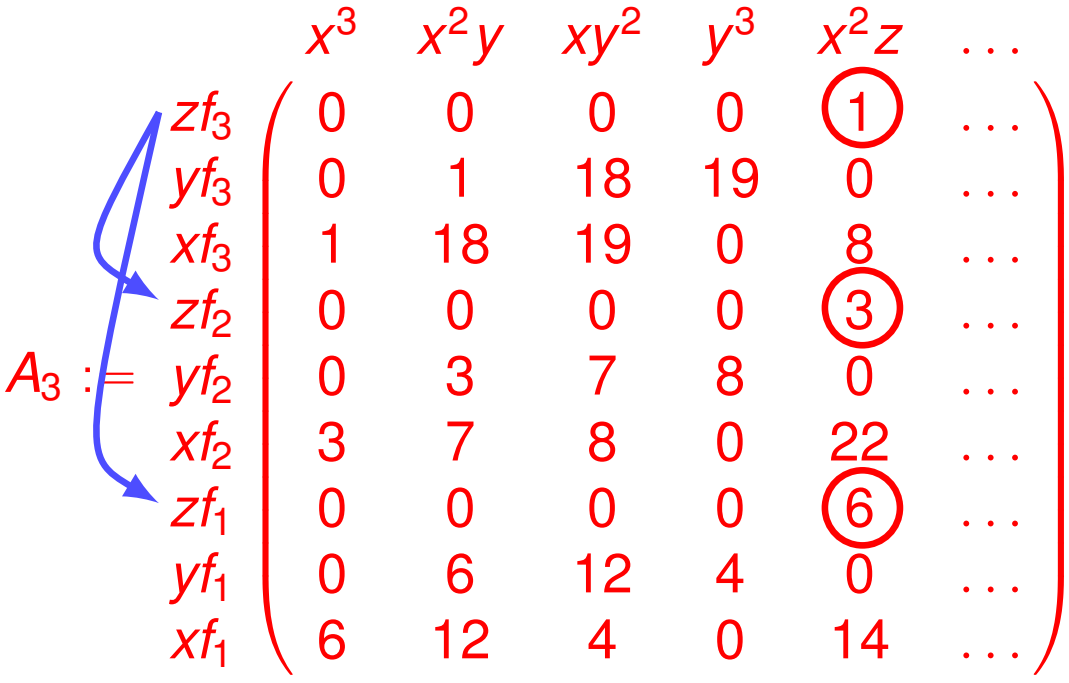
Degree 3 (first try)

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

Degree 3 (first try)



Degree 3 (first try)



Degree 3 (first try)

Already
Done !

$f_2 \longrightarrow f_4$

$f_1 \longrightarrow f_5$

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

Degree 3

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

Degree 3

$$
\tilde{A}_3 := \begin{array}{c} \\ xf_3 \\ yf_3 \\ yf_2 \\ xf_2 \\ zf_3 \\ zf_2 \\ zf_1 \\ yf_1 \\ xf_1 \end{array}
\begin{array}{c}
\begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & xyz & y^2z & xz^2 & yz^2 & z^3 \end{array} \\
\left(\begin{array}{cccccccccc}
1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 & 0 \\
 & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 \\
 & & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 \\
 & & & 1 & 0 & 0 & 8 & 1 & 18 & 15 \\
 & & & & 1 & 18 & 19 & 8 & 5 & 7 \\
 & & & & & 1 & 3 & 2 & 4 & 22 \\
 & & & & & & 1 & 12 & 20 & 18 \\
 & & & & & & & 1 & 11 & 13 \\
 & & & & & & & & 1 & 18
\end{array}\right)
\end{array}
$$

Degree 3

Summary: we have constructed 3 new polynomials

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

And 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

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

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 (but 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

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

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

Need “some” computation

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):

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

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

Degree 4 II

$$A_4 := \begin{bmatrix}
1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 \\
 & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 & & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 \\
 & & & 1 & 3 & 0 & 0 & 2 & 4 & 0 & 0 & 22 & 0 & 0 & 0 \\
 & & & & 1 & 0 & 0 & 0 & 8 & 0 & 1 & 18 & 0 & 15 & 0 \\
 & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 & 0 \\
 & & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 \\
 & & & & & & & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 \\
 & & & & & & & & 1 & 0 & 0 & 8 & 1 & 18 & 15 \\
 & & & & & & & & & 1 & 18 & 19 & 8 & 5 & 7 \\
 & & & & & & & & & & 1 & 11 & 0 & 13 & 0 \\
 & & & & & & & & & & & 1 & 12 & 20 & 18 \\
 & & & & & & & & & & & & 1 & 11 & 13 \\
 & & & & & & & & & & & & & 1 & 18 \\
 & & & & & & & & & & 1 & 3 & 2 & 4 & 22
\end{bmatrix}$$

Degree 4 III

$$A_4 := \left[\begin{array}{cccccccccc|ccccc}
1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 \\
 & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 & & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 \\
 & & & 1 & 3 & 0 & 0 & 2 & 4 & 0 & 0 & 22 & 0 & 0 & 0 \\
 & & & & 1 & 0 & 0 & 0 & 8 & 0 & 1 & 18 & 0 & 15 & 0 \\
 & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 & 0 \\
 & & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 \\
 & & & & & & & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 \\
 & & & & & & & & 1 & 0 & 0 & 8 & 1 & 18 & 15 \\
 & & & & & & & & & 1 & 18 & 19 & 8 & 5 & 7 \\
\hline
 & & & & & & & & & & 1 & 11 & 0 & 13 & 0 \\
 & & & & & & & & & & & 1 & 12 & 20 & 18 \\
 & & & & & & & & & & & & 1 & 11 & 13 \\
 & & & & & & & & & & & & & 1 & 18 \\
 & & & & & & & & & & 1 & 3 & 2 & 4 & 22
\end{array}\right]$$

Degree 4 IV

We need to consider only a small sub-matrix:

$$A_4' := \begin{array}{c} \\ yf_7 \\ z^2f_5 \\ zf_7 \\ zf_8 \\ z^2f_4 \end{array} \begin{array}{c} \begin{array}{ccccc} xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \end{array} \\ \begin{pmatrix} 1 & 11 & 0 & 13 & 0 \\ & 1 & 12 & 20 & 18 \\ & & 1 & 11 & 13 \\ & & & 1 & 18 \\ 1 & 3 & 2 & 4 & 22 \end{pmatrix} \end{array}$$

F5 Criterion : analysis

Example: compute a Gröbner basis of $[f_1, f_2, f_3]$

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

$$u(f_2 f_3 - f_3 f_2) + v(f_1 f_3 - f_3 f_1) + w(f_2 f_1 - f_1 f_2) = 0$$

F5 Criterion : analysis

Example: compute a Gröbner basis of $[f_1, f_2, f_3]$

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

$$u(f_2 f_3 - f_3 f_2) + v(f_1 f_3 - f_3 f_1) + w(f_2 f_1 - f_1 f_2) = 0$$

where u, v, w are arbitrary polynomials.

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 + u\, f_2 f_3 - u\, f_3 f_2 + v\, f_1 f_3 - w f_1 f_2 = 0$$

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 \longrightarrow 0$$

F5 Criterion : analysis

Example: compute a Gröbner basis of $[f_1, f_2, f_3]$

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

$$u(f_2 f_3 - f_3 f_2) + v(f_1 f_3 - f_3 f_1) + w(f_2 f_1 - f_1 f_2) = 0$$

where u, v, w are arbitrary polynomials.

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 + u\, f_2 f_3 - u\, f_3 f_2 + v\, f_1 f_3 - w f_1 f_2 = 0$$

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 \longrightarrow 0$$

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

F5 Criterion : analysis

Example: compute a Gröbner basis of $[f_1, f_2, f_3]$

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

$$u(f_2 f_3 - f_3 f_2) + v(f_1 f_3 - f_3 f_1) + w(f_2 f_1 - f_1 f_2) = 0$$

where u, v, w are arbitrary polynomials.

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 + u\, f_2 f_3 - u\, f_3 f_2 + v\, f_1 f_3 - w f_1 f_2 = 0$$

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 \longrightarrow 0$$

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

F_5 Criterion: compute a Gröbner basis G' of $Id(f_2, f_3)$.

Remove row $t\, f_1$ iff t reducible by $\mathrm{LT}(G')$

Keep row $t\, f_1$ iff t not reducible by $\mathrm{LT}(G')$

Références I


B. Buchberger.
An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal.
Journal of Symbolic Computation, 41(3-4):475–511, 3 2006.


Buchberger B.
Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.
PhD thesis, Innsbruck, 1965.


Buchberger B.
An Algorithmical Criterion for the Solvability of Algebraic Systems.
Aequationes Mathematicae, 4(3):374–383, 1970.
(German).


Cox D., Little J., and O'Shea D.
Ideals, Varieties and Algorithms.
Springer Verlag, New York, 1992.

Références II


Joachim von zur Gathen and Jürgen Gerhard .
Modern Computer Algebra.
Cambridge Press, 1999.