Complexity aspects of Gröbner basis attacks on multivariate post-quantum cryptosystems

Young Cryptographers in Genova 2023

Sriram Gopalakrishnan, Vincent Neiger, Mohab Safey El Din

December 1, 2023

Sorbonne Université, CNRS, LIP6, France
University of Waterloo, David R. Cheriton School of Computer Science, Canada

Determinantal systems

Determinantal systems

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \end{pmatrix}$$

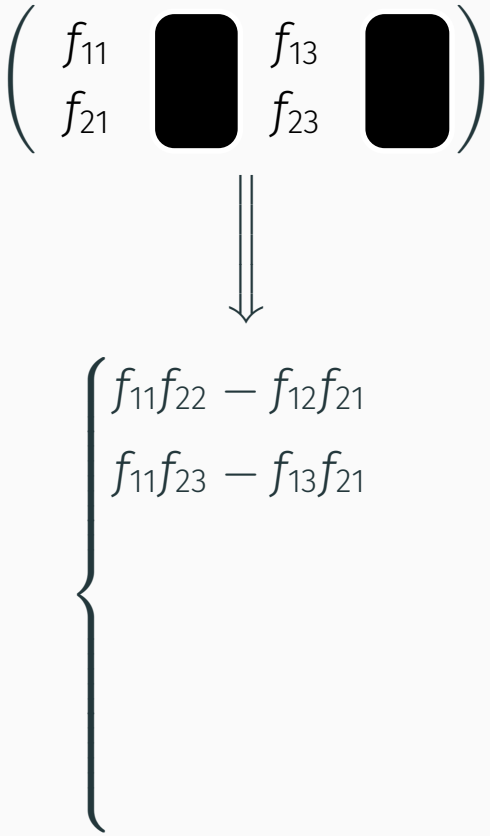
Determinantal systems

$$\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \boxed{}$$

$$\Downarrow$$

$$\begin{cases} f_{11}f_{22} - f_{12}f_{21} \\ \\ \\ \\ \\ \\ \end{cases}$$

Determinantal systems



Determinantal systems

$$\begin{pmatrix} f_{11} & \blacksquare & f_{14} \\ f_{21} & & f_{24} \end{pmatrix}$$

$$\Downarrow$$

$$\begin{cases} f_{11}f_{22} - f_{12}f_{21} \\ f_{11}f_{23} - f_{13}f_{21} \\ f_{11}f_{24} - f_{14}f_{21} \\ \\ \\ \\ \end{cases}$$

Determinantal systems

$$\begin{pmatrix} \blacksquare & f_{12} & f_{13} & \blacksquare \\ & f_{22} & f_{23} & \end{pmatrix}$$

$$\Downarrow$$

$$\begin{cases} f_{11}f_{22} - f_{12}f_{21} \\ f_{11}f_{23} - f_{13}f_{21} \\ f_{11}f_{24} - f_{14}f_{21} \\ f_{12}f_{23} - f_{13}f_{22} \\ \\ \end{cases}$$

Determinantal systems

$$\begin{pmatrix} \blacksquare & f_{12} & \blacksquare & f_{14} \\ & f_{22} & & f_{24} \end{pmatrix}$$

$$\Downarrow$$

$$\begin{cases} f_{11}f_{22} - f_{12}f_{21} \\ f_{11}f_{23} - f_{13}f_{21} \\ f_{11}f_{24} - f_{14}f_{21} \\ f_{12}f_{23} - f_{13}f_{22} \\ f_{12}f_{24} - f_{14}f_{22} \\ \end{cases}$$

Determinantal systems

$$\begin{pmatrix} \blacksquare & f_{13} & f_{14} \\ & f_{23} & f_{24} \end{pmatrix}$$

$$\Downarrow$$

$$\begin{cases} f_{11}f_{22} - f_{12}f_{21} \\ f_{11}f_{23} - f_{13}f_{21} \\ f_{11}f_{24} - f_{14}f_{21} \\ f_{12}f_{23} - f_{13}f_{22} \\ f_{12}f_{24} - f_{14}f_{22} \\ f_{13}f_{24} - f_{14}f_{23} \end{cases}$$

Determinantal systems

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \end{pmatrix}$$

$$\Downarrow$$

$$\begin{cases} f_{11}f_{22} - f_{12}f_{21} \\ f_{11}f_{23} - f_{13}f_{21} \\ f_{11}f_{24} - f_{14}f_{21} \\ f_{12}f_{23} - f_{13}f_{22} \\ f_{12}f_{24} - f_{14}f_{22} \\ f_{13}f_{24} - f_{14}f_{23} \end{cases}$$

The MinRank Problem

$f_{i,j}$ are **linear forms** in $\mathbb{k}[x_1, \ldots, x_k]$.
Find $\boldsymbol{a} \in \overline{\mathbb{k}}^k$ with $\mathbf{rank}(M(\boldsymbol{a})) \leq r$.

Determinantal systems

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \end{pmatrix}$$

$$\Downarrow$$

$$\begin{cases} f_{11}f_{22} - f_{12}f_{21} \\ f_{11}f_{23} - f_{13}f_{21} \\ f_{11}f_{24} - f_{14}f_{21} \\ f_{12}f_{23} - f_{13}f_{22} \\ f_{12}f_{24} - f_{14}f_{22} \\ f_{13}f_{24} - f_{14}f_{23} \end{cases}$$

i.e. $f_{i,j} = a_1x_1 + \cdots + a_kx_k + b$

The MinRank Problem

$f_{i,j}$ are **linear forms** in $\mathbb{k}[x_1, \ldots, x_k]$.
Find $\boldsymbol{a} \in \overline{\mathbb{k}}^k$ with $\mathbf{rank}(M(\boldsymbol{a})) \leq r$.

Determinantal systems

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \end{pmatrix}$$

$$\Downarrow$$

$$\begin{cases} f_{11}f_{22} - f_{12}f_{21} \\ f_{11}f_{23} - f_{13}f_{21} \\ f_{11}f_{24} - f_{14}f_{21} \\ f_{12}f_{23} - f_{13}f_{22} \\ f_{12}f_{24} - f_{14}f_{22} \\ f_{13}f_{24} - f_{14}f_{23} \end{cases}$$

i.e. $f_{i,j} = a_1x_1 + \cdots + a_kx_k + b$

- HFE
- OV

- GeMSS
- Rainbow

The MinRank Problem

$f_{i,j}$ are **linear forms** in $\mathbb{k}[x_1, \ldots, x_k]$.
Find $\boldsymbol{a} \in \overline{\mathbb{k}}^k$ with $\mathbf{rank}(M(\boldsymbol{a})) \leq r$.

Determinantal systems

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \end{pmatrix}$$

$$\Downarrow$$

$$\begin{cases} f_{11}f_{22} - f_{12}f_{21} \\ f_{11}f_{23} - f_{13}f_{21} \\ f_{11}f_{24} - f_{14}f_{21} \\ f_{12}f_{23} - f_{13}f_{22} \\ f_{12}f_{24} - f_{14}f_{22} \\ f_{13}f_{24} - f_{14}f_{23} \end{cases}$$

i.e. $f_{i,j} = a_1x_1 + \cdots + a_kx_k + b$

Security of post-quantum cryptosystems $\longleftrightarrow$ **Complexity** of MinRank

- HFE
- OV

- GeMSS
- Rainbow

The MinRank Problem

$f_{i,j}$ are **linear forms** in $\mathbb{k}[x_1, \ldots, x_k]$.
Find $\boldsymbol{a} \in \overline{\mathbb{k}}^k$ with $\mathbf{rank}(M(\boldsymbol{a})) \leq r$.

Gröbner bases

$F \subseteq \mathbb{k}[x_1, \ldots, x_k]$ a polynomial system.

Gröbner bases

$F \subseteq \mathbb{k}[x_1, \ldots, x_k]$ a polynomial system.

Definition (Gröbner bases)

A $\succ$-*Gröbner basis* is a finite generating set G for $\langle F \rangle$ such that $\langle \mathsf{LM}_\succ(G) \rangle = \mathsf{LM}_\succ(\langle F \rangle)$.

Gröbner bases

$F \subseteq \mathbb{k}[x_1, \ldots, x_k]$ a polynomial system.

Definition (Gröbner bases)

A $\succ$-*Gröbner basis* is a finite generating set G for $\langle F \rangle$ such that $\langle \mathsf{LM}_\succ(G) \rangle = \mathsf{LM}_\succ(\langle F \rangle)$.

Theorem (Buchberger's criterion, [Buchberger, 1976])

$g_1, \ldots, g_m$ is a $\succ$-Gröbner basis for $\langle g_1, \ldots, g_m \rangle$ if and only if all S-pairs reduce to zero upon division by $g_1, \ldots, g_m$.

Gröbner bases

$F \subseteq \mathbb{k}[x_1, \ldots, x_k]$ a polynomial system.

Definition (Gröbner bases)

A $\succ$-*Gröbner basis* is a finite generating set G for $\langle F \rangle$ such that $\langle \mathsf{LM}_\succ(G) \rangle = \mathsf{LM}_\succ(\langle F \rangle)$.

Theorem (Buchberger's criterion, [Buchberger, 1976])

$g_1, \ldots, g_m$ is a $\succ$-Gröbner basis for $\langle g_1, \ldots, g_m \rangle$ if and only if all S-pairs reduce to zero upon division by $g_1, \ldots, g_m$.

Complexity

Doubly exponential in the number of variables. [Mayr, Mayer, 1982]

Gröbner bases

$F \subseteq \mathbb{k}[x_1, \ldots, x_k]$ a polynomial system.

Definition (Gröbner bases)

A $\succ$-*Gröbner basis* is a finite generating set G for $\langle F \rangle$ such that $\langle \mathrm{LM}_\succ(G) \rangle = \mathrm{LM}_\succ(\langle F \rangle)$.

Theorem (Buchberger's criterion, [Buchberger, 1976])

$g_1, \ldots, g_m$ is a $\succ$-Gröbner basis for $\langle g_1, \ldots, g_m \rangle$ if and only if all S-pairs reduce to zero upon division by $g_1, \ldots, g_m$.

Complexity

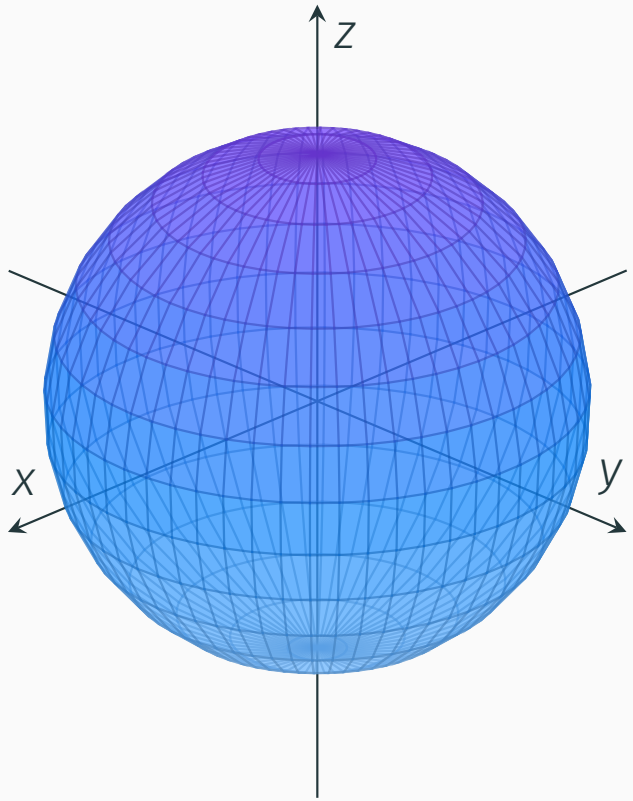
Doubly exponential in the number of variables. [Mayr, Mayer, 1982]

For zero-dimensional systems:

$$\max_{f \in F} \{\deg f\}^{O(\#\text{ of variables})}$$ [Lazard, 1983]

An example

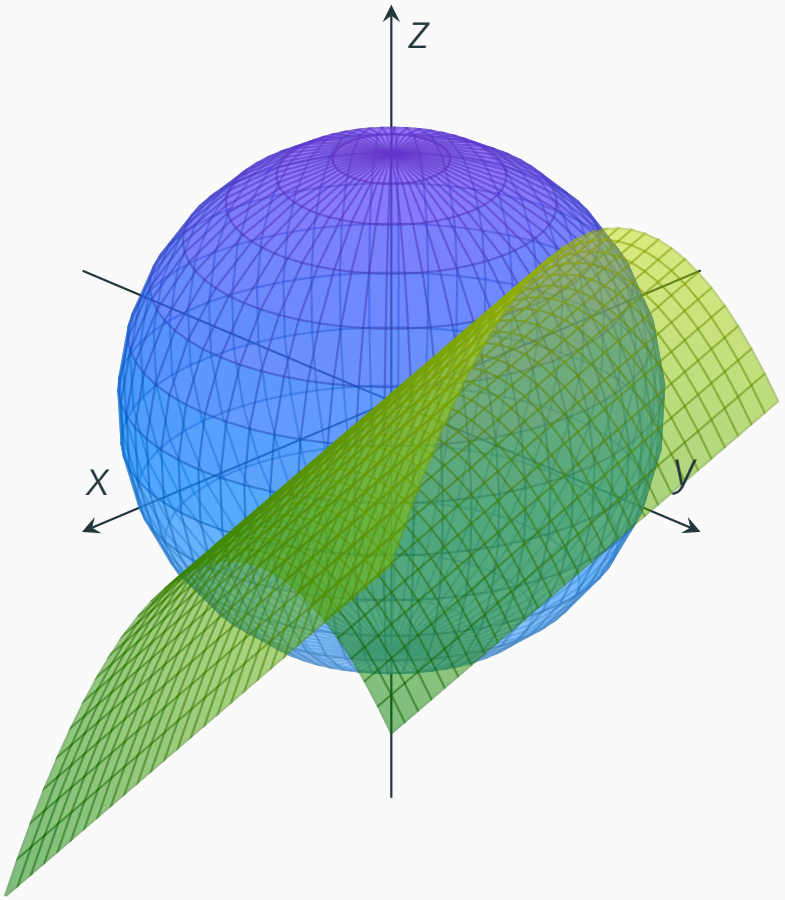
$$f_1 = x^2 + y^2 + z^2 - 1$$



An example

$$f_1 = x^2 + y^2 + z^2 - 1$$

$$f_2 = x^2 - y + z$$

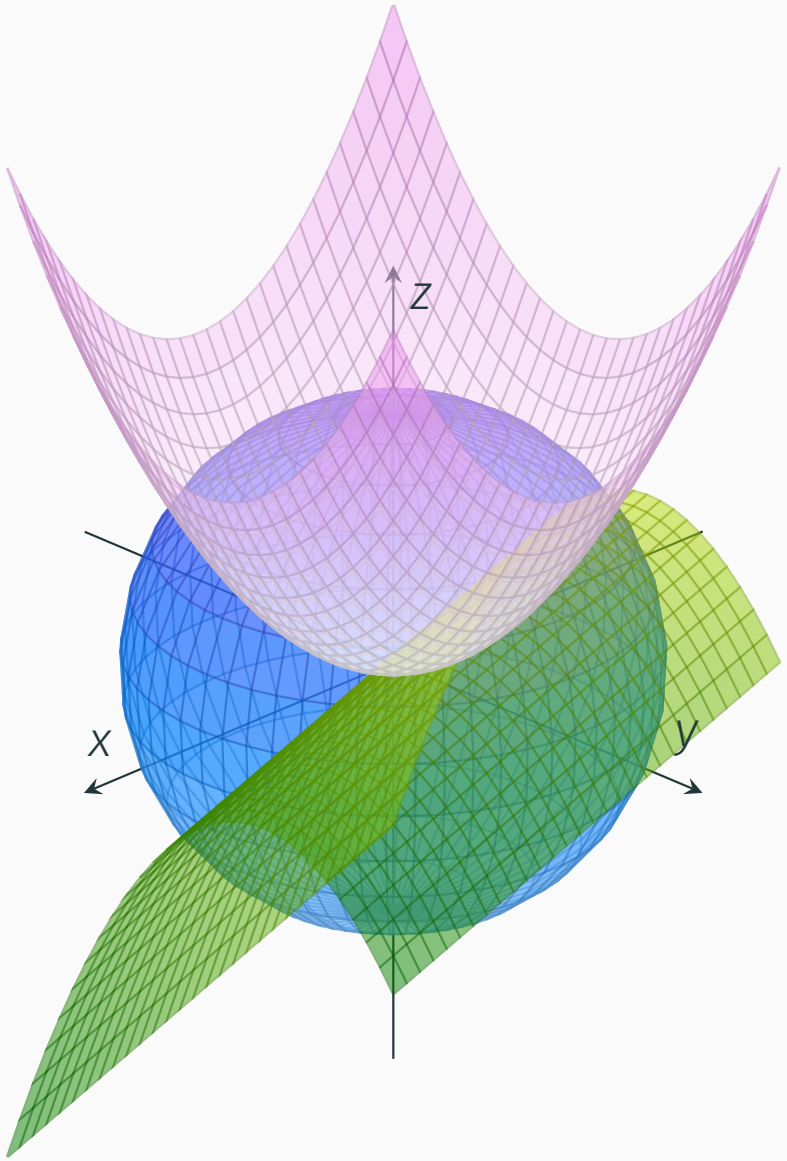


An example

$$f_1 = x^2 + y^2 + z^2 - 1$$

$$f_2 = x^2 - y + z$$

$$f_3 = x^2 + y^2 - z$$

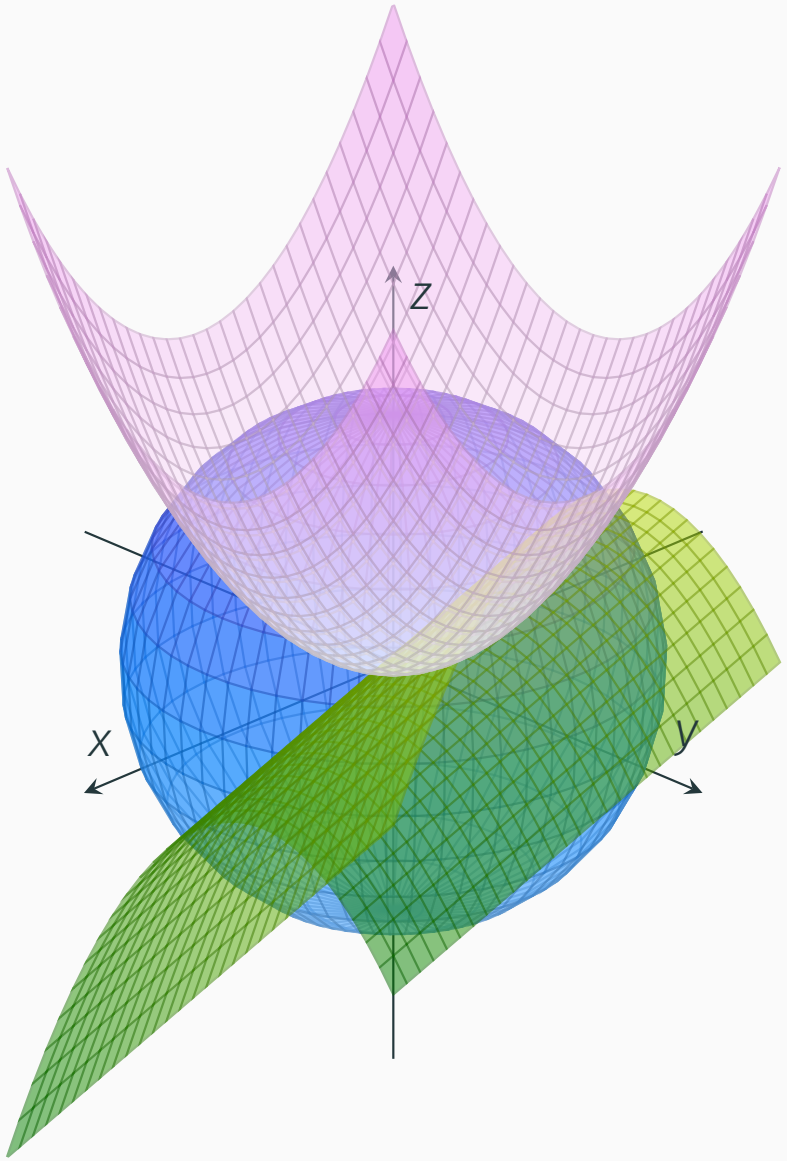


An example

$$f_1 = x^2 + y^2 + z^2 - 1$$
$$f_2 = x^2 - y + z$$
$$f_3 = x^2 + y^2 - z$$

Gröbner basis algorithm

$$x^2 - y + z$$
$$y^2 + y - 2z$$
$$z^2 + z - 1$$



An example

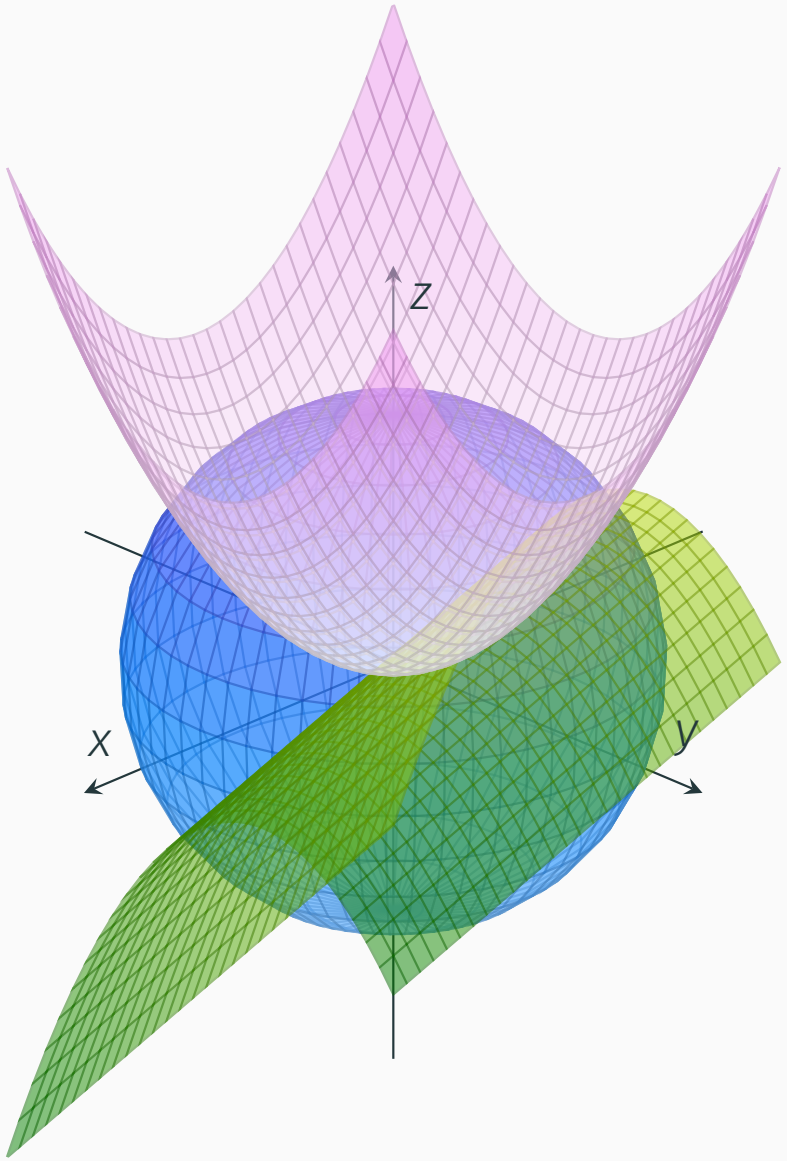
$$f_1 = x^2 + y^2 + z^2 - 1$$
$$f_2 = x^2 - y + z$$
$$f_3 = x^2 + y^2 - z$$

Gröbner basis algorithm

$$x^2 - y + z$$

$$y^2 + y - 2z$$

$$z^2 + z - 1$$



An example

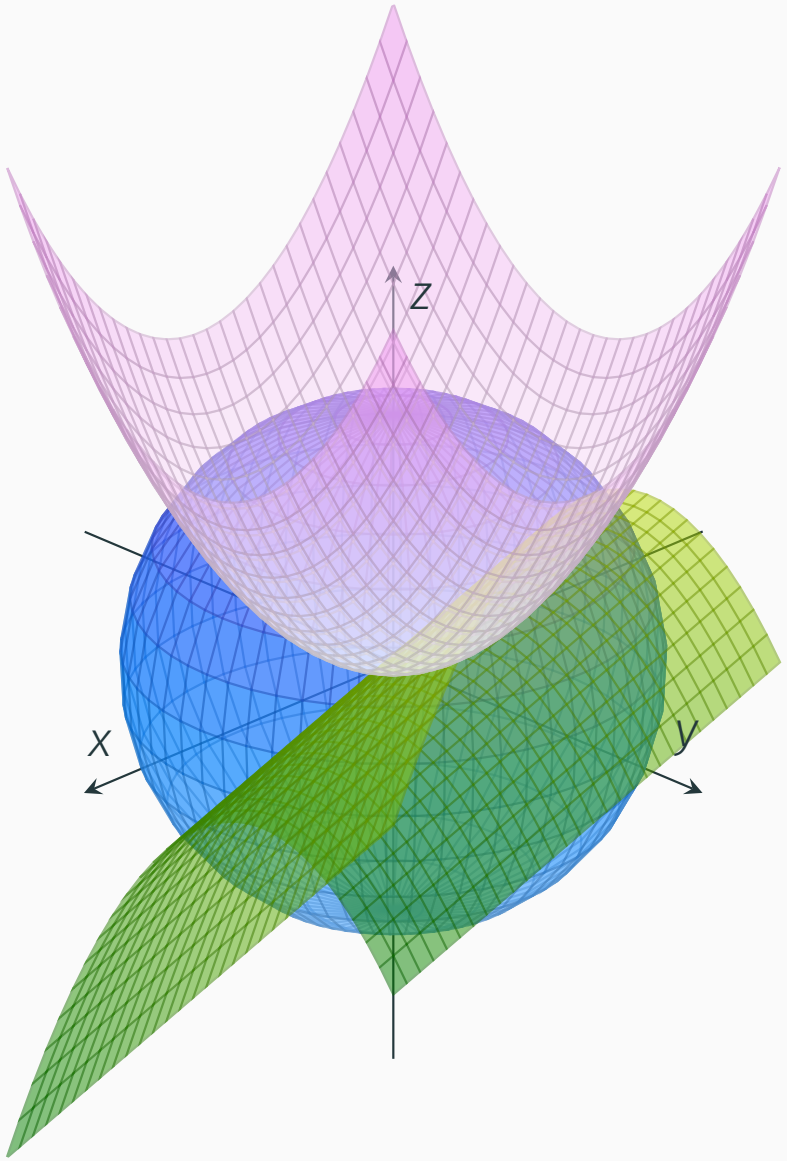
$$f_1 = x^2 + y^2 + z^2 - 1$$
$$f_2 = x^2 - y + z$$
$$f_3 = x^2 + y^2 - z$$

Gröbner basis algorithm

$$x^2 - y + z$$

$$y^2 + y - 2z$$

$$z^2 + z - 1$$

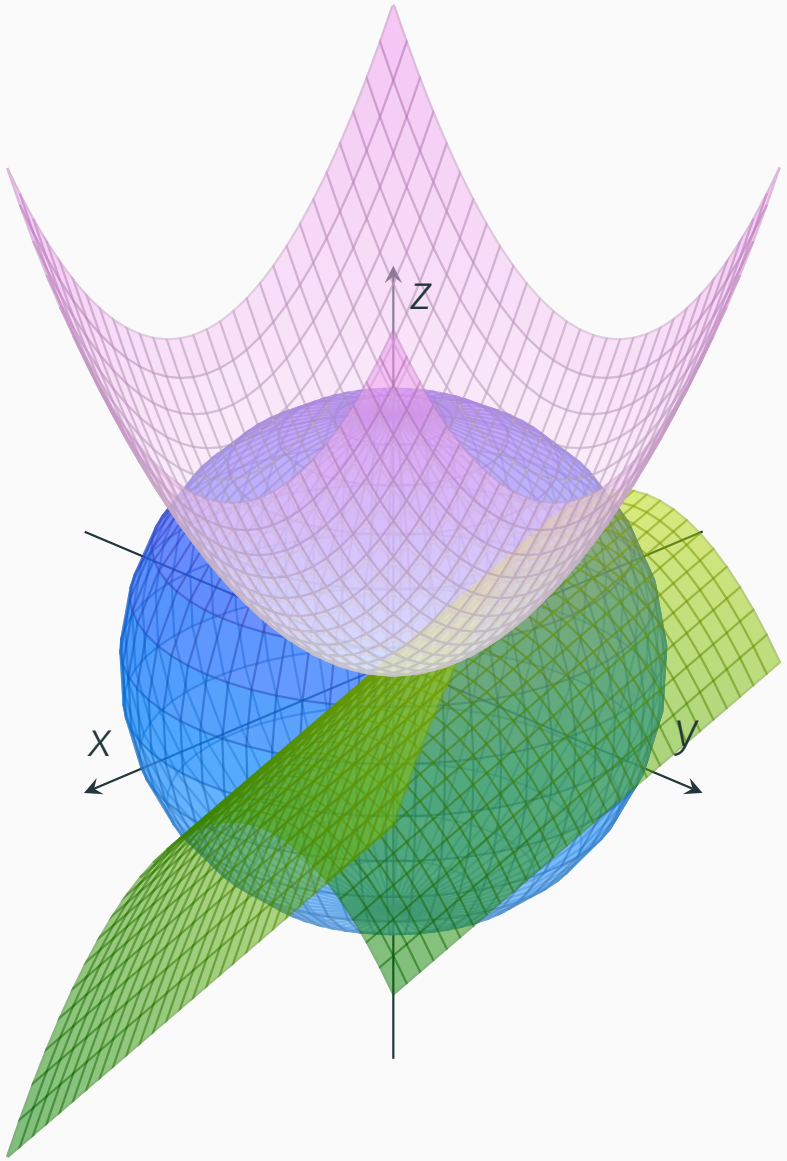


An example

$$f_1 = x^2 + y^2 + z^2 - 1$$
$$f_2 = x^2 - y + z$$
$$f_3 = x^2 + y^2 - z$$

Gröbner basis algorithm

$$x^2 - y + z$$
$$y^2 + y - 2z$$
$$z^2 + z - 1$$

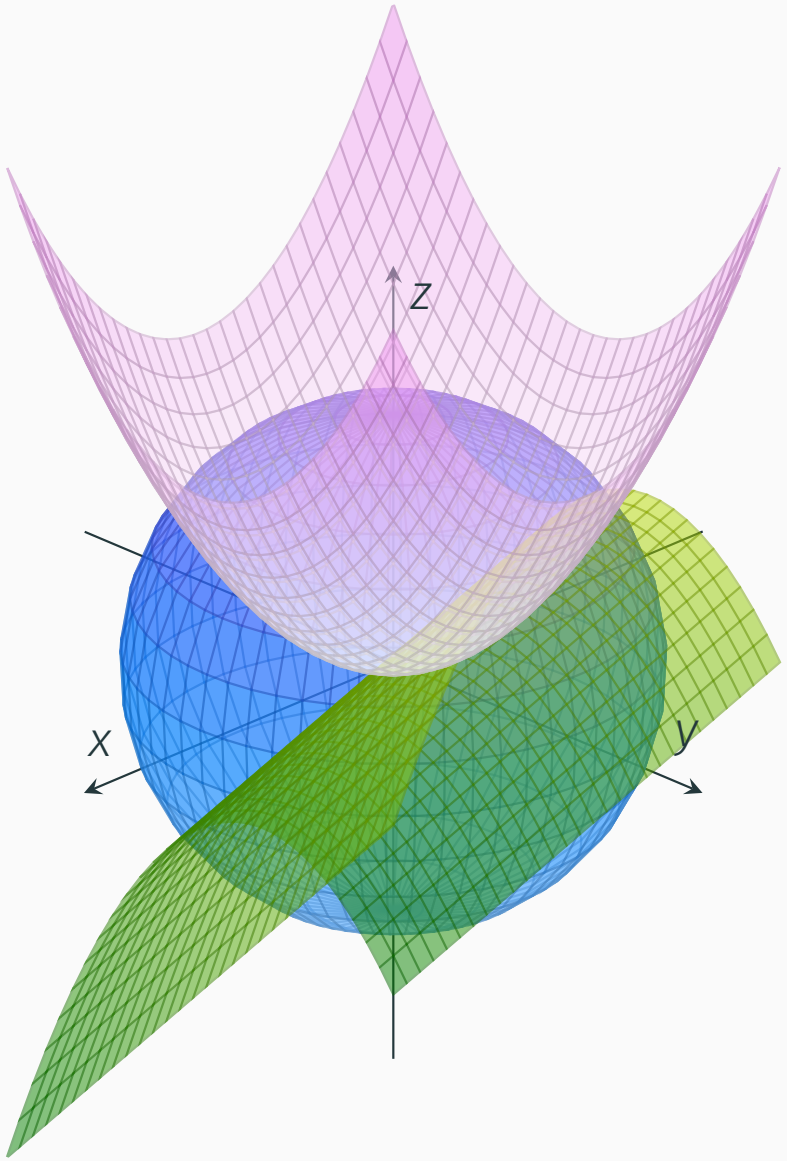


An example

$$f_1 = x^2 + y^2 + z^2 - 1$$
$$f_2 = x^2 - y + z$$
$$f_3 = x^2 + y^2 - z$$

Gröbner basis algorithm

$$x^2 - y + z$$
$$y^2 + y - 2z$$
$$z^2 + z - 1$$

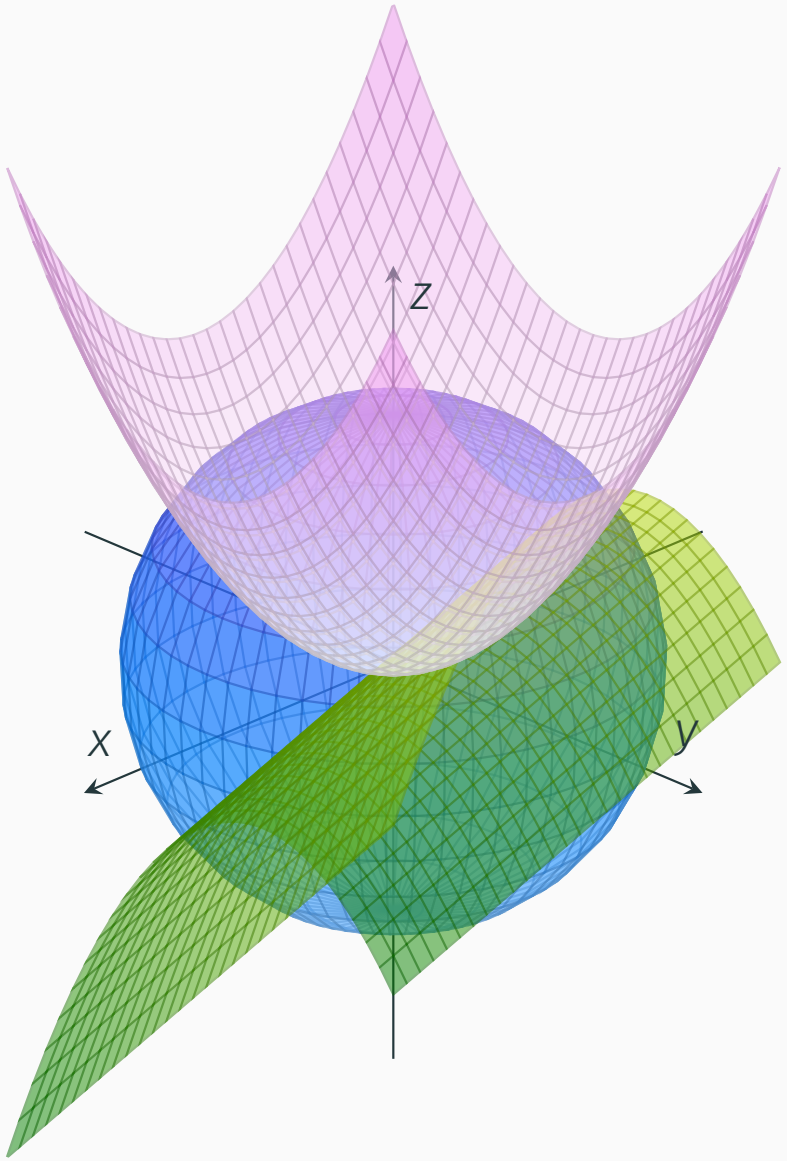


An example

$$f_1 = x^2 + y^2 + z^2 - 1$$
$$f_2 = x^2 - y + z$$
$$f_3 = x^2 + y^2 - z$$

Gröbner basis algorithm

$$x^2 - y + z$$
$$y^2 + y - 2z$$
$$z^2 + z - 1$$

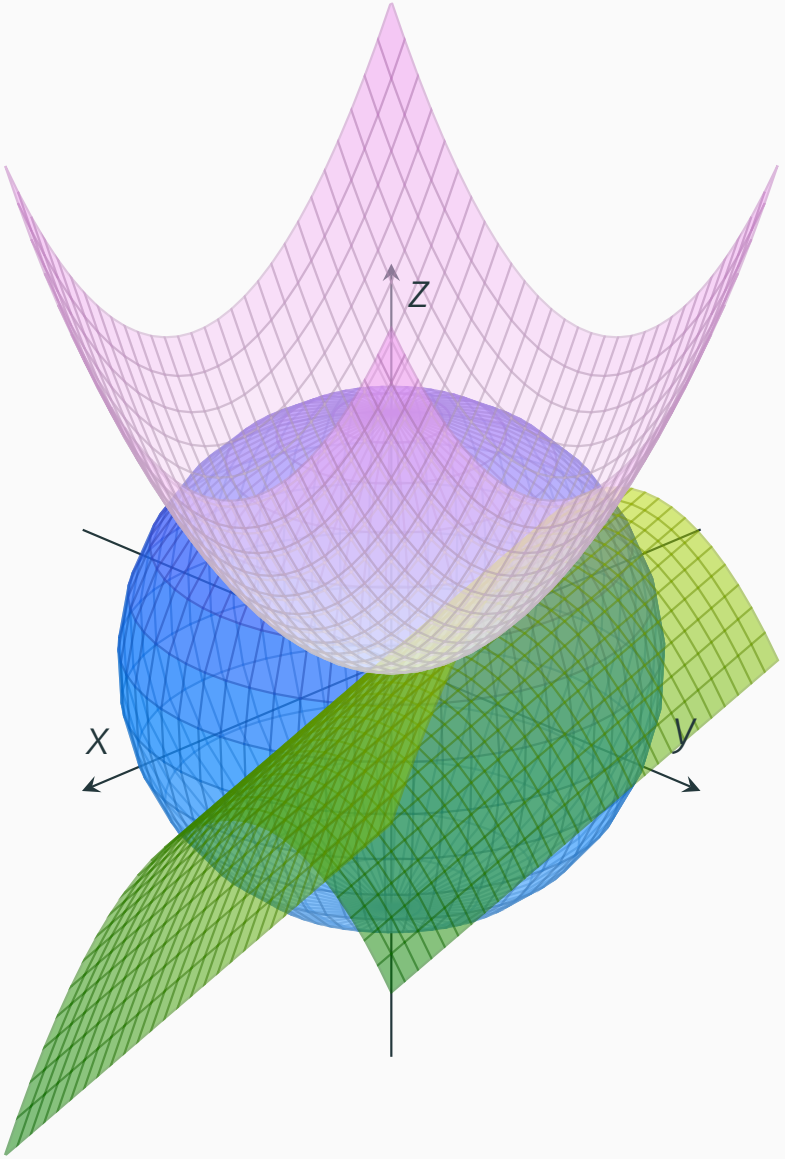


An example

$$f_1 = x^2 + y^2 + z^2 - 1$$
$$f_2 = x^2 - y + z$$
$$f_3 = x^2 + y^2 - z$$

Gröbner basis algorithm

$$x^2 - y + z$$
$$y^2 + y - 2z$$
$$z^2 + z - 1$$



Macaulay matrices - linearization

Assume F homogeneous.

Macaulay matrices - linearization

Assume F homogeneous.

$$\begin{cases} f_1 = 2x^2 + 11xy - y^2 \\ f_2 = 4x^2 + xy - 2y^2 \\ f_3 = -6x^2 - xy + y^2 \end{cases}$$

$$\begin{array}{c} \begin{array}{cccc} x^3 & x^2y & xy^2 & y^3 \end{array} \\ \begin{pmatrix} & & & \\ & & & \\ & & & \end{pmatrix} \end{array}$$

Macaulay matrices - linearization

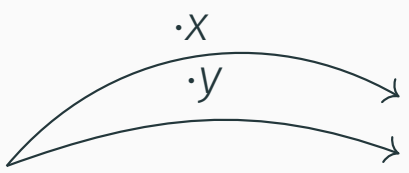
Assume F homogeneous.

$$\begin{cases} f_1 = 2x^2 + 11xy - y^2 \\ f_2 = 4x^2 + xy - 2y^2 \\ f_3 = -6x^2 - xy + y^2 \end{cases} \xrightarrow{\cdot x} \begin{array}{c} \\ xf_1 \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{cccc} x^3 & x^2y & xy^2 & y^3 \end{array} \\ \begin{pmatrix} 2 & 11 & -1 & 0 \\ & & & \\ & & & \\ & & & \end{pmatrix} \end{array}$$

Macaulay matrices - linearization

Assume F homogeneous.

$$\begin{cases} f_1 = 2x^2 + 11xy - y^2 \\ f_2 = 4x^2 + xy - 2y^2 \\ f_3 = -6x^2 - xy + y^2 \end{cases}$$

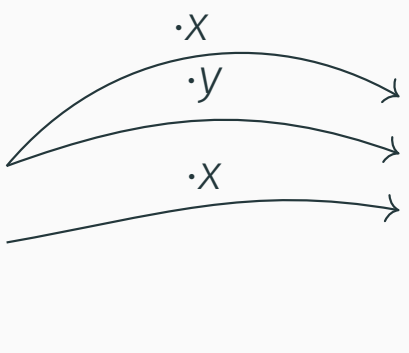


$$\begin{array}{c} \\ xf_1 \\ yf_1 \end{array} \begin{array}{c} \begin{array}{cccc} x^3 & x^2y & xy^2 & y^3 \end{array} \\ \begin{pmatrix} 2 & 11 & -1 & 0 \\ 0 & 2 & 11 & -1 \end{pmatrix} \end{array}$$

Macaulay matrices - linearization

Assume F homogeneous.

$$\begin{cases} f_1 = 2x^2 + 11xy - y^2 \\ f_2 = 4x^2 + xy - 2y^2 \\ f_3 = -6x^2 - xy + y^2 \end{cases}$$

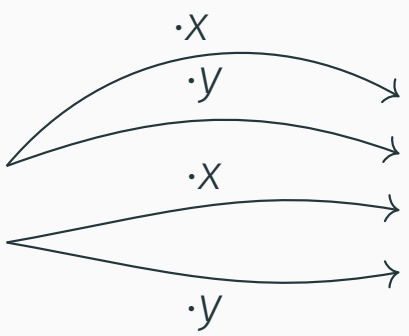


$$\begin{array}{c} \begin{array}{cccc} x^3 & x^2y & xy^2 & y^3 \end{array} \\ \begin{pmatrix} 2 & 11 & -1 & 0 \\ 0 & 2 & 11 & -1 \\ 4 & 1 & -2 & 0 \\ & & & \\ & & & \\ & & & \end{pmatrix} \end{array}$$

Macaulay matrices - linearization

Assume F homogeneous.

$$\begin{cases} f_1 = 2x^2 + 11xy - y^2 \\ f_2 = 4x^2 + xy - 2y^2 \\ f_3 = -6x^2 - xy + y^2 \end{cases}$$

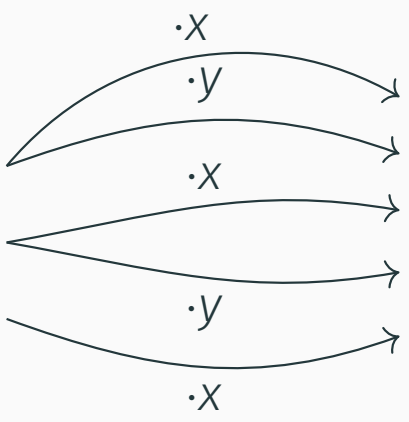


$$\begin{array}{c} \\ xf_1 \\ yf_1 \\ xf_2 \\ yf_2 \end{array} \begin{array}{c} \begin{array}{cccc} x^3 & x^2y & xy^2 & y^3 \end{array} \\ \begin{pmatrix} 2 & 11 & -1 & 0 \\ 0 & 2 & 11 & -1 \\ 4 & 1 & -2 & 0 \\ 0 & 4 & 1 & -2 \end{pmatrix} \end{array}$$

Macaulay matrices - linearization

Assume F homogeneous.

$$\begin{cases} f_1 = 2x^2 + 11xy - y^2 \\ f_2 = 4x^2 + xy - 2y^2 \\ f_3 = -6x^2 - xy + y^2 \end{cases}$$

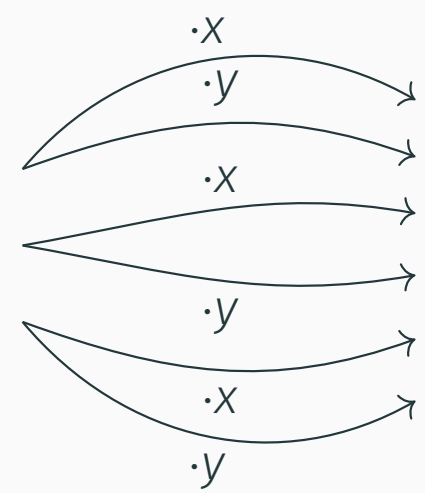


$$\begin{array}{c} \\ xf_1 \\ yf_1 \\ xf_2 \\ yf_2 \\ xf_3 \end{array} \begin{array}{c} \begin{array}{cccc} x^3 & x^2y & xy^2 & y^3 \end{array} \\ \begin{pmatrix} 2 & 11 & -1 & 0 \\ 0 & 2 & 11 & -1 \\ 4 & 1 & -2 & 0 \\ 0 & 4 & 1 & -2 \\ -6 & -1 & 1 & 0 \end{pmatrix} \end{array}$$

Macaulay matrices - linearization

Assume F homogeneous.

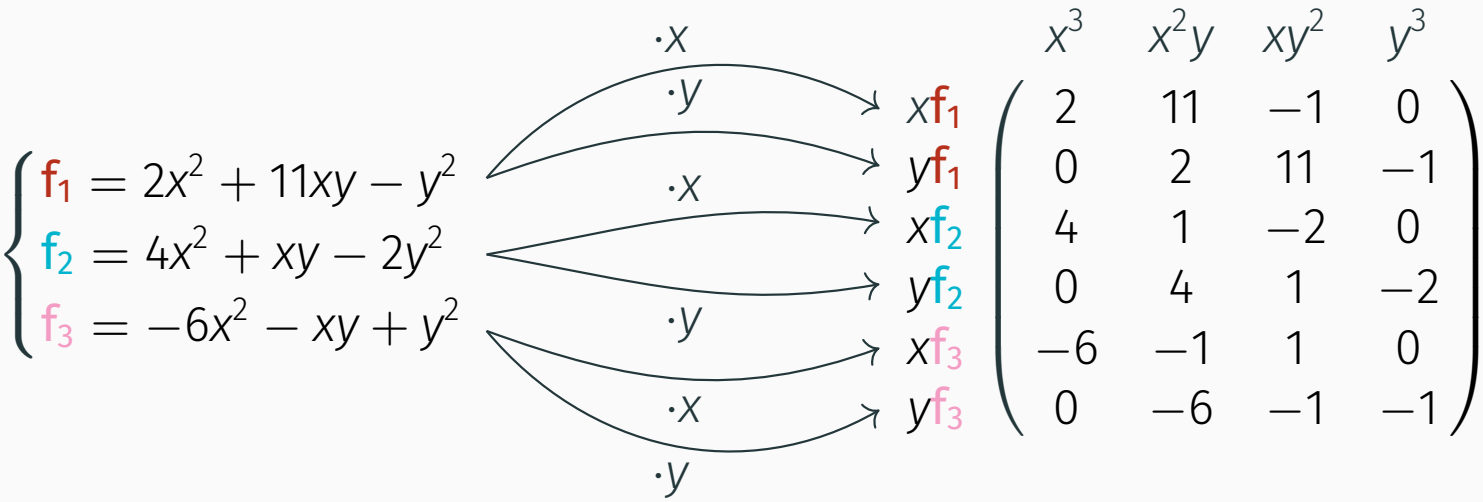
$$\begin{cases} f_1 = 2x^2 + 11xy - y^2 \\ f_2 = 4x^2 + xy - 2y^2 \\ f_3 = -6x^2 - xy + y^2 \end{cases}$$



$$\begin{array}{c} \\ xf_1 \\ yf_1 \\ xf_2 \\ yf_2 \\ xf_3 \\ yf_3 \end{array} \begin{array}{c} \begin{array}{cccc} x^3 & x^2y & xy^2 & y^3 \end{array} \\ \begin{pmatrix} 2 & 11 & -1 & 0 \\ 0 & 2 & 11 & -1 \\ 4 & 1 & -2 & 0 \\ 0 & 4 & 1 & -2 \\ -6 & -1 & 1 & 0 \\ 0 & -6 & -1 & -1 \end{pmatrix} \end{array}$$

Macaulay matrices - linearization

Assume F homogeneous.



Theorem (Macaulay bound, [Lazard, 1983])

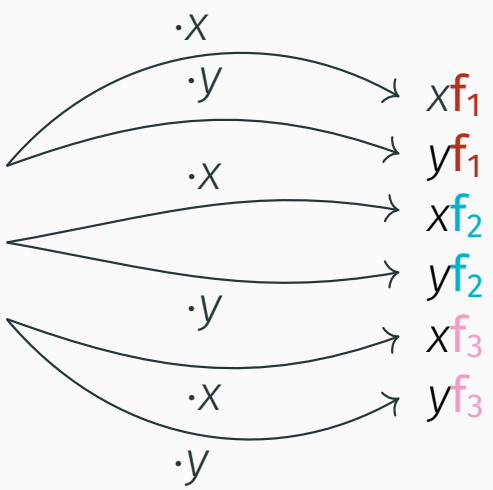
The maximum degree of a polynomial in the ***grevlex*** *Gröbner basis of a generic polynomial system $f_1, \ldots, f_m$ is*

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

Macaulay matrices - linearization

Assume F homogeneous.

$$\begin{cases} f_1 = 2x^2 + 11xy - y^2 \\ f_2 = 4x^2 + xy - 2y^2 \\ f_3 = -6x^2 - xy + y^2 \end{cases}$$



$$\begin{array}{c} \begin{matrix} x^3 & x^2y & xy^2 & y^3 \end{matrix} \\ \begin{pmatrix} 2 & 11 & -1 & 0 \\ 0 & 2 & 11 & -1 \\ 4 & 1 & -2 & 0 \\ 0 & 4 & 1 & -2 \\ -6 & -1 & 1 & 0 \\ 0 & -6 & -1 & -1 \end{pmatrix} \end{array}$$

Theorem (Macaulay bound, [Lazard, 1983])

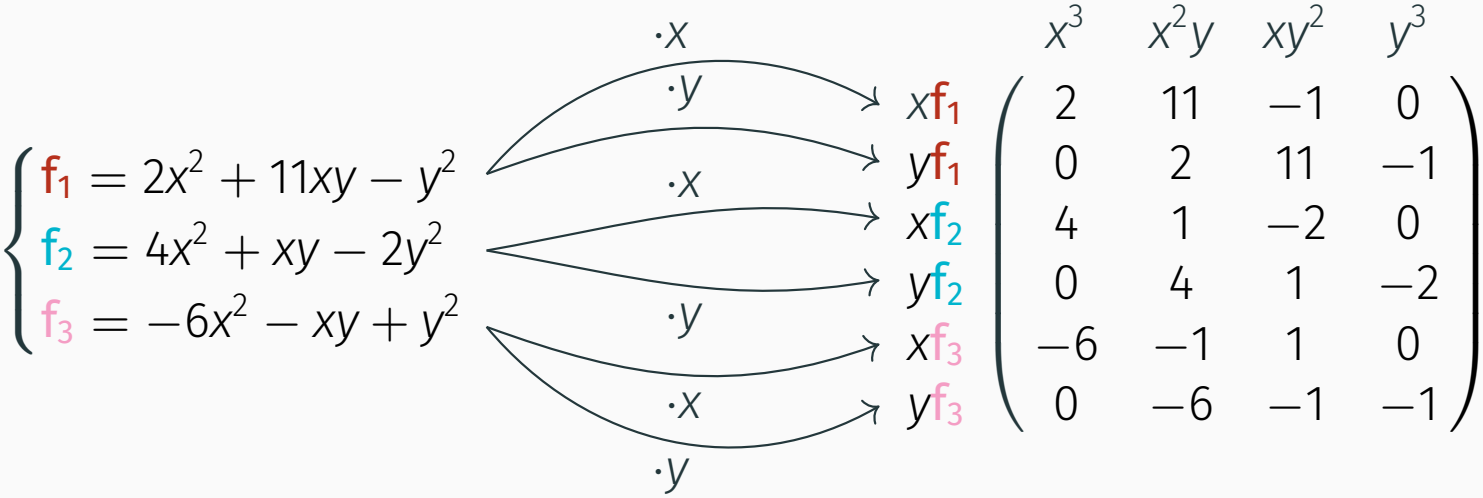
The maximum degree of a polynomial in the ***grevlex*** *Gröbner basis of a generic polynomial system $f_1, \ldots, f_m$ is*

algebraic property: regularity

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

Macaulay matrices - linearization

Assume F homogeneous.



Theorem (Macaulay bound, [Lazard, 1983])

The maximum degree of a polynomial in the ***grevlex*** *Gröbner basis of a generic polynomial system $f_1, \ldots, f_m$ is*

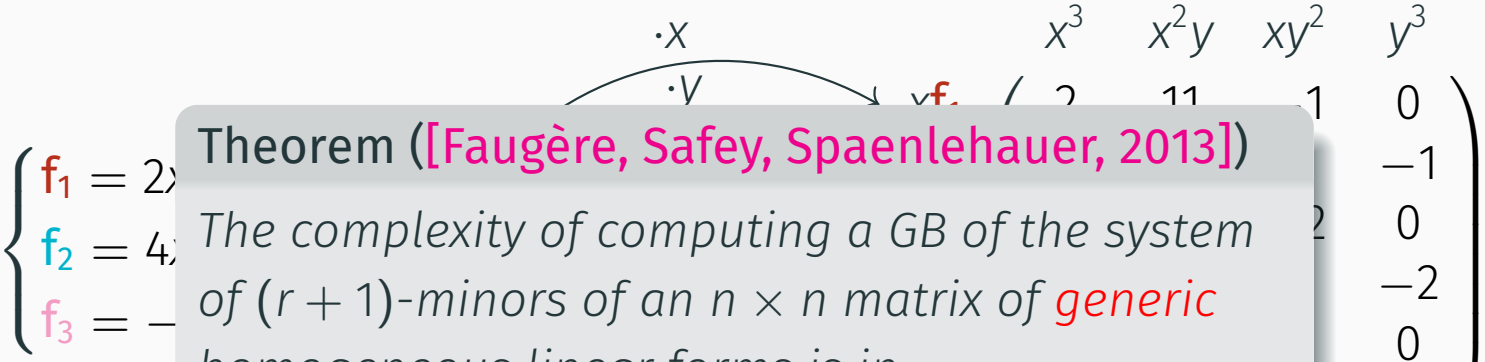
algebraic property: regularity

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

The rows of the echelonization of the Macaulay matrix of F in degree d form the elements of degree d of a $\succ$-Gröbner basis for F.

Macaulay matrices - linearization

Assume F homogeneous.



Theorem ([Faugère, Safey, Spaenlehauer, 2013])

The complexity of computing a GB of the system of $(r+1)$-minors of an $n \times n$ matrix of generic homogeneous linear forms is in

$$O\left(\binom{n}{r+1}^2 \cdot \binom{k+r(n-r)+1}{k}^{\omega}\right).$$

Theorem (Ma

*The maximum degree of a polynomial in the **grevlex** Gröbner basis of a generic polynomial system $f_1, \ldots, f_m$ is*

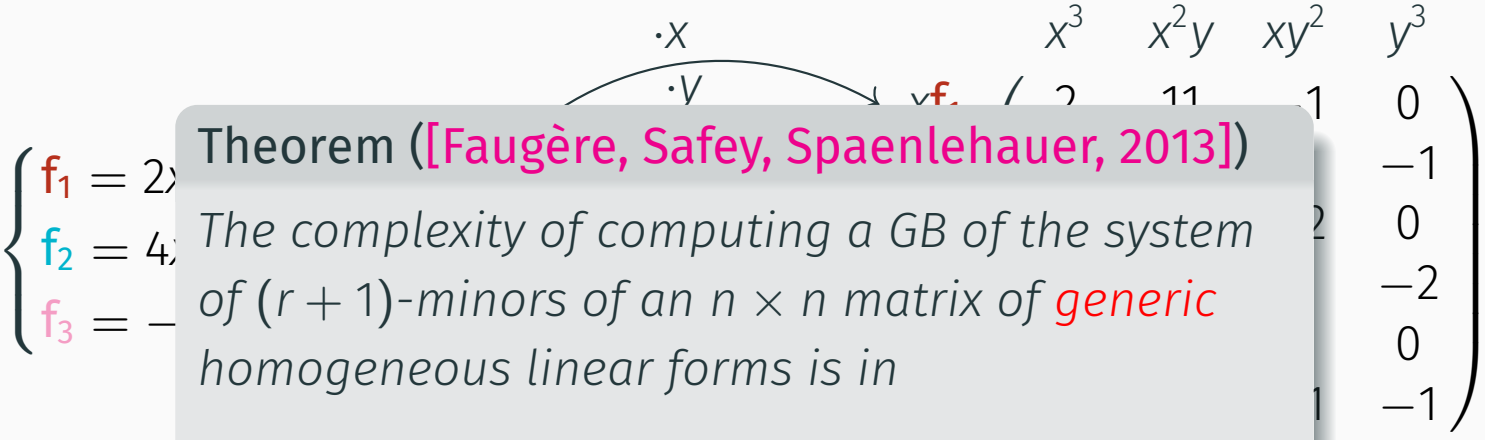
algebraic property: regularity

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

The rows of the echelonization of the Macaulay matrix of F in degree d form the elements of degree d of a $\succ$-Gröbner basis for F.

Macaulay matrices - linearization

Assume F homogeneous.



Theorem ([Faugère, Safey, Spaenlehauer, 2013])

The complexity of computing a GB of the system of $(r+1)$-minors of an $n \times n$ matrix of generic homogeneous linear forms is in

$$O\left(\binom{n}{r+1}^2 \cdot \binom{k+r(n-r)+1}{k}^{\omega}\right).$$

Theorem (Ma

*The maximum degree of a polynomial in the **grevlex** Gröbner basis of a generic polynomial system $f_1, \ldots, f_m$ is*

alge
prop
regu

This upper bound is not very sharp since the Macaulay matrices are not full rank!

The rows of the echelonization of the Macaulay matrix of F in degree d form the elements of degree d of a $\succ$-Gröbner basis for F.

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$$\widetilde{\mathcal{M}_2}$$

$$\begin{array}{c} \\ (1,1) \\ (2,1) \\ (3,1) \end{array} \begin{array}{c} \begin{array}{cccccc} x^2 & xy & y^2 & xz & yz & z^2 \end{array} \\ \begin{pmatrix} 1 & 1 & 2 & 1 & 1 & 4 \\ 0 & 1 & 0 & 0 & 2 & 4 \\ 0 & 0 & 1 & 2 & 0 & 4 \end{pmatrix} \end{array}$$

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$\widetilde{\mathcal{M}_2}$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$\widetilde{\mathcal{M}_2}$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$\widetilde{\mathcal{M}_2}$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$\widetilde{\mathcal{M}_2}$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$\widetilde{\mathcal{M}_2}$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$\widetilde{\mathcal{M}}_2$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$\widetilde{\mathcal{M}_2}$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

Lazard: $\mathcal{M}_4$ is 18×15.

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$\widetilde{\mathcal{M}_2}$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

Lazard: $\mathcal{M}_4$ is 18×15.

F5: $\mathcal{M}_4$ is 15×15 and full rank!

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ$ = grevlex.

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$(f_1, \ldots, f_m)$ generic

$\widetilde{\mathcal{M}_2}$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

Lazard: $\mathcal{M}_4$ is 18×15.

F5: $\mathcal{M}_4$ is 15×15 and full rank!

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$(f_1, \ldots, f_m)$ generic

$\Downarrow$

$\widetilde{\mathcal{M}_2}$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

Lazard: $\mathcal{M}_4$ is 18×15.

F5: $\mathcal{M}_4$ is 15×15 and full rank!

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ =$ grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$(f_1, \ldots, f_m)$ generic

$\Downarrow$

No reductions to zero.

$\widetilde{\mathcal{M}_2}$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

Lazard: $\mathcal{M}_4$ is 18×15.

F5: $\mathcal{M}_4$ is 15×15 and full rank!

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ$ = grevlex .

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$
$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$
$$f_3 = 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2$$

$(f_1, \ldots, f_m)$ generic

$\Downarrow$

- **No** reductions to zero.
- Precise complexity analysis [1]

$\widetilde{\mathcal{M}_2}$

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

Lazard: $\mathcal{M}_4$ is 18×15.

F5: $\mathcal{M}_4$ is 15×15 and full rank!

$\mathcal{M}_4$

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

[1] [Bardet, Faugère, Salvy, 2015]

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ$ = grevlex.

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$

$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$

$$f_3 = 4x^2 + xy + \cdots$$

$$\widetilde{\mathcal{M}_2}$$

$(f_1, \ldots, f_m)$ generic

$\Downarrow$

zero.

y analysis [1]

Determinantal systems are not generic!

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0	0	2	4
$(3,1)$	0	0	1	2	0	4

Lazard: $\mathcal{M}_4$ is 18×15.

F5: $\mathcal{M}_4$ is 15×15 and full rank!

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
$(1,xz)$	0	0	0	0	0	5	5	3	0	5	5	0	6	0	0
$(1,yz)$	0	0	0	0	0	0	5	5	3	0	5	5	0	6	0
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

[1] [Bardet, Faugère, Salvy, 2015]

The F_5 algorithm ([Faugère, 2002])

Let $\mathbb{k} = \mathbb{F}_7$, $\succ$ = grevlex.

$$f_1 = 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2$$

$$f_2 = 2x^2 + xy + 4y^2 + 2xz + 4z^2$$

$$f_3 = 4x^2 + xy + \cdots$$

$$\widetilde{\mathcal{M}_2}$$

$(f_1, \ldots, f_m)$ generic

$\Downarrow$

zero.

y analysis [1]

Determinantal systems are not generic!

How do we remove reductions to zero?

	x^2	xy	y^2	xz	yz	z^2
$(1,1)$	1	1	2	1	1	4
$(2,1)$	0	1	0			
$(3,1)$	0	0	1			

	x^4	x^3y	x^2y^2	xy^3	y^4	x^3z	x^2yz	xy^2z	y^3z	x^2z^2	xyz^2	y^2z^2	xz^3	yz^3	z^4
$(1,x^2)$	5	5	3	0	0	5	5	0	0	6	0	0	0	0	0
$(1,xy)$	0	5	5	3	0	0	5	5	0	0	6	0	0	0	0
$(1,y^2)$	0	0	5	5	3	0	0	5	5	0	0	6	0	0	0
									5	5	0	6	0	0	
									0	5	5	0	6	0	
$(1,z^2)$	0	0	0	0	0	0	0	0	0	5	5	3	5	5	6
$(2,x^2)$	2	1	4	0	0	2	0	0	0	4	0	0	0	0	0
$(2,xy)$	0	2	1	4	0	0	2	0	0	0	4	0	0	0	0
$(2,y^2)$	0	0	2	1	4	0	0	2	0	0	0	4	0	0	0
$(2,xz)$	0	0	0	0	0	2	1	4	0	2	0	0	4	0	0
$(2,yz)$	0	0	0	0	0	0	2	1	4	0	2	0	0	4	0
$(2,z^2)$	0	0	0	0	0	0	0	0	0	2	1	4	2	0	4
$(3,x^2)$	4	1	4	0	0	3	5	0	0	2	0	0	0	0	0
$(3,xy)$	0	4	1	4	0	0	3	5	0	0	2	0	0	0	0
$(3,y^2)$	0	0	4	1	4	0	0	3	5	0	0	2	0	0	0
$(3,xz)$	0	0	0	0	0	4	1	4	0	3	5	0	2	0	0
$(3,yz)$	0	0	0	0	0	0	4	1	4	0	3	5	0	2	0
$(3,z^2)$	0	0	0	0	0	0	0	0	0	4	1	4	3	5	2

Lazard: $\mathcal{M}_4$ is 18×15.

F5: $\mathcal{M}_4$ is 15×15 and full rank!

[1] [Bardet, Faugère, Salvy, 2015]

Contributions ([G., Neiger, Safey El Din, 2023])

Contributions ([G., Neiger, Safey El Din, 2023])

M is an $n \times n$ matrix of generic linear forms over $\mathbb{k}[x_1, \ldots, x_k]$, $r \leq n-1$. Let $F_r(M)$ be the system of $(r+1)$-minors of M. Suppose $F_r(M)$ is zero-dimensional.

Contributions ([G., Neiger, Safey El Din, 2023])

M is an $n \times n$ matrix of generic linear forms over $\mathbb{k}[x_1, \ldots, x_k]$, $r \leq n-1$. Let $F_r(M)$ be the system of $(r+1)$-minors of M. Suppose $F_r(M)$ is zero-dimensional.

New F_5-type criteria

- Allows us to avoid all reductions to zero in degree $r+2$

$$\rightsquigarrow \binom{n}{r+2}^2 \left(\frac{2(r+2)(r+1)}{n-r-1} + 2r + 2 \right) \text{ reductions avoided.}$$

Contributions ([G., Neiger, Safey El Din, 2023])

M is an $n \times n$ matrix of generic linear forms over $\mathbb{k}[x_1, \ldots, x_k]$, $r \leq n-1$. Let $F_r(M)$ be the system of $(r+1)$-minors of M. Suppose $F_r(M)$ is zero-dimensional.

New F_5-type criteria

- Allows us to avoid all reductions to zero in degree $r+2$

$$\rightsquigarrow \binom{n}{r+2}^2 \left(\frac{2(r+2)(r+1)}{n-r-1} + 2r + 2 \right) \text{ reductions avoided.}$$

- When $r = n-2$, allows us to avoid **all** reductions to zero.

Contributions ([G., Neiger, Safey El Din, 2023])

M is an $n \times n$ matrix of generic linear forms over $\mathbb{k}[x_1, \ldots, x_k]$, $r \leq n-1$. Let $F_r(M)$ be the system of $(r+1)$-minors of M. Suppose $F_r(M)$ is zero-dimensional.

New F_5-type criteria

- Allows us to avoid all reductions to zero in degree $r+2$

$$\rightsquigarrow \binom{n}{r+2}^2 \left(\frac{2(r+2)(r+1)}{n-r-1} + 2r + 2 \right) \text{ reductions avoided.}$$

- When $r = n-2$, allows us to avoid **all** reductions to zero.

Contributions ([G., Neiger, Safey El Din, 2023])

M is an $n \times n$ matrix of generic linear forms over $\mathbb{k}[x_1, \ldots, x_k]$, $r \leq n-1$. Let $F_r(M)$ be the system of $(r+1)$-minors of M. Suppose $F_r(M)$ is zero-dimensional.

New F_5-type criteria

- Allows us to avoid all reductions to zero in degree $r+2$

$$\rightsquigarrow \binom{n}{r+2}^2 \left(\frac{2(r+2)(r+1)}{n-r-1} + 2r + 2 \right) \text{ reductions avoided.}$$

- When $r = n-2$, allows us to avoid **all** reductions to zero.

Theorem ([G., Neiger, Safey El Din, 2023])

The complexity of computing a grevlex Gröbner basis for the system of $(n-1)$-minors of M is in

Homogeneous: $O(n^{4\omega-1})$

Affine: $O(n^{4\omega})$

Contributions ([G., Neiger, Safey El Din, 2023])

M is an $n \times n$ matrix of generic linear forms over $\mathbb{k}[x_1, \ldots, x_k]$, $r \leq n-1$. Let $F_r(M)$ be the system of $(r+1)$-minors of M. Suppose $F_r(M)$ is zero-dimensional.

New F_5-type criteria

- Allows us to avoid all reductions to zero in degree $r+2$

$$\rightsquigarrow \binom{n}{r+2}^2 \left(\frac{2(r+2)(r+1)}{n-r-1} + 2r + 2 \right) \text{ reductions avoided.}$$

- When $r = n-2$, allows us to avoid **all** reductions to zero.

Theorem ([G., Neiger, Safey El Din, 2023])

The complexity of computing a grevlex Gröbner basis for the system of $(n-1)$-minors of M is in

Homogeneous: $O(n^{4\omega-1}) \rightsquigarrow O(n^{2\omega+3})$ *and* $|GB| \in \Omega(n^6)$ *conjecturally*

Affine: $O(n^{4\omega})$

Syzygies

Definition (Syzygy)

$(a_1, \ldots, a_m) \in \Bbbk[x_1, \ldots, x_k]^m$ with

$$a_1 f_1 + \cdots + a_m f_m = 0$$

is called a **syzygy** of $f_1, \ldots, f_m$.

Syzygies

Definition (Syzygy)

$(a_1, \ldots, a_m) \in \mathbb{k}[x_1, \ldots, x_k]^m$ with

$$a_1 f_1 + \cdots + a_m f_m = 0$$

is called a **syzygy** of $f_1, \ldots, f_m$.

Example (Koszul syzygies)

$$f_i = \mathrm{LT}(f_i) + \mathrm{tail}(f_i)$$

$$\Downarrow$$

$$\mathrm{LT}(f_i) f_j = f_j f_i - \mathrm{tail}(f_i) f_j$$

Syzygies

Definition (Syzygy)

$(a_1, \ldots, a_m) \in \mathbb{k}[x_1, \ldots, x_k]^m$ with

$$a_1 f_1 + \cdots + a_m f_m = 0$$

is called a **syzygy** of $f_1, \ldots, f_m$.

Example (Koszul syzygies)

$$f_i = \mathrm{LT}(f_i) + \mathrm{tail}(f_i)$$

$$\Downarrow$$

$$\underbrace{\mathrm{LT}(f_i) f_j}_{\substack{\text{row of} \\ \text{Macaulay} \\ \text{matrix}}} = f_j f_i - \mathrm{tail}(f_i) f_j$$

Syzygies

Definition (Syzygy)

$(a_1, \ldots, a_m) \in \mathbb{k}[x_1, \ldots, x_k]^m$ with

$$a_1 f_1 + \cdots + a_m f_m = 0$$

is called a **syzygy** of $f_1, \ldots, f_m$.

Example (Koszul syzygies)

$$f_i = \mathrm{LT}(f_i) + \mathrm{tail}(f_i)$$

$$\Downarrow$$

$$\underbrace{\mathrm{LT}(f_i) f_j}_{\substack{\text{row of} \\ \text{Macaulay} \\ \text{matrix}}} = \underbrace{f_j f_i - \mathrm{tail}(f_i) f_j}_{\substack{\text{combination of} \\ \text{rows of} \\ \text{Macaulay matrix}}}$$

Syzygies

Definition (Syzygy)

$(a_1, \ldots, a_m) \in \mathbb{k}[x_1, \ldots, x_k]^m$ with

$$a_1 f_1 + \cdots + a_m f_m = 0$$

is called a **syzygy** of $f_1, \ldots, f_m$.

Example (Koszul syzygies)

$$f_i = \mathrm{LT}(f_i) + \mathrm{tail}(f_i)$$

$$\Downarrow$$

$$\underbrace{\mathrm{LT}(f_i) f_j}_{\substack{\text{row of} \\ \text{Macaulay} \\ \text{matrix}}} = \underbrace{f_j f_i - \mathrm{tail}(f_i) f_j}_{\substack{\text{combination of} \\ \text{rows of} \\ \text{Macaulay matrix}}}$$

Syzygies

Definition (Syzygy)

$(a_1, \ldots, a_m) \in \mathbb{k}[x_1, \ldots, x_k]^m$ with

$$a_1 f_1 + \cdots + a_m f_m = 0$$

is called a **syzygy** of $f_1, \ldots, f_m$.

Example (Koszul syzygies)

$$f_i = \mathrm{LT}(f_i) + \mathrm{tail}(f_i)$$

$$\Downarrow$$

$$\underbrace{\mathrm{LT}(f_i) f_j}_{\substack{\text{row of} \\ \text{Macaulay} \\ \text{matrix}}} = \underbrace{f_j f_i - \mathrm{tail}(f_i) f_j}_{\substack{\text{combination of} \\ \text{rows of} \\ \text{Macaulay matrix}}}$$

Theorem ([Hilbert, 1890])

Free resolution $0 \to \mathcal{E}_\ell \xrightarrow{d_\ell} \mathcal{E}_{\ell-1} \xrightarrow{d_{\ell-1}} \cdots \to \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F \rangle \to 0 \implies$

$$\mathrm{Syz}_k(F) = \ker(d_k) = \mathrm{im}(d_{k+1}).$$

The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.

The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix}$$

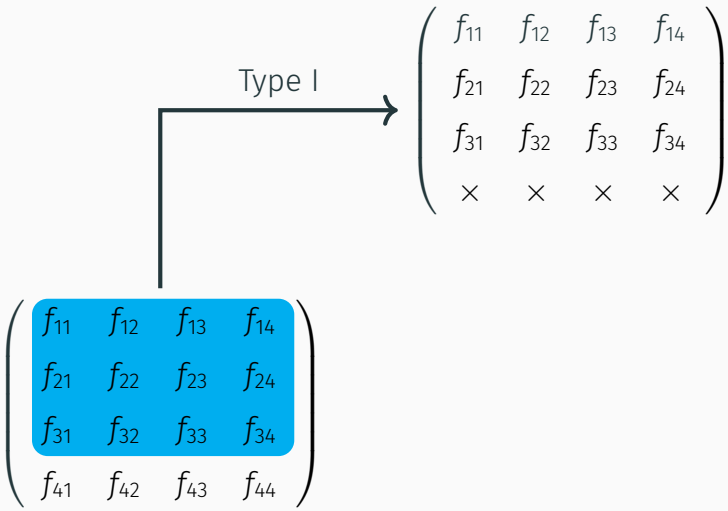
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix}$$

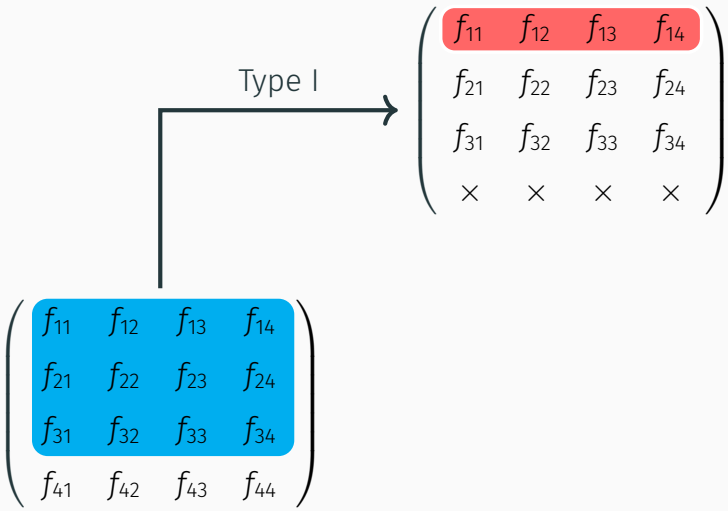
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



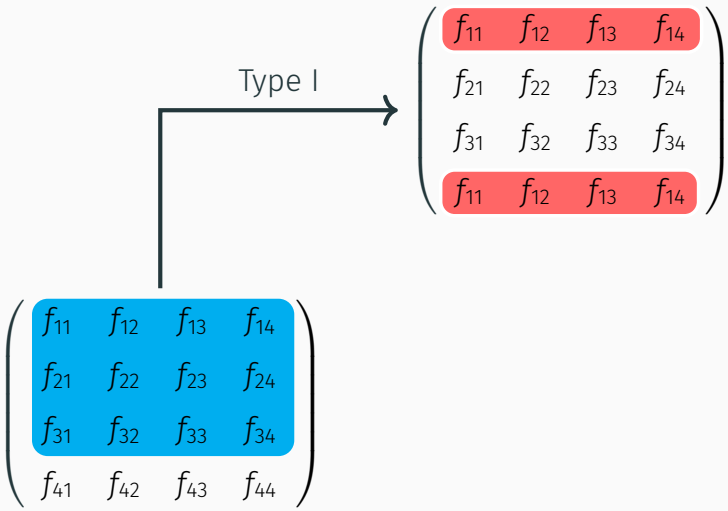
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



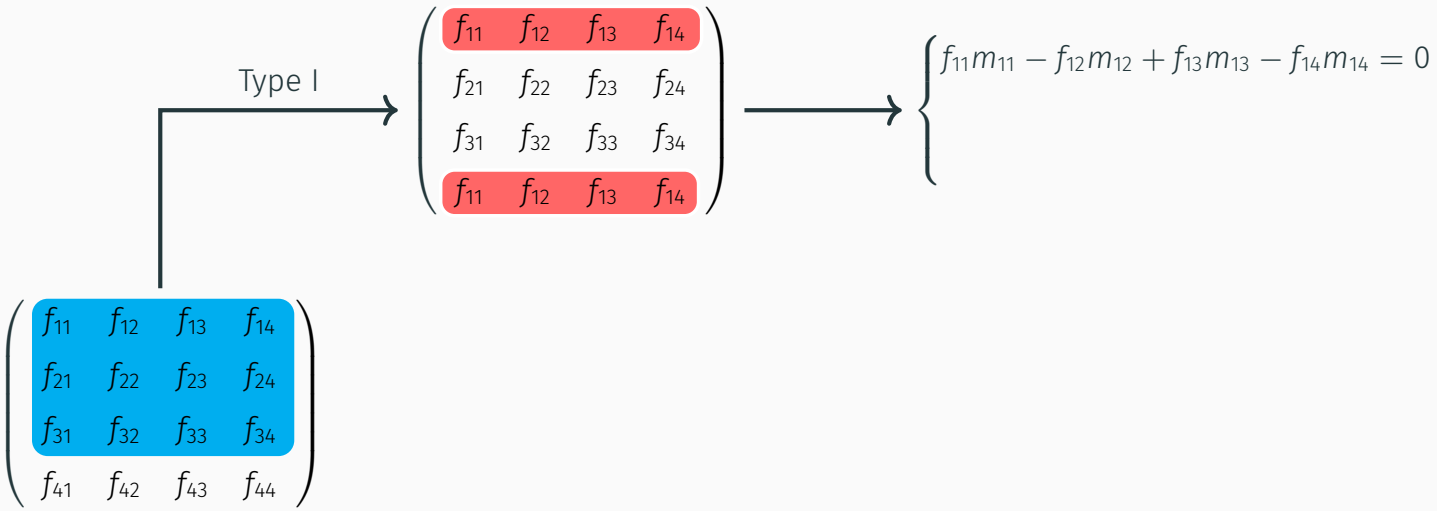
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



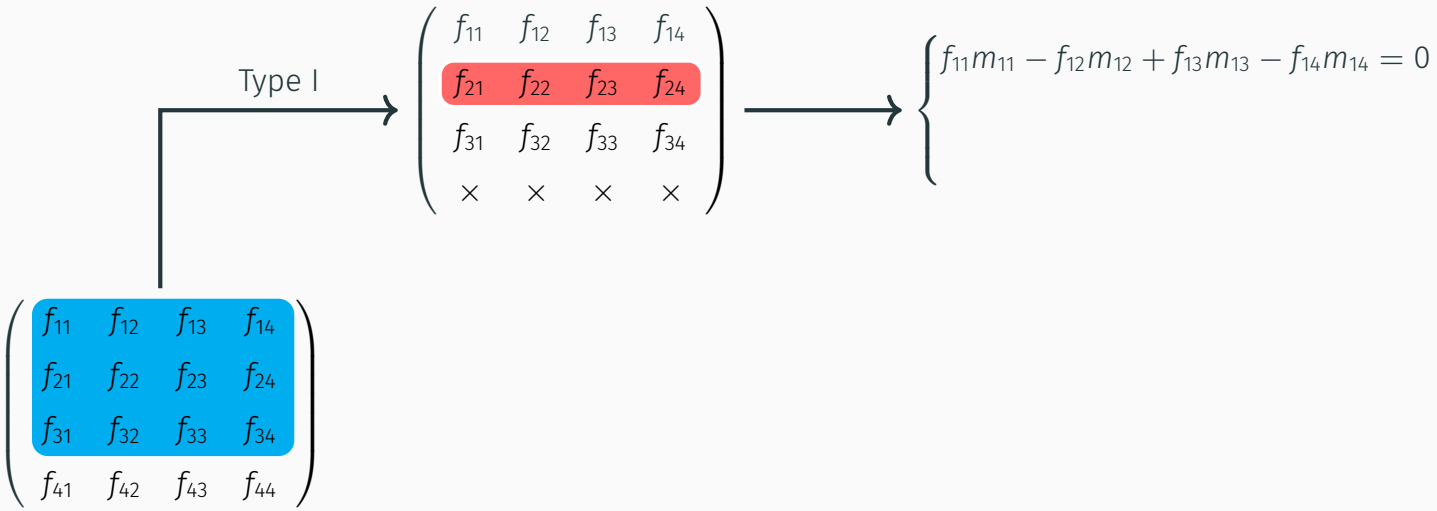
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



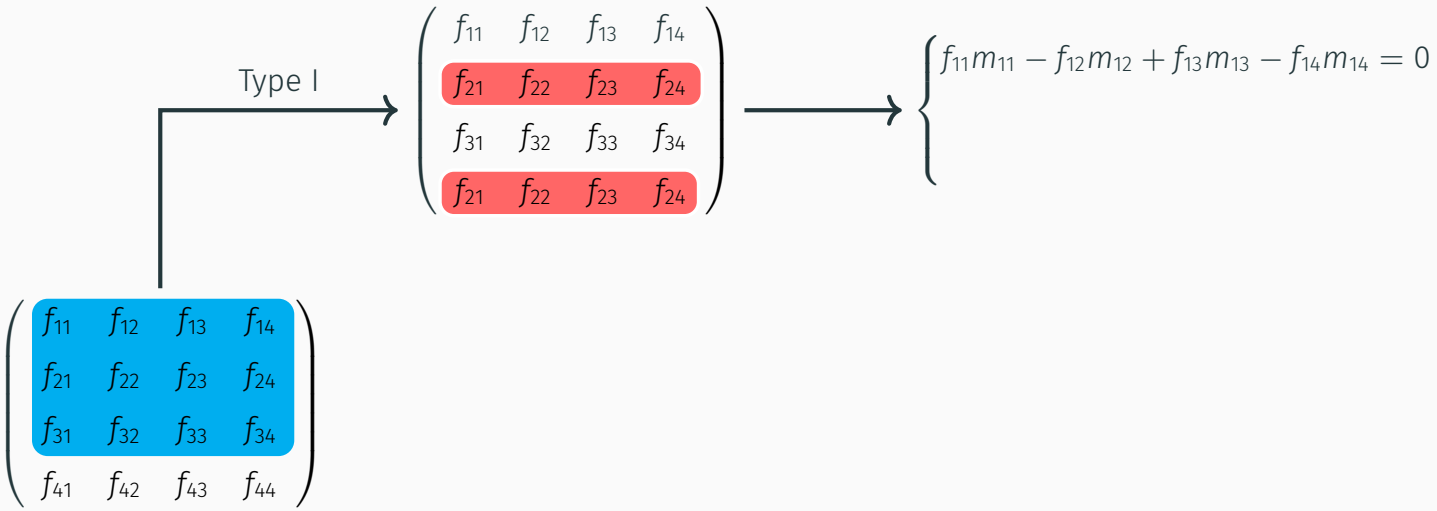
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



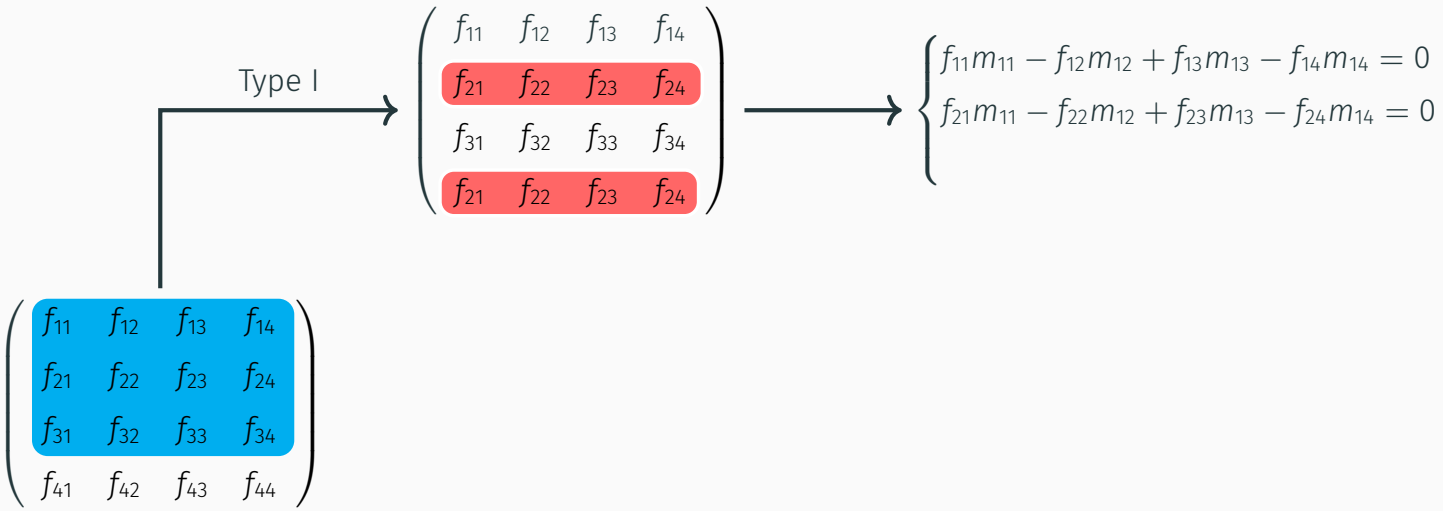
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



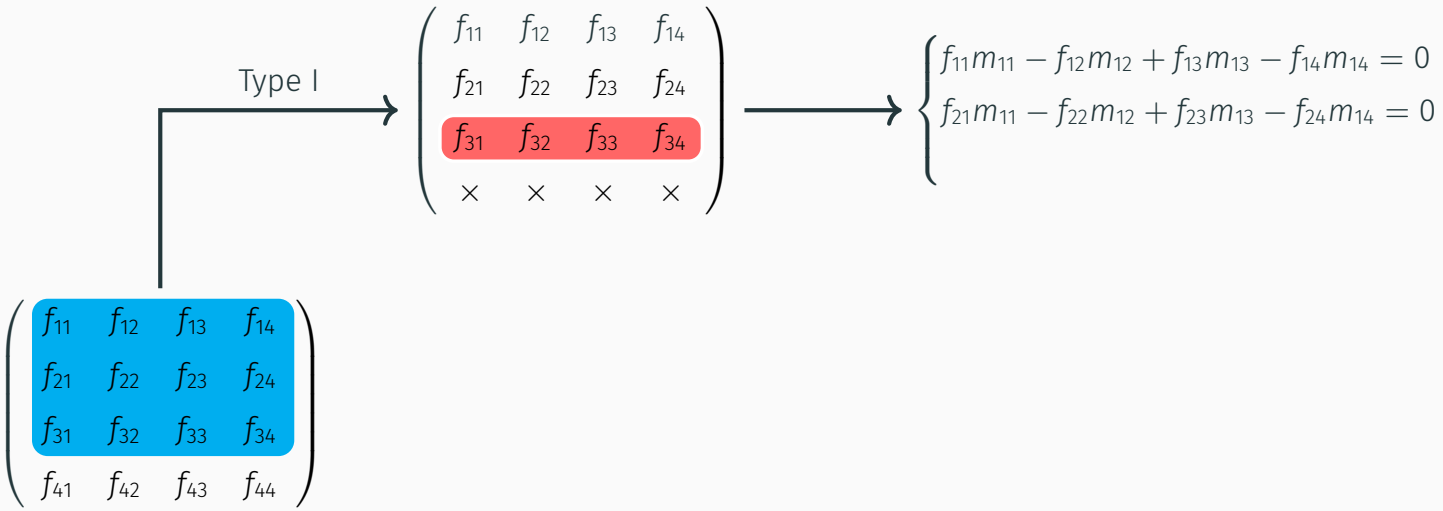
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



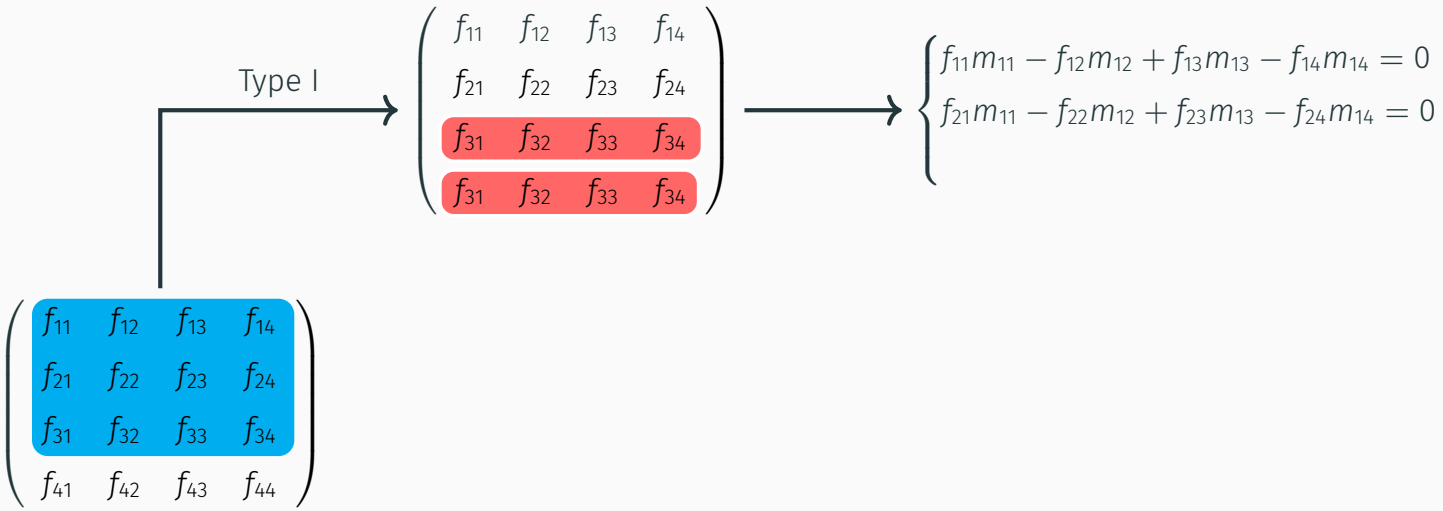
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



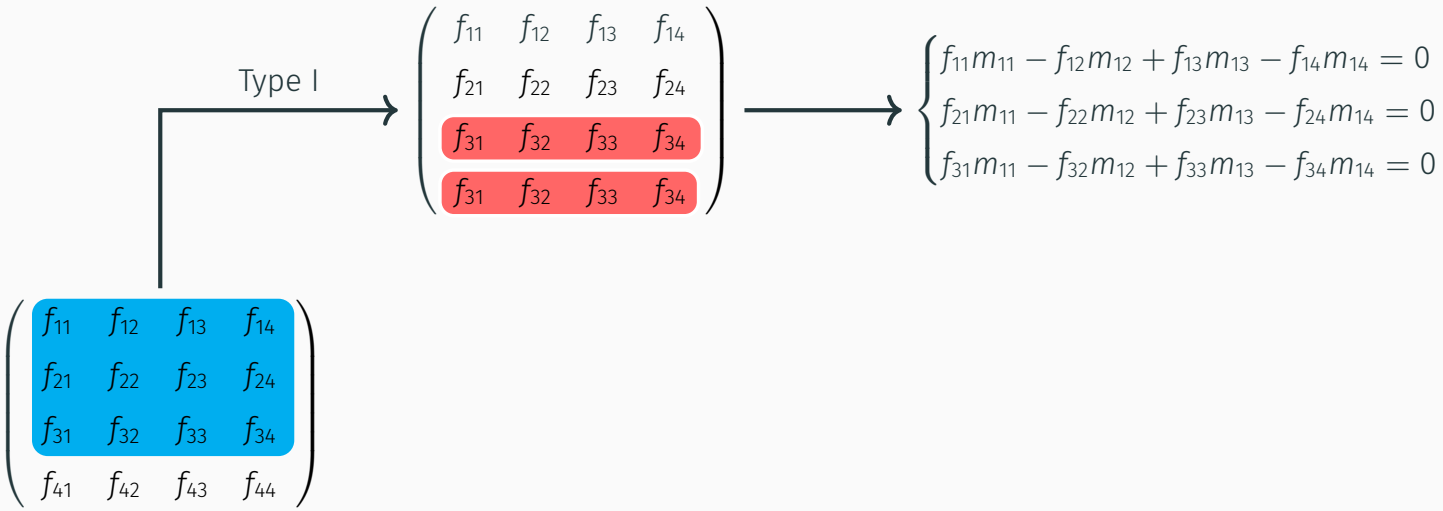
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



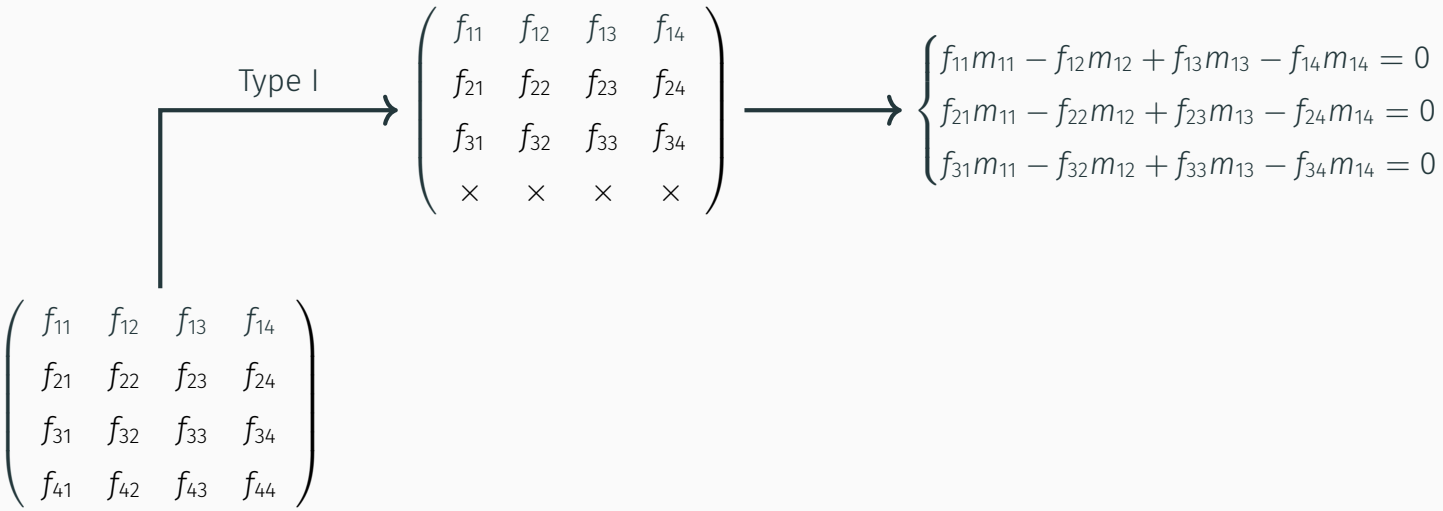
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



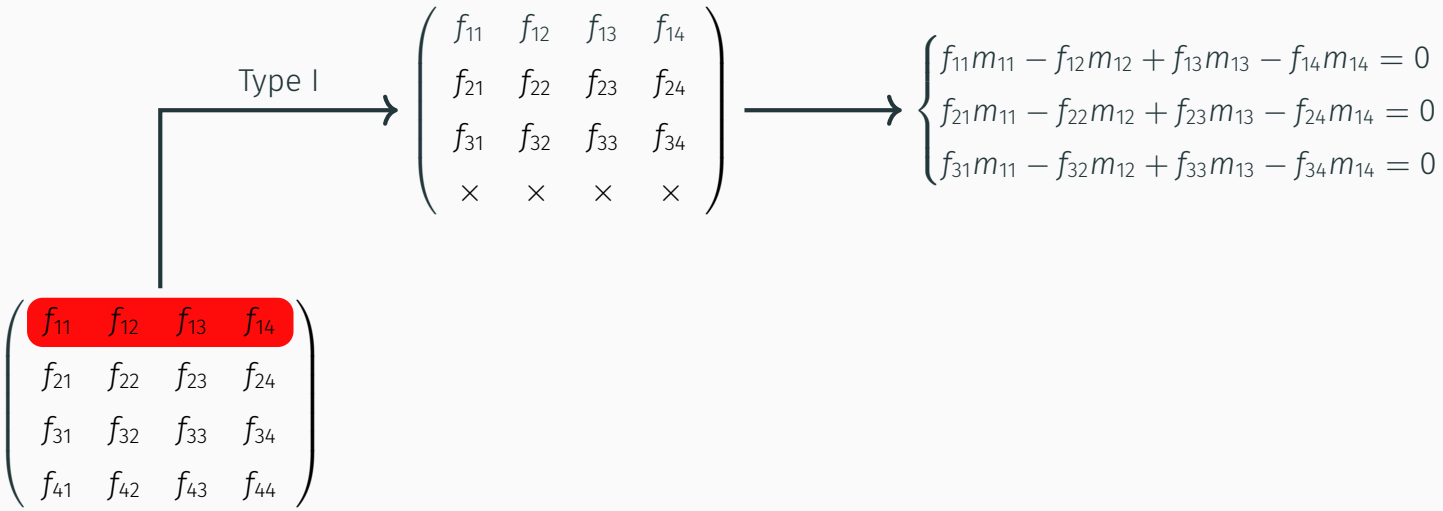
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



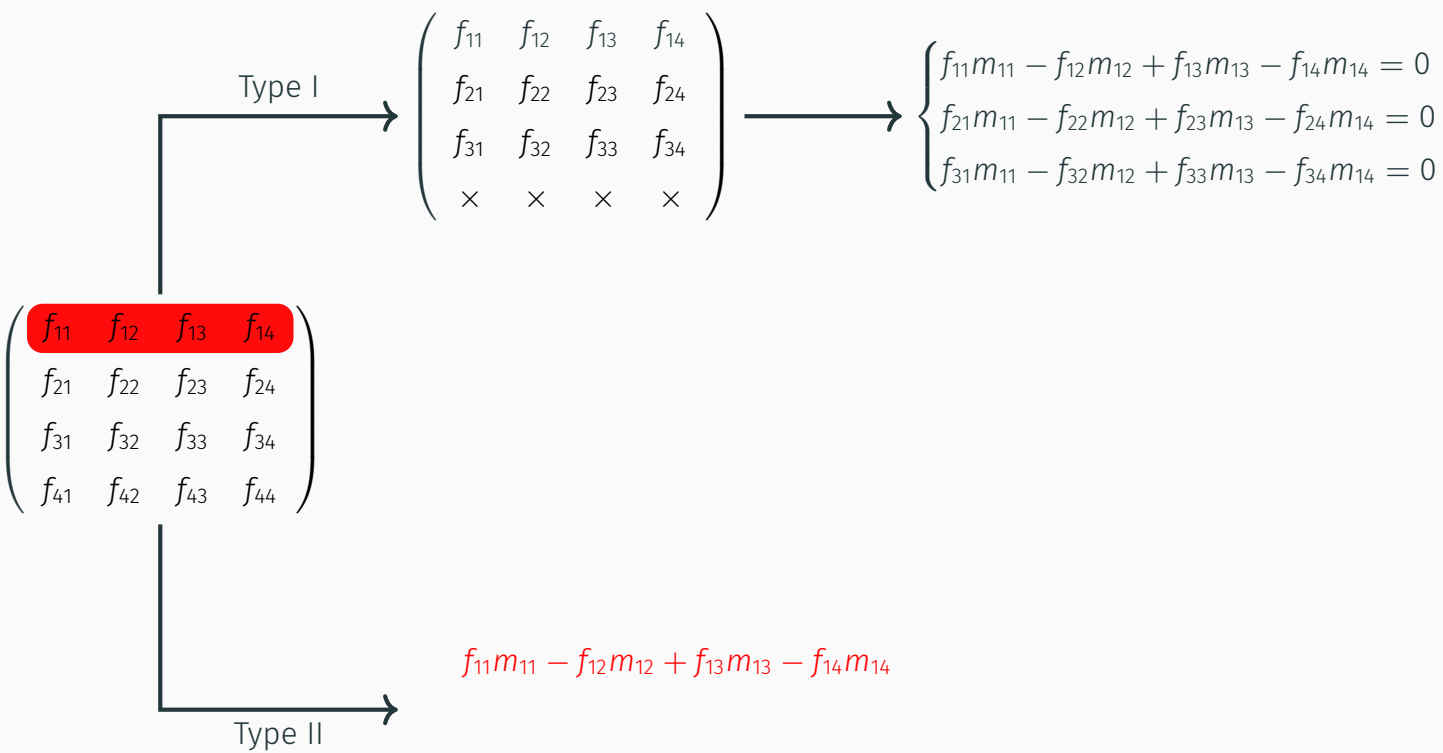
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



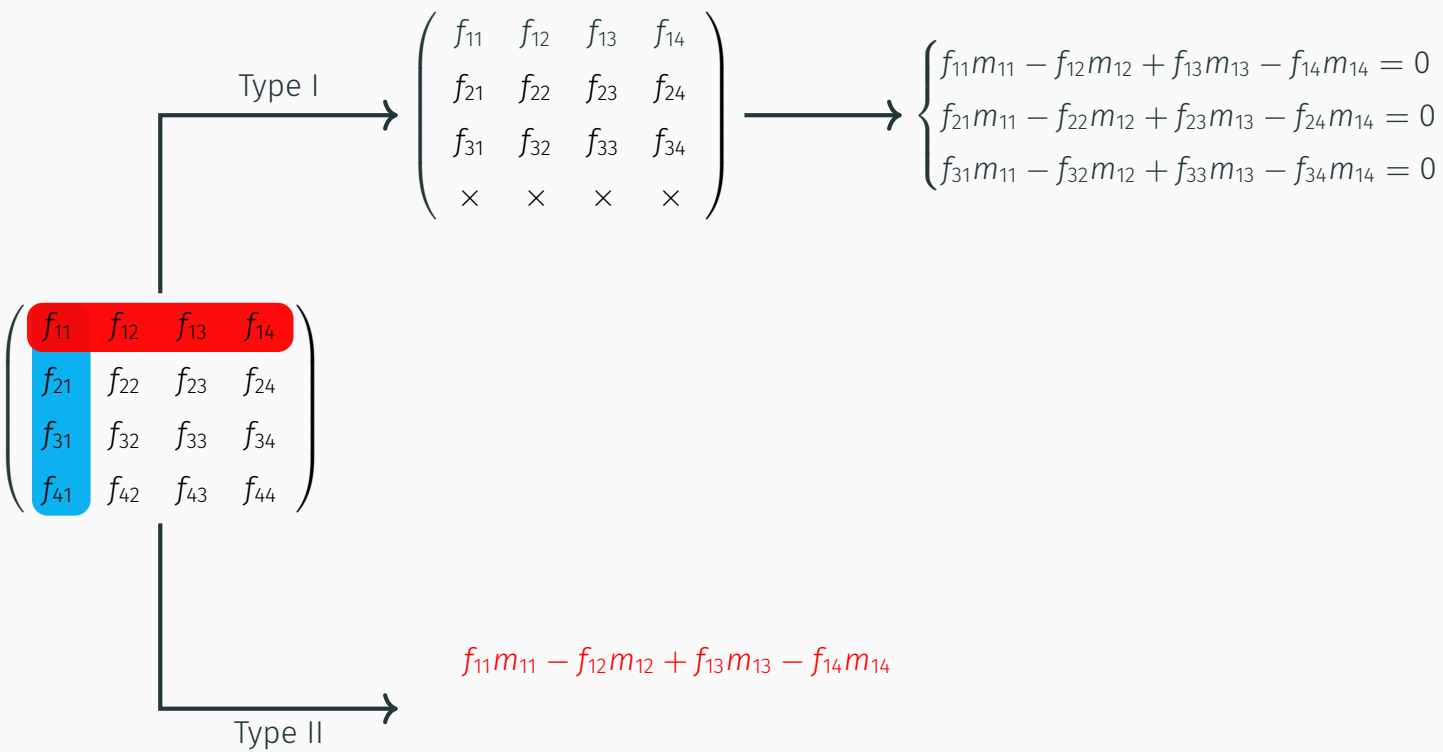
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



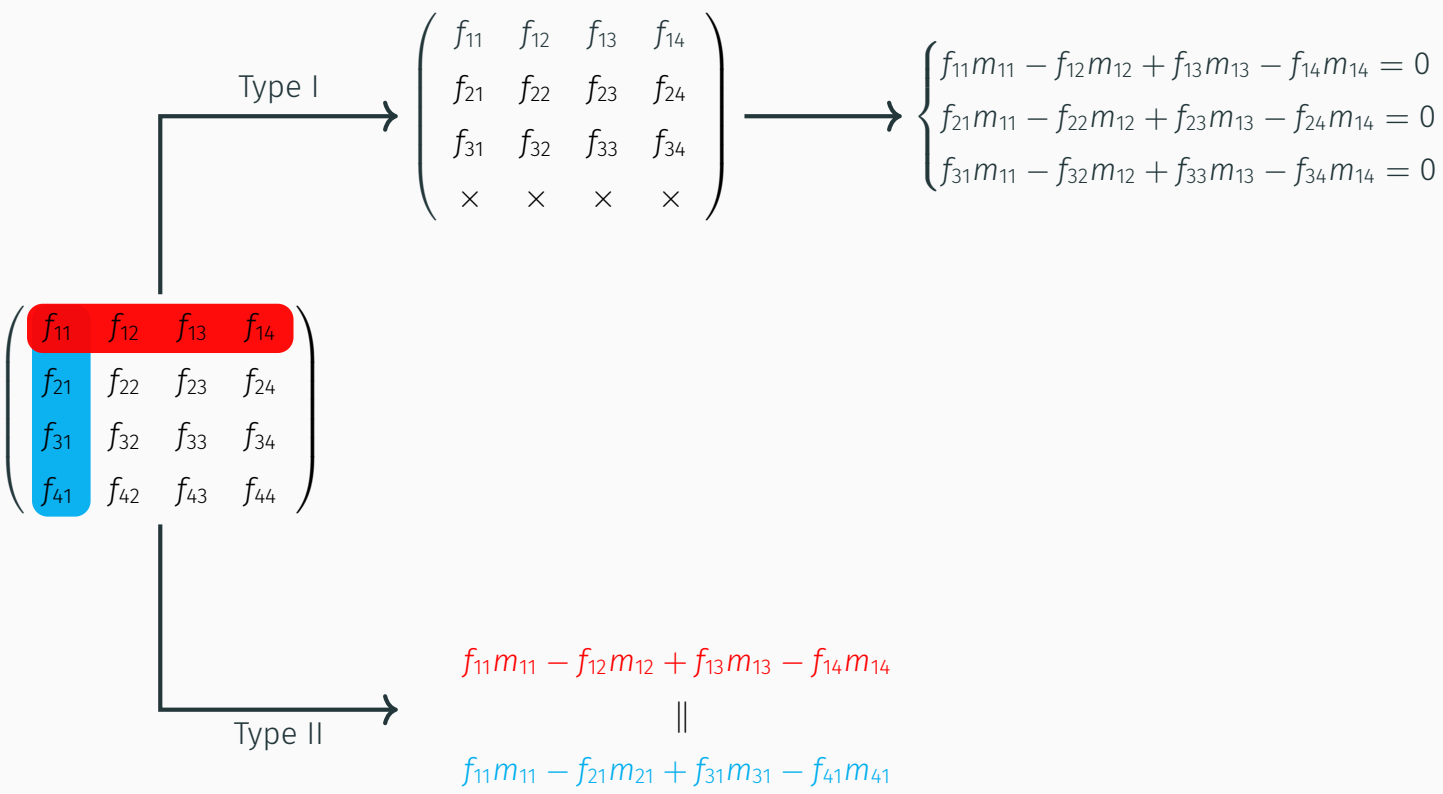
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



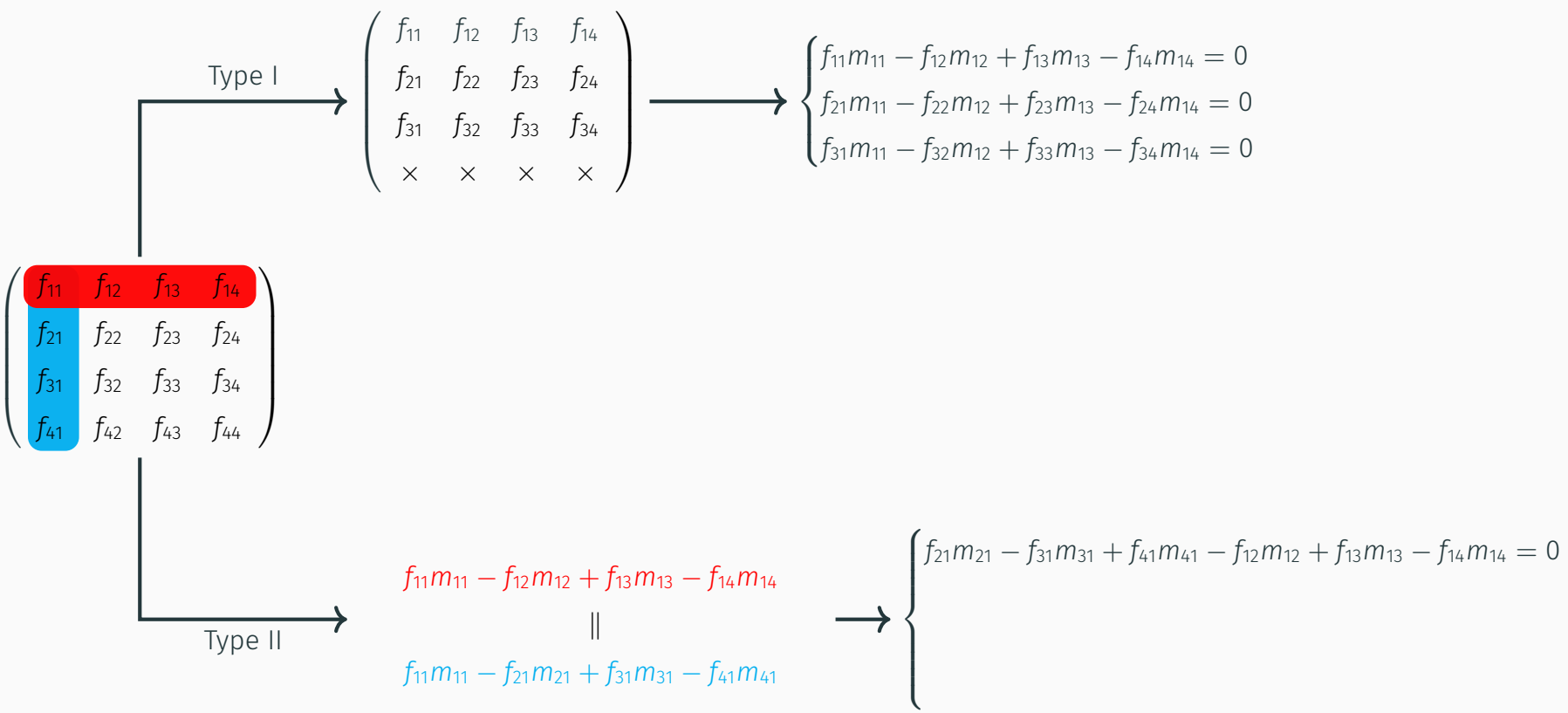
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



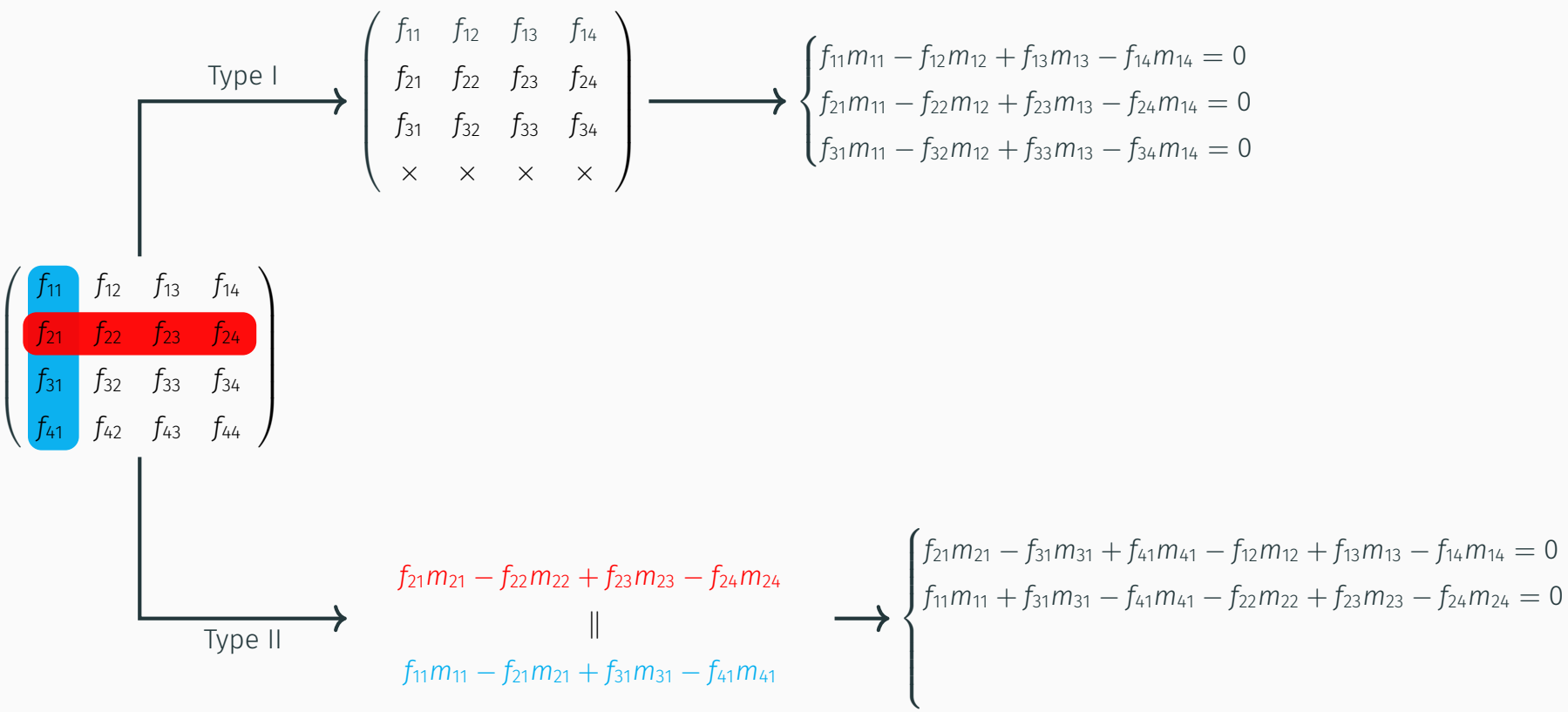
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



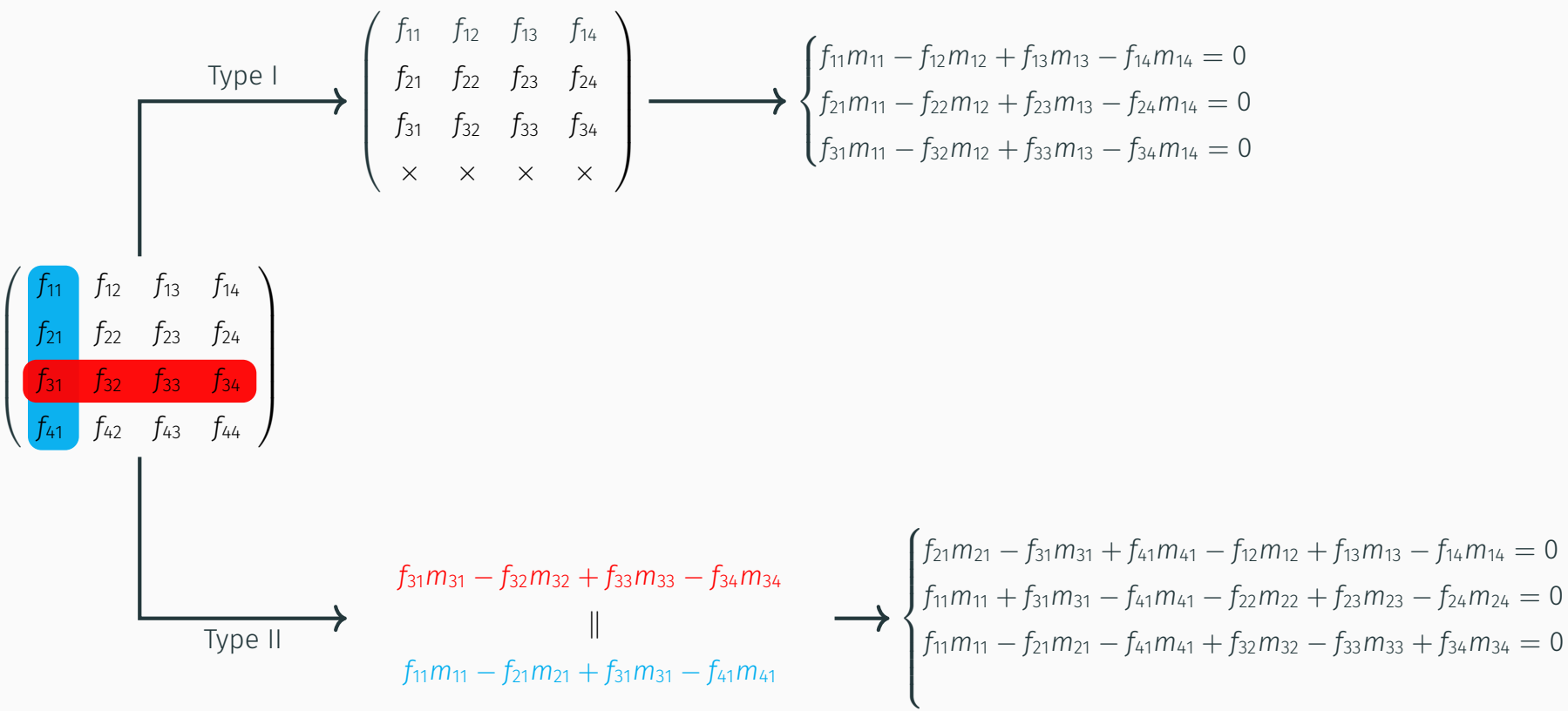
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



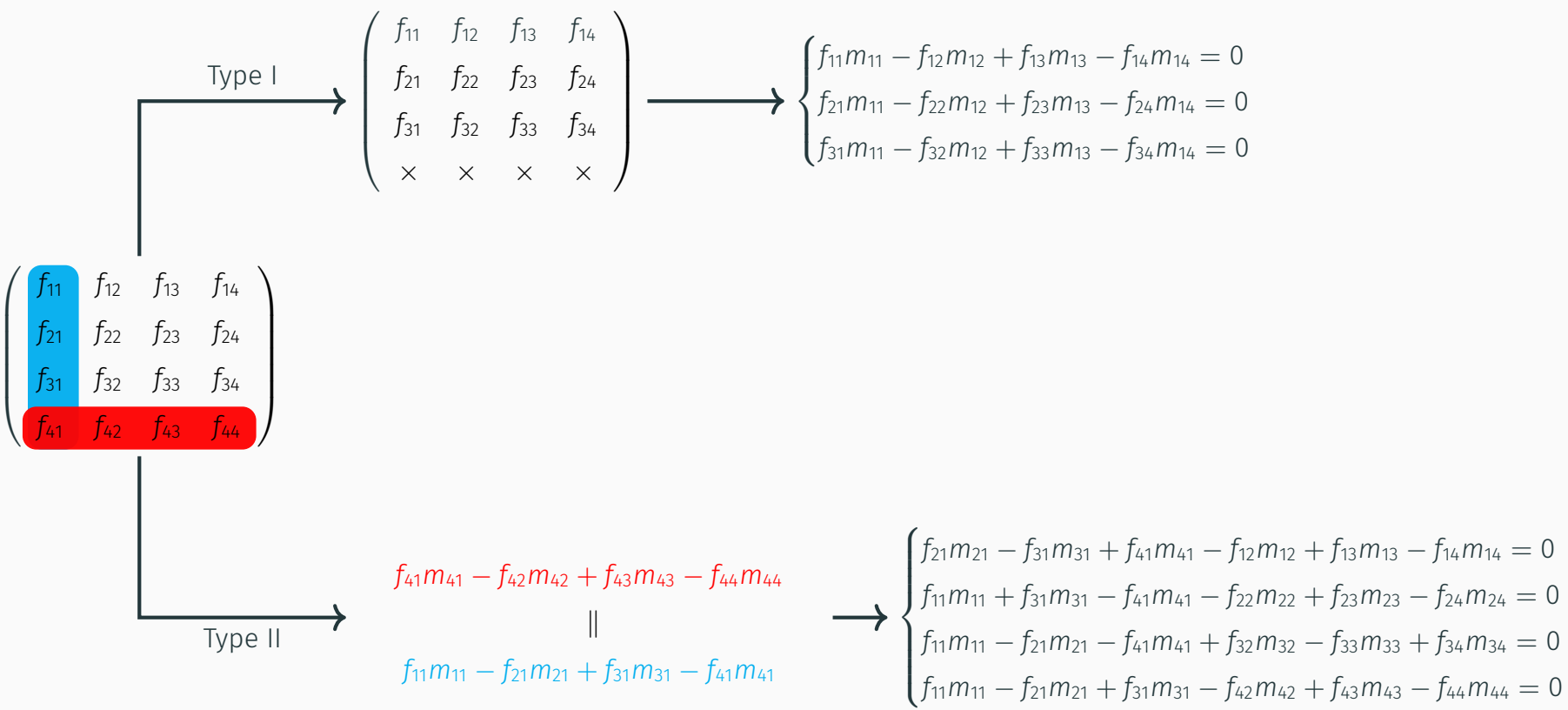
The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix}$$

Type I →

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ \times & \times & \times & \times \end{pmatrix} \longrightarrow \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ f_{31}m_{11} - f_{32}m_{12} + f_{33}m_{13} - f_{34}m_{14} = 0 \end{cases}$$

Type II →

$$f_{41}m_{41} - f_{42}m_{42} + f_{43}m_{43} - f_{44}m_{44}$$
$$\| $$
$$f_{11}m_{11} - f_{21}m_{21} + f_{31}m_{31} - f_{41}m_{41}$$

$$\longrightarrow \begin{cases} f_{21}m_{21} - f_{31}m_{31} + f_{41}m_{41} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{11}m_{11} + f_{31}m_{31} - f_{41}m_{41} - f_{22}m_{22} + f_{23}m_{23} - f_{24}m_{24} = 0 \\ f_{11}m_{11} - f_{21}m_{21} - f_{41}m_{41} + f_{32}m_{32} - f_{33}m_{33} + f_{34}m_{34} = 0 \\ f_{11}m_{11} - f_{21}m_{21} + f_{31}m_{31} - f_{42}m_{42} + f_{43}m_{43} - f_{44}m_{44} = 0 \end{cases}$$

Theorem ([Kurano, 1989])

The syzygies between the $(r+1)$-minors of M are generated by the syzygies between the $(r+1)$ minors of the $(r+2) \times (r+2)$ submatrices of M.

The Gulliksen-Negård complex

m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix}$$

Type I →
$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ \times & \times & \times & \times \end{pmatrix} \longrightarrow \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ f_{31}m_{11} - f_{32}m_{12} + f_{33}m_{13} - f_{34}m_{14} = 0 \end{cases}$$

Type II →
$$f_{41}m_{41} - f_{42}m_{42} + f_{43}m_{43} - f_{44}m_{44}$$
$$\| $$
$$f_{11}m_{11} - f_{21}m_{21} + f_{31}m_{31} - f_{41}m_{41}$$
$$\longrightarrow \begin{cases} f_{21}m_{21} - f_{31}m_{31} + f_{41}m_{41} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{11}m_{11} + f_{31}m_{31} - f_{41}m_{41} - f_{22}m_{22} + f_{23}m_{23} - f_{24}m_{24} = 0 \\ f_{11}m_{11} - f_{21}m_{21} - f_{41}m_{41} + f_{32}m_{32} - f_{33}m_{33} + f_{34}m_{34} = 0 \\ f_{11}m_{11} - f_{21}m_{21} + f_{31}m_{31} - f_{42}m_{42} + f_{43}m_{43} - f_{44}m_{44} = 0 \end{cases}$$

Theorem ([Kurano, 1989])

The syzygies between the $(r+1)$-minors of M are generated by the syzygies between the $(r+1)$ minors of the $(r+2) \times (r+2)$ submatrices of M.

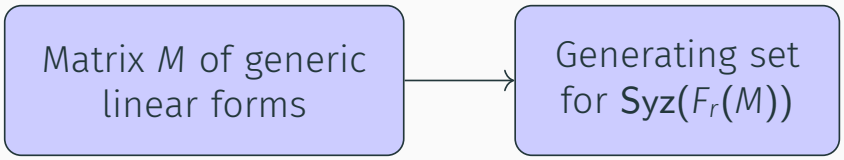
Takeaway: we can reduce to the case $r = n - 2$.

New F_5 algorithms - the general case

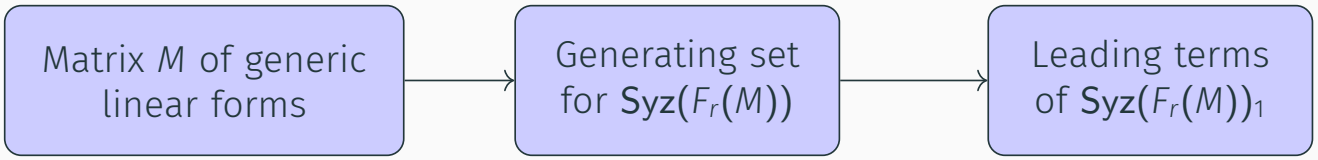
New F_5 algorithms - the general case

Matrix M of generic linear forms

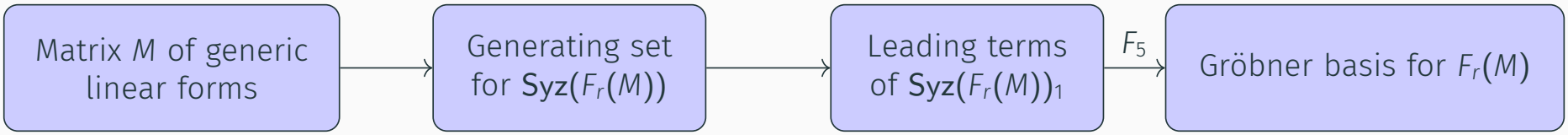
New F_5 algorithms - the general case



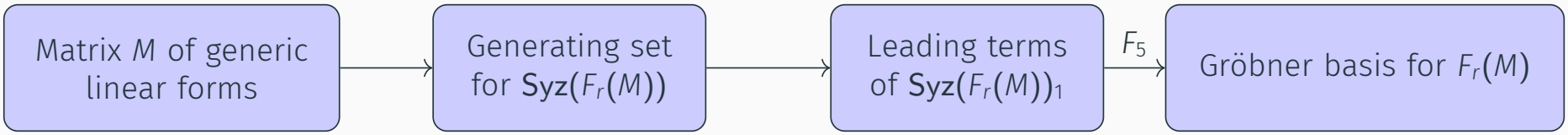
New F_5 algorithms - the general case



New F_5 algorithms - the general case

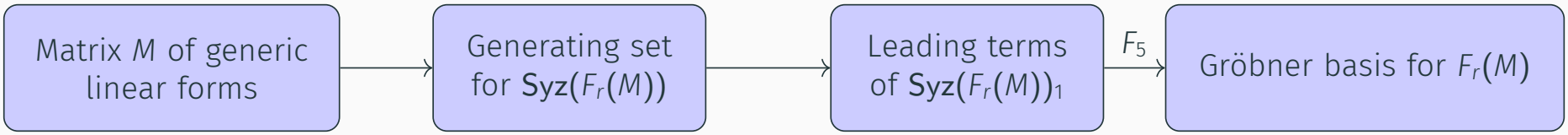


New F_5 algorithms - the general case



$$\#\,\mathsf{Syz}(F_r(M)) = \binom{n}{r+2}^2 \left(\frac{2(r+2)(r+1)}{n-r-1} + 2r + 2\right).$$

New F_5 algorithms - the general case

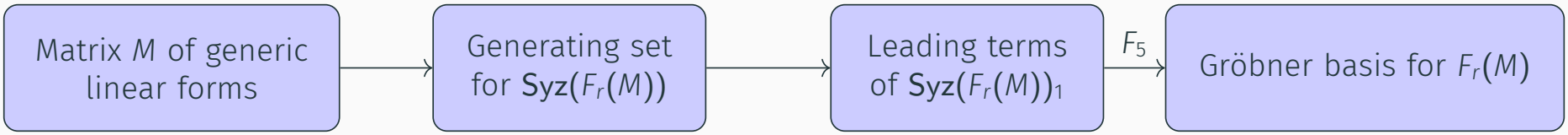


$$\#\,\mathsf{Syz}(F_r(M)) = \binom{n}{r+2}^2 \left(\frac{2(r+2)(r+1)}{n-r-1} + 2r + 2\right).$$

Theorem ([Eagon, Hochster, 1971])

$F_r(M)$ has a free resolution of length $(n-r)^2$.

New F_5 algorithms - the general case



$$\#\,\mathsf{Syz}(F_r(M)) = \binom{n}{r+2}^2 \left(\frac{2(r+2)(r+1)}{n-r-1} + 2r + 2\right).$$

Theorem ([Eagon, Hochster, 1971])

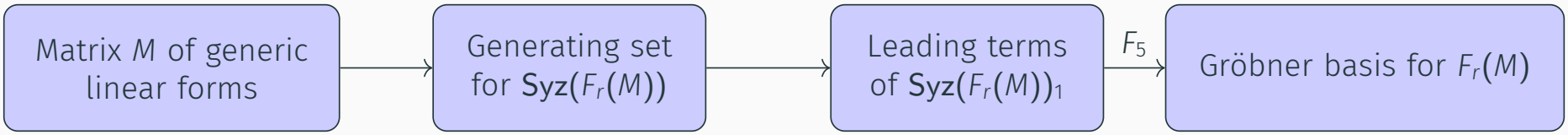
$F_r(M)$ has a free resolution of length $(n-r)^2$.

$$\mathsf{Syz}_k(F_r(M)) \neq 0$$

for

$$1 < k < (n-r)^2.$$

New F_5 algorithms - the general case



$$\#\,\mathsf{Syz}(F_r(M)) = \binom{n}{r+2}^2 \left(\frac{2(r+2)(r+1)}{n-r-1} + 2r + 2\right).$$

Theorem ([Eagon, Hochster, 1971])

$F_r(M)$ has a free resolution of length $(n-r)^2$.

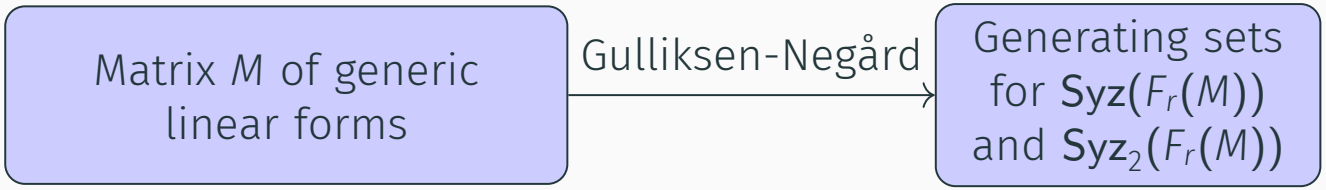
$\mathsf{Syz}_k(F_r(M)) \neq 0$ for $1 < k < (n-r)^2$. $\Longrightarrow$ Cannot efficiently compute a Gröbner basis for $\mathsf{Syz}(F_r(M))$

New F_5 algorithms - the case $r = n - 2$

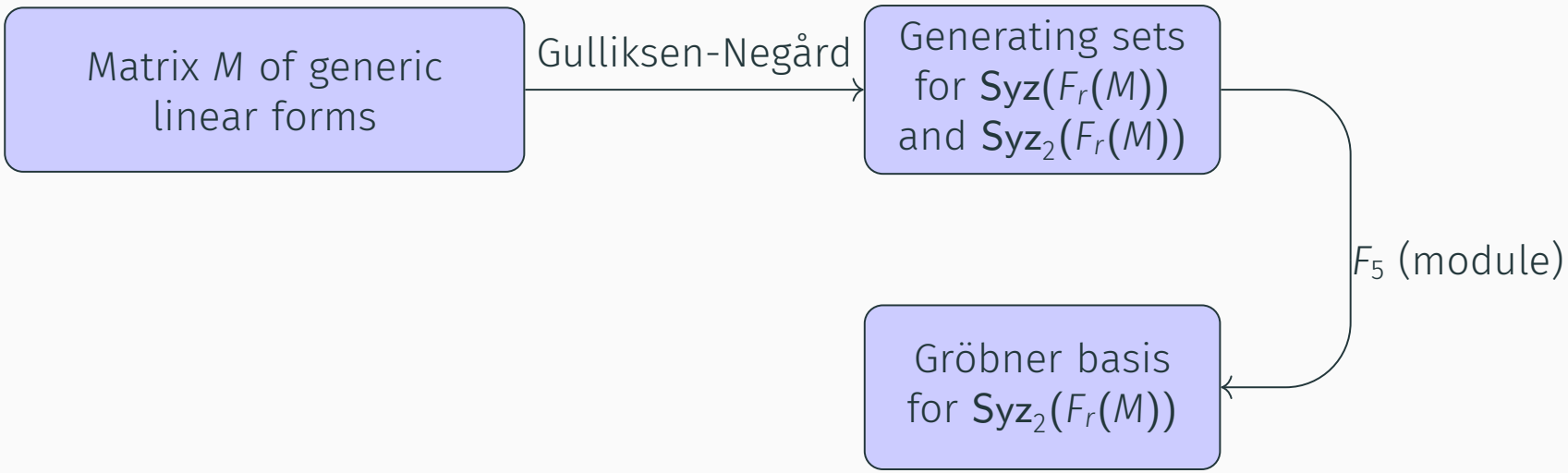
New F_5 algorithms - the case $r = n - 2$

Matrix M of generic linear forms

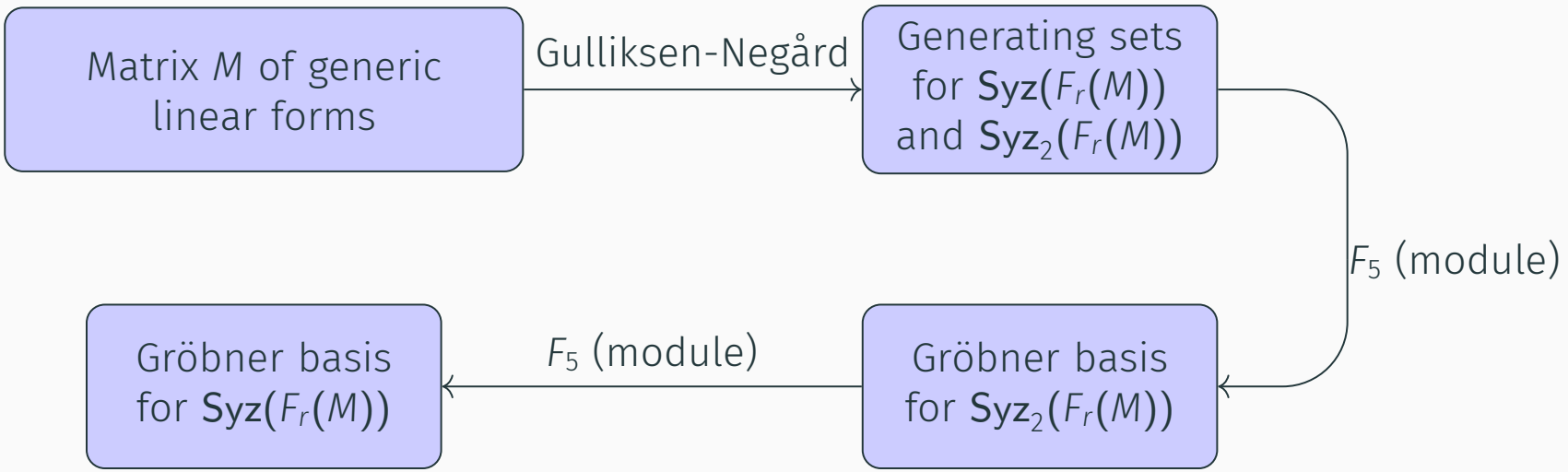
New F_5 algorithms - the case $r = n - 2$



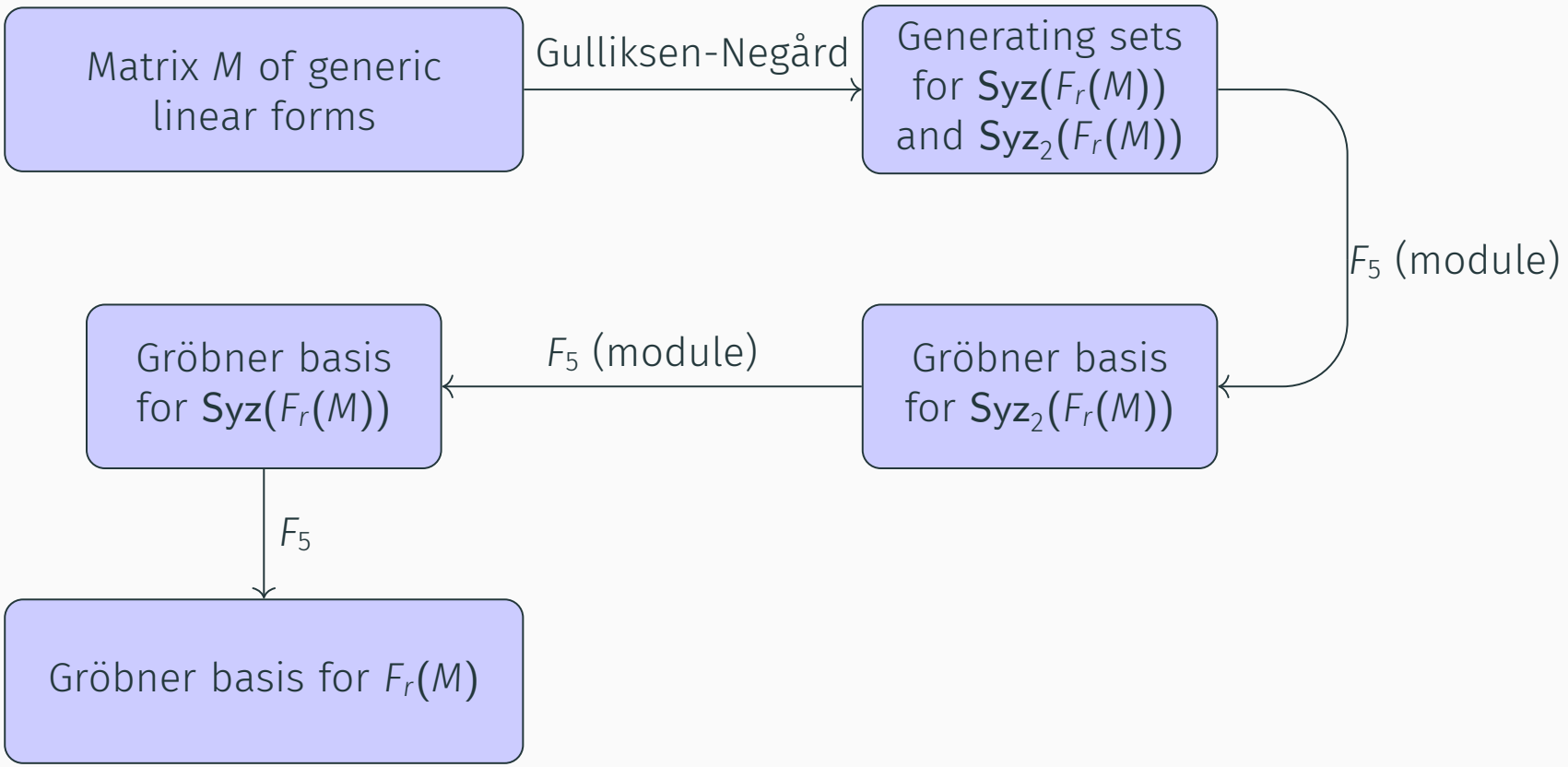
New F_5 algorithms - the case $r = n - 2$



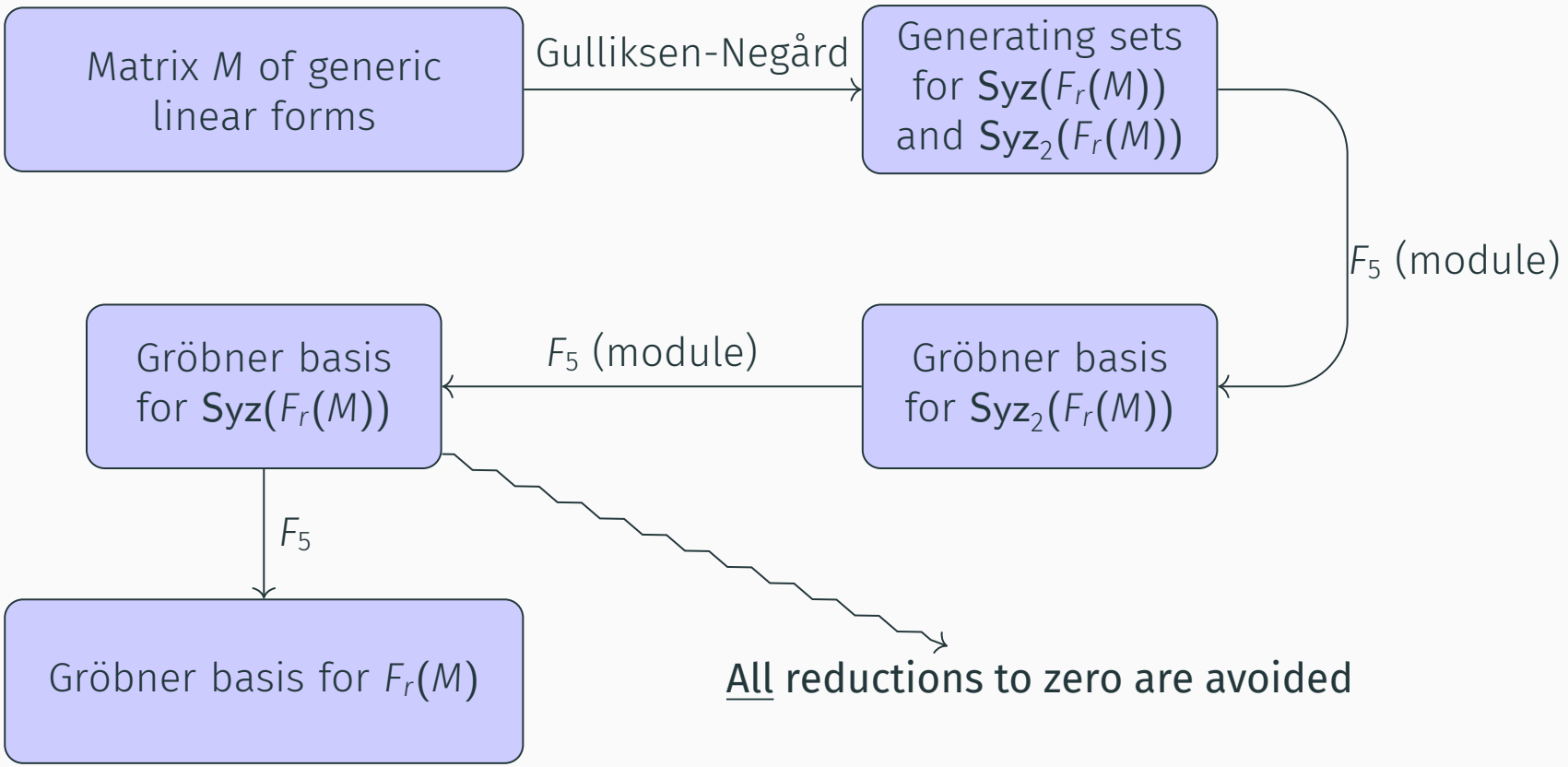
New F_5 algorithms - the case $r = n - 2$



New F_5 algorithms - the case $r = n - 2$



New F_5 algorithms - the case $r = n - 2$



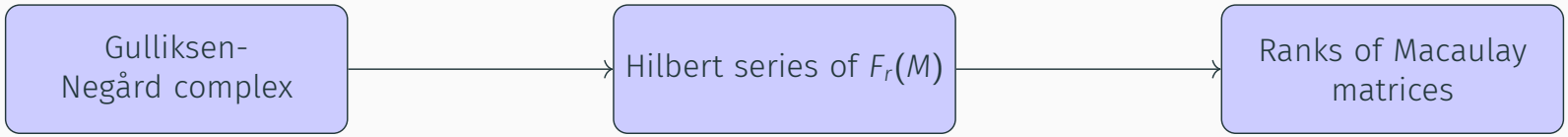
A complexity analysis in the case $r = n - 2$

A complexity analysis in the case $r = n - 2$

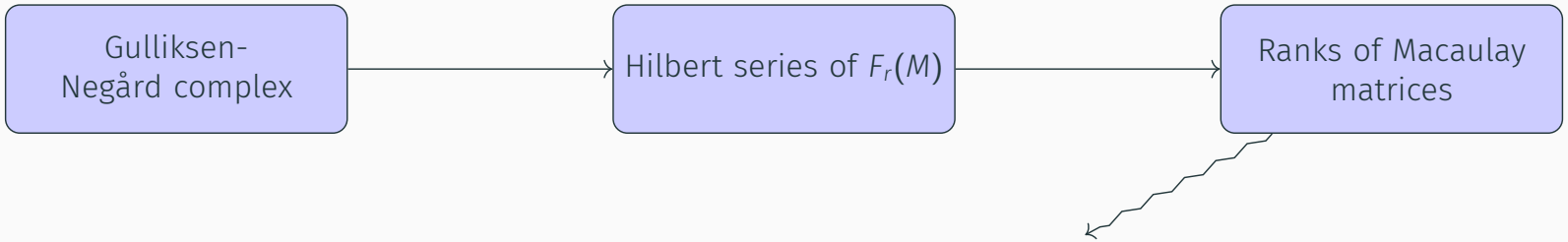
Gulliksen-
Negård complex

A complexity analysis in the case $r = n - 2$

A complexity analysis in the case $r = n - 2$



A complexity analysis in the case $r = n - 2$

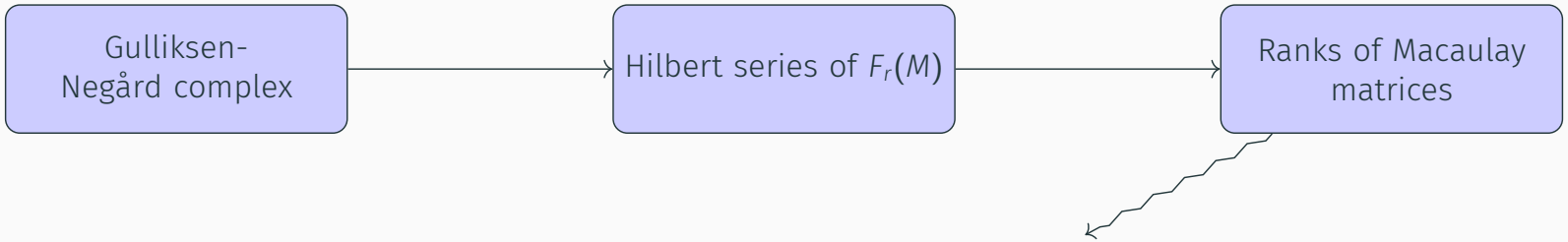


Theorem ([G., Neiger, Safey, 2023])

Let M be a matrix of generic linear forms in four variables. The complexity of computing a grevlex-Gröbner basis for $F_r(M)$ is in

$$O\left(\left(\sum_{d=n-1}^{2n-3} \frac{(d^2+(-2n+4)d+4n^2-4n+3)(2+d-n)}{3}\right)^{\omega-1}\binom{2n}{3}\right).$$

A complexity analysis in the case $r = n - 2$



Theorem ([G., Neiger, Safey, 2023])

Let M be a matrix of generic linear forms in four variables. The complexity of computing a grevlex-Gröbner basis for $F_r(M)$ is in

$$O\left(\left(\sum_{d=n-1}^{2n-3} \frac{(d^2+(-2n+4)d+4n^2-4n+3)(2+d-n)}{3}\right)^{\omega-1}\binom{2n}{3}\right).$$

Asymptotically:

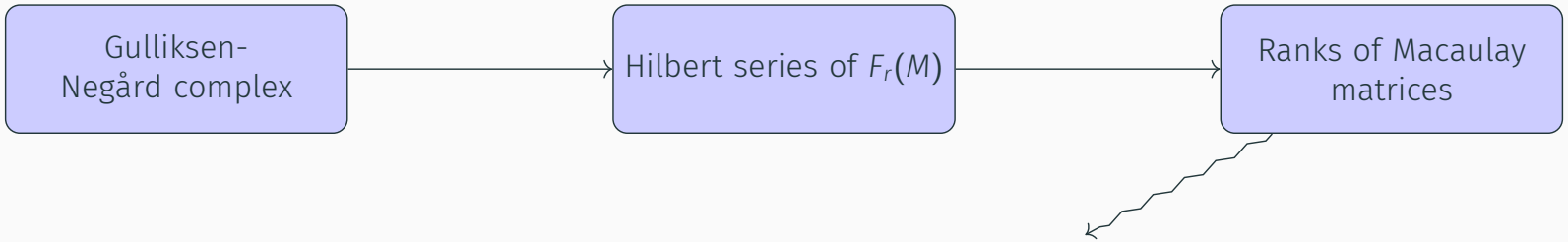
[Faugère, Safey, Spaenlehauer, 2013]

$$O\left(n^{5\omega+2}\right)$$

[G., Neiger, Safey El Din, 2023]

$$O\left(n^{4\omega-1}\right)$$

A complexity analysis in the case $r = n - 2$



Theorem ([G., Neiger, Safey, 2023])

Let M be a matrix of generic linear forms in four variables. The complexity of computing a grevlex-Gröbner basis for $F_r(M)$ is in

$$O\left(\left(\sum_{d=n-1}^{2n-3} \frac{(d^2+(-2n+4)d+4n^2-4n+3)(2+d-n)}{3}\right)^{\omega-1}\binom{2n}{3}\right).$$

Asymptotically:

[Faugère, Safey, Spaenlehauer, 2013]

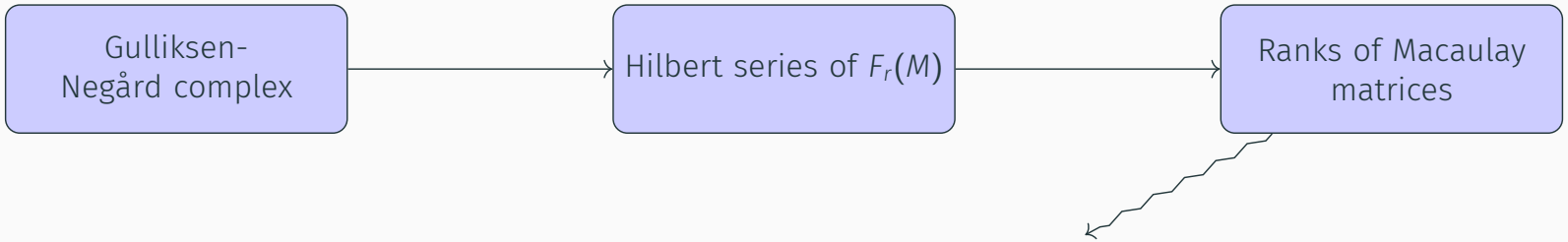
$$O\left(n^{5\omega+2}\right)$$

[G., Neiger, Safey El Din, 2023]

$$O\left(n^{4\omega-1}\right)$$

Refined further to $O(n^{2\omega+3})$ + $|GB| \in \Omega(n^6)$...

A complexity analysis in the case $r = n - 2$



Theorem ([G., Neiger, Safey, 2023])

Let M be a matrix of generic linear forms in four variables. The complexity of computing a grevlex-Gröbner basis for $F_r(M)$ is in

$$O\left(\left(\sum_{d=n-1}^{2n-3} \frac{(d^2+(-2n+4)d+4n^2-4n+3)(2+d-n)}{3}\right)^{\omega-1}\binom{2n}{3}\right).$$

Asymptotically:

[Faugère, Safey, Spaenlehauer, 2013]

$$O\left(n^{5\omega+2}\right)$$

[G., Neiger, Safey El Din, 2023]

$$O\left(n^{4\omega-1}\right)$$

Refined further to $O(n^{2\omega+3})$ + $|GB| \in \Omega(n^6)$...

...assuming a specific Zariski open subset of $\mathbb{A}_{\overline{k}}^{4n^2}$ is nonempty.

Hilbert series

Theorem ([Hilbert, 1890])

L graded, with ***graded*** *free resolution:*

$$0 \to \mathcal{E}_k \to \mathcal{E}_{k-1} \to \cdots \to \mathcal{E}_0 \to L \to 0.$$

Then $\mathsf{HF}_L(d) = \sum_{j=0}^{k} (-1)^j \, \mathsf{HF}_{\mathcal{E}_j}(d)$.

Hilbert series

Theorem ([Hilbert, 1890])

L graded, with ***graded*** *free resolution:*

$$0 \to \mathcal{E}_k \to \mathcal{E}_{k-1} \to \cdots \to \mathcal{E}_0 \to L \to 0.$$

Then $\mathsf{HF}_L(d) = \sum_{j=0}^{k} (-1)^j \mathsf{HF}_{\mathcal{E}_j}(d)$.

Gulliksen-Negård $\rightsquigarrow$

$$\mathsf{HF}_{\mathcal{E}_0} \quad (d) =$$

$$\mathsf{HF}_{\mathcal{E}_1} \quad (d) =$$

$$\mathsf{HF}_{\mathcal{E}_2} \quad (d) =$$

Hilbert series

Theorem ([Hilbert, 1890])

L graded, with **graded** *free resolution:*

$$0 \to \mathcal{E}_k \to \mathcal{E}_{k-1} \to \cdots \to \mathcal{E}_0 \to L \to 0.$$

Then $\mathrm{HF}_L(d) = \sum_{j=0}^{k} (-1)^j \mathrm{HF}_{\mathcal{E}_j}(d)$.

Gulliksen-Negård $\rightsquigarrow$

$$\mathrm{HF}_{\mathcal{E}_0(n-1)}(d) =$$

$$\mathrm{HF}_{\mathcal{E}_1(n)}(d) =$$

$$\mathrm{HF}_{\mathcal{E}_2(n+1)}(d) =$$

Hilbert series

Theorem ([Hilbert, 1890])

L graded, with **graded** *free resolution:*

$$0 \to \mathcal{E}_k \to \mathcal{E}_{k-1} \to \cdots \to \mathcal{E}_0 \to L \to 0.$$

Then $\mathrm{HF}_L(d) = \sum_{j=0}^{k} (-1)^j \mathrm{HF}_{\mathcal{E}_j}(d)$.

Gulliksen-Negård $\rightsquigarrow$

$$\mathrm{HF}_{\mathcal{E}_0(\mathrm{n}-1)}(d) = n^2 \binom{3+d-(\mathrm{n}-1)}{3}$$

$$\mathrm{HF}_{\mathcal{E}_1(\mathrm{n})}(d) = (2n^2-2) \binom{3+d-\mathrm{n}}{3}$$

$$\mathrm{HF}_{\mathcal{E}_2(\mathrm{n}+1)}(d) = n^2 \binom{3+d-(\mathrm{n}+1)}{3}$$

Hilbert series

Theorem ([Hilbert, 1890])

L graded, with graded *free resolution*

Then $\mathrm{HF}_L(d) =$

Corollary

The Macaulay matrix in degree d for $\mathcal{I}_{n-2}(M)$ *has rank*

$$n^2\binom{4+d-n}{3} - (2n^2-2)\binom{3+d-n}{3} + n^2\binom{2+d-n}{3}$$

Gulliksen-Negård $\rightsquigarrow$

$$\mathrm{HF}_{\mathcal{E}_0(\mathrm{n}-1)}(d) = n^2\binom{3+d-(\mathrm{n}-1)}{3}$$

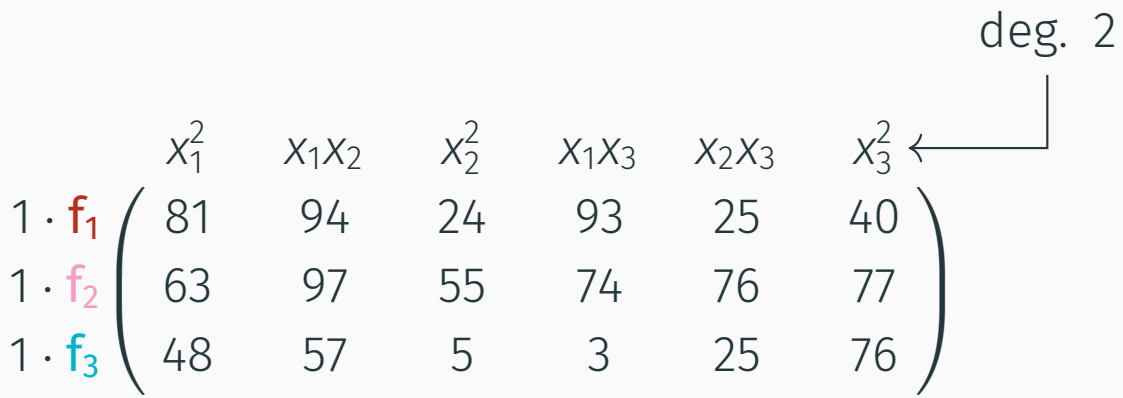
$$\mathrm{HF}_{\mathcal{E}_1(\mathrm{n})}(d) = (2n^2-2)\binom{3+d-\mathrm{n}}{3}$$

$$\mathrm{HF}_{\mathcal{E}_2(\mathrm{n}+1)}(d) = n^2\binom{3+d-(\mathrm{n}+1)}{3}$$

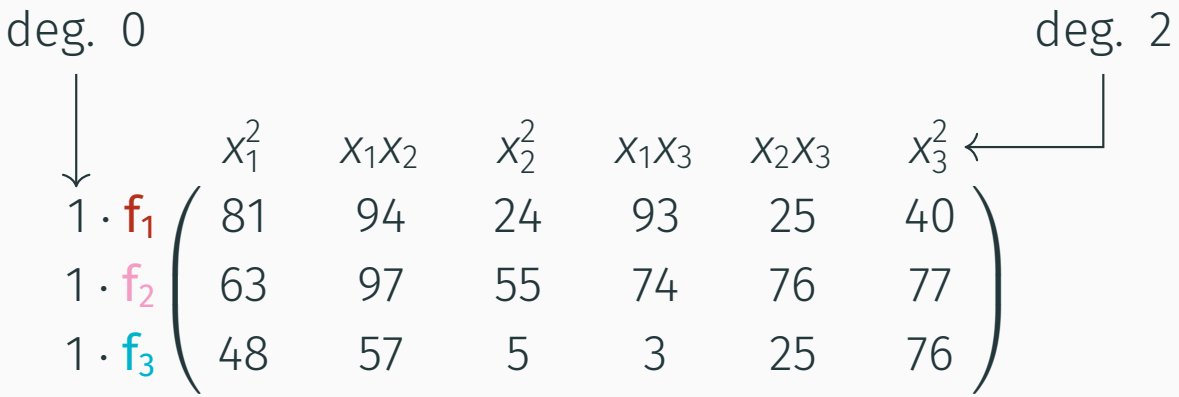
Structured Macaulay matrices

$$
\begin{array}{c}
 & \begin{array}{cccccc} x_1^2 & x_1x_2 & x_2^2 & x_1x_3 & x_2x_3 & x_3^2 \end{array} \\
\begin{array}{c} 1 \cdot f_1 \\ 1 \cdot f_2 \\ 1 \cdot f_3 \end{array} & \begin{pmatrix} 81 & 94 & 24 & 93 & 25 & 40 \\ 63 & 97 & 55 & 74 & 76 & 77 \\ 48 & 57 & 5 & 3 & 25 & 76 \end{pmatrix}
\end{array}
$$

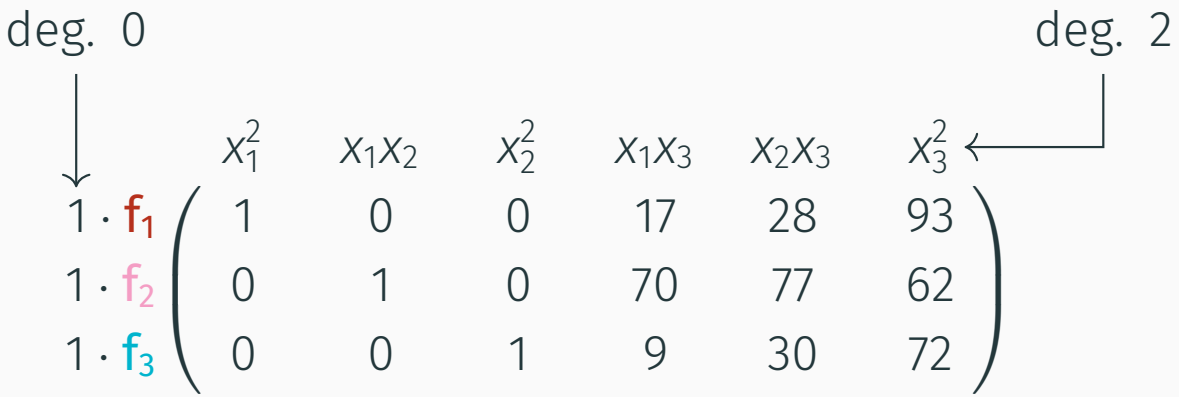
Structured Macaulay matrices



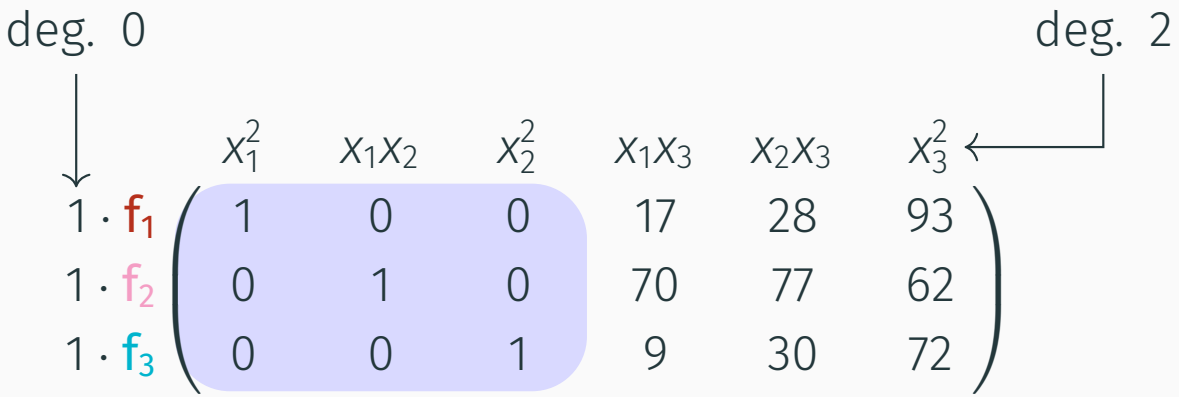
Structured Macaulay matrices



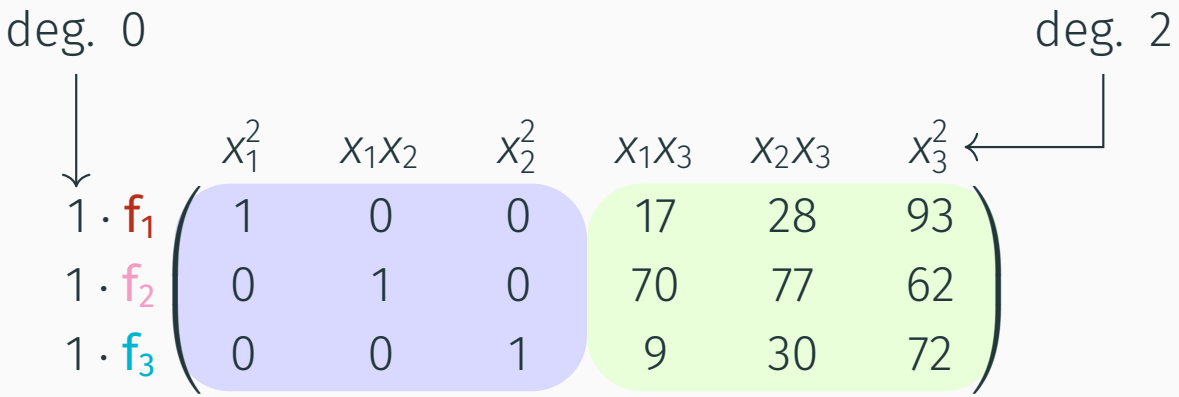
Structured Macaulay matrices



Structured Macaulay matrices

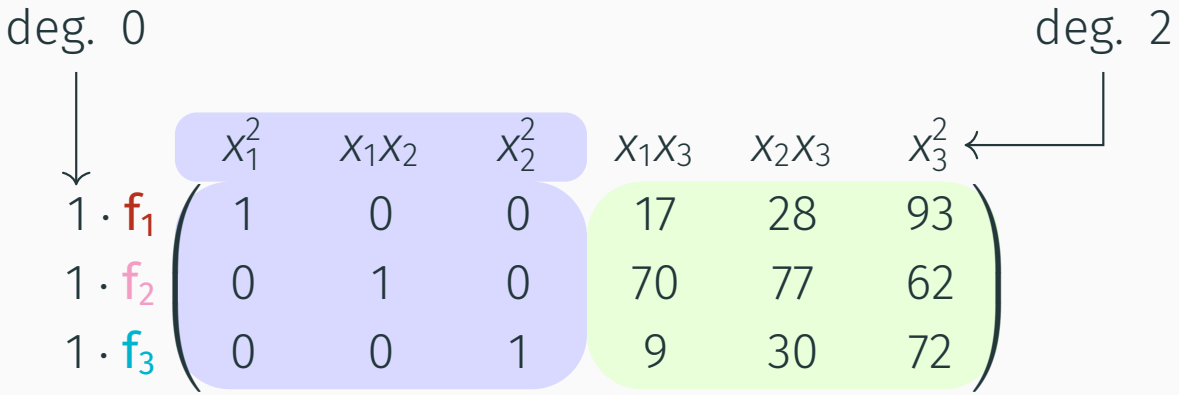


Structured Macaulay matrices



Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$



Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	17	28	0	93	0	0
$x_2 \cdot f_1$	0	1	0	0	0	17	28	0	93	0
$x_2 \cdot f_2$	0	0	1	0	0	70	77	0	62	0
$x_2 \cdot f_3$	0	0	0	1	0	9	30	0	72	0
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	17	28	0	93	0	0
$x_2 \cdot f_1$	0	1	0	0	0	17	28	0	93	0
$x_2 \cdot f_2$	0	0	1	0	0	70	77	0	62	0
$x_2 \cdot f_3$	0	0	0	1	0	9	30	0	72	0
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	17	28	0	93	0	0
$x_2 \cdot f_1$	0	1	0	0	0	17	28	0	93	0
$x_2 \cdot f_2$	0	0	1	0	0	70	77	0	62	0
$x_2 \cdot f_3$	0	0	0	1	0	9	30	0	72	0
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	17	28	0	93	0	0
$x_2 \cdot f_1$	0	1	0	0	0	17	28	0	93	0
$x_2 \cdot f_2$	0	0	1	0	0	70	77	0	62	0
$x_2 \cdot f_3$	0	0	0	1	0	9	30	0	72	0
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	17	28	0	93	0	0
$x_2 \cdot f_1$	0	1	0	0	0	17	28	0	93	0
$x_2 \cdot f_2$	0	0	1	0	0	70	77	0	62	0
$x_2 \cdot f_3$	0	0	0	1	0	9	30	0	72	0
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	66	95	16
$x_2 \cdot f_1$	0	1	0	0	0	0	0	73	65	61
$x_2 \cdot f_2$	0	0	1	0	0	0	0	63	38	14
$x_2 \cdot f_3$	0	0	0	1	0	0	0	9	95	9
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	66	95	16
$x_2 \cdot f_1$	0	1	0	0	0	0	0	73	65	61
$x_2 \cdot f_2$	0	0	1	0	0	0	0	63	38	14
$x_2 \cdot f_3$	0	0	0	1	0	0	0	9	95	9
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	66	95	16
$x_2 \cdot f_1$	0	1	0	0	0	0	0	73	65	61
$x_2 \cdot f_2$	0	0	1	0	0	0	0	63	38	14
$x_2 \cdot f_3$	0	0	0	1	0	0	0	9	95	9
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	0	0	0	0	0	0	75	25	68
$x_1 \cdot f_3$	0	0	0	0	0	0	0	79	26	16

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	66	95	16
$x_2 \cdot f_1$	0	1	0	0	0	0	0	73	65	61
$x_2 \cdot f_2$	0	0	1	0	0	0	0	63	38	14
$x_2 \cdot f_3$	0	0	0	1	0	0	0	9	95	9
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	0	0	0	0	0	0	75	25	68
$x_1 \cdot f_3$	0	0	0	0	0	0	0	79	26	16

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	66	95	16
$x_2 \cdot f_1$	0	1	0	0	0	0	0	73	65	61
$x_2 \cdot f_2$	0	0	1	0	0	0	0	63	38	14
$x_2 \cdot f_3$	0	0	0	1	0	0	0	9	95	9
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	66	95	16
$x_2 \cdot f_1$	0	1	0	0	0	0	0	73	65	61
$x_2 \cdot f_2$	0	0	1	0	0	0	0	63	38	14
$x_2 \cdot f_3$	0	0	0	1	0	0	0	9	95	9
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	0	0	3
$x_2 \cdot f_1$	0	1	0	0	0	0	0	0	0	40
$x_2 \cdot f_2$	0	0	1	0	0	0	0	0	0	57
$x_2 \cdot f_3$	0	0	0	1	0	0	0	0	0	12
$x_3 \cdot f_1$	0	0	0	0	1	0	0	0	0	27
$x_3 \cdot f_2$	0	0	0	0	0	1	0	0	0	68
$x_3 \cdot f_3$	0	0	0	0	0	0	1	0	0	95
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Structured Macaulay matrices

$(\mathrm{LM}_{\succ}(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	0	0	3
$x_2 \cdot f_1$	0	1	0	0	0	0	0	0	0	40
$x_2 \cdot f_2$	0	0	1	0	0	0	0	0	0	57
$x_2 \cdot f_3$	0	0	0	1	0	0	0	0	0	12
$x_3 \cdot f_1$	0	0	0	0	1	0	0	0	0	27
$x_3 \cdot f_2$	0	0	0	0	0	1	0	0	0	68
$x_3 \cdot f_3$	0	0	0	0	0	0	1	0	0	95
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Structured Macaulay matrices

$(\mathrm{LM}_\succ(I))_2 = \{x_1^2, x_1x_2, x_2^2\}$

$(\mathrm{LM}_\succ(I))_3 \setminus \langle(\mathrm{LM}_\succ(I))_2\rangle = \{x_1x_3^2, x_2x_3^2\}$

deg. 1 ↓ deg. 3 ↓

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	0	0	3
$x_2 \cdot f_1$	0	1	0	0	0	0	0	0	0	40
$x_2 \cdot f_2$	0	0	1	0	0	0	0	0	0	57
$x_2 \cdot f_3$	0	0	0	1	0	0	0	0	0	12
$x_3 \cdot f_1$	0	0	0	0	1	0	0	0	0	27
$x_3 \cdot f_2$	0	0	0	0	0	1	0	0	0	68
$x_3 \cdot f_3$	0	0	0	0	0	0	1	0	0	95
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Reverse lexicographic ideals

Reverse lexicographic ideals

$$
\begin{array}{c}
 & \begin{array}{ccccccc} x_1^2 & x_1x_2 & x_2^2 & x_1x_3 & x_2x_3 & x_3^2 \end{array} \\
\begin{array}{r} 1 \cdot f_1 \\ 1 \cdot f_2 \\ 1 \cdot f_3 \end{array} & \left(\begin{array}{ccccccc} 1 & 0 & 0 & 17 & 28 & 93 \\ 0 & 1 & 0 & 70 & 77 & 62 \\ 0 & 0 & 1 & 9 & 30 & 72 \end{array} \right)
\end{array}
$$

Reverse lexicographic ideals

contiguous block

	x_1^2	x_1x_2	x_2^2	x_1x_3	x_2x_3	x_3^2
$1 \cdot f_1$	1	0	0	17	28	93
$1 \cdot f_2$	0	1	0	70	77	62
$1 \cdot f_3$	0	0	1	9	30	72

Reverse lexicographic ideals

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	0	0	3
$x_2 \cdot f_1$	0	1	0	0	0	0	0	0	0	40
$x_2 \cdot f_2$	0	0	1	0	0	0	0	0	0	57
$x_2 \cdot f_3$	0	0	0	1	0	0	0	0	0	12
$x_3 \cdot f_1$	0	0	0	0	1	0	0	0	0	27
$x_3 \cdot f_2$	0	0	0	0	0	1	0	0	0	68
$x_3 \cdot f_3$	0	0	0	0	0	0	1	0	0	95
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Reverse lexicographic ideals

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	0	0	3
$x_2 \cdot f_1$	0	1	0	0	0	0	0	0	0	40
$x_2 \cdot f_2$	0	0	1	0	0	0	0	0	0	57
$x_2 \cdot f_3$	0	0	0	1	0	0	0	0	0	12
$x_3 \cdot f_1$	0	0	0	0	1	0	0	0	0	27
$x_3 \cdot f_2$	0	0	0	0	0	1	0	0	0	68
$x_3 \cdot f_3$	0	0	0	0	0	0	1	0	0	95
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Reverse lexicographic ideals

contiguous block

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	0	0	3
$x_2 \cdot f_1$	0	1	0	0	0	0	0	0	0	40
$x_2 \cdot f_2$	0	0	1	0	0	0	0	0	0	57
$x_2 \cdot f_3$	0	0	0	1	0	0	0	0	0	12
$x_3 \cdot f_1$	0	0	0	0	1	0	0	0	0	27
$x_3 \cdot f_2$	0	0	0	0	0	1	0	0	0	68
$x_3 \cdot f_3$	0	0	0	0	0	0	1	0	0	95
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Reverse lexicographic ideals

contiguous block

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	0	0	3
$x_2 \cdot f_1$	0	1	0	0	0	0	0	0	0	40
$x_2 \cdot f_2$	0	0	1	0	0	0	0	0	0	57
$x_2 \cdot f_3$	0	0	0	1	0	0	0	0	0	12
$x_3 \cdot f_1$	0	0	0	0	1	0	0	0	0	27
$x_3 \cdot f_2$	0	0	0	0	0	1	0	0	0	68
$x_3 \cdot f_3$	0	0	0	0	0	0	1	0	0	95
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Definition (Reverse lexicographic ideal)

An ideal $\mathcal{I}$ is called **reverse lexicographic** if for any $\sigma \in \mathbf{LM}_{\succ}(\mathcal{I})$ and for any monomial τ of degree $\deg(\sigma)$, if $\tau \succ_{drl} \sigma$, then $\tau \in \mathbf{LM}_{\succ}(\mathcal{I})$.

Reverse lexicographic ideals

contiguous block

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	0	0	3
$x_2 \cdot f_1$	0	1	0	0	0	0	0	0	0	40
$x_2 \cdot f_2$	0	0	1	0	0	0	0	0	0	57
$x_2 \cdot f_3$	0	0	0	1	0	0	0	0	0	12
$x_3 \cdot f_1$	0	0	0	0	1	0	0	0	0	27
$x_3 \cdot f_2$	0	0	0	0	0	1	0	0	0	68
$x_3 \cdot f_3$	0	0	0	0	0	0	1	0	0	95
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Definition (Reverse lexicographic ideal)

An ideal $\mathcal{I}$ is called **reverse lexicographic** if for any $\sigma \in \mathbf{LM}_{\succ}(\mathcal{I})$ and for any monomial τ of degree $\deg(\sigma)$, if $\tau \succ_{drl} \sigma$, then $\tau \in \mathbf{LM}_{\succ}(\mathcal{I})$.

Reverse lexicographic ideals

contiguous block

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	0	0	3
$x_2 \cdot f_1$	0	1	0	0	0	0	0	0	0	40
$x_2 \cdot f_2$	0	0	1	0	0	0	0	0	0	57
$x_2 \cdot f_3$	0	0	0	1	0	0	0	0	0	12
$x_3 \cdot f_1$	0	0	0	0	1	0	0	0	0	27
$x_3 \cdot f_2$	0	0	0	0	0	1	0	0	0	68
$x_3 \cdot f_3$	0	0	0	0	0	0	1	0	0	95
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Theorem

If for any degree d, the reduced row echelon form of the Macaulay matrix $\mathcal{M}_d$ is of the form $\left(\begin{array}{c|c} I & X \end{array} \right)$, then $\mathcal{I}$ is reverse lexicographic.

Reverse lexicographic ideals

contiguous block

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	0	0	0	0	0	3
$x_2 \cdot f_1$	0	1	0	0	0	0	0	0	0	40
$x_2 \cdot f_2$	0	0	1	0	0	0	0	0	0	57
$x_2 \cdot f_3$	0	0	0	1	0	0	0	0	0	12
$x_3 \cdot f_1$	0	0	0	0	1	0	0	0	0	27
$x_3 \cdot f_2$	0	0	0	0	0	1	0	0	0	68
$x_3 \cdot f_3$	0	0	0	0	0	0	1	0	0	95
$x_1 \cdot f_2$	0	0	0	0	0	0	0	1	0	18
$x_1 \cdot f_3$	0	0	0	0	0	0	0	0	1	78

Genericity: $\det(\quad) \neq 0$.

Theorem

If for any degree d, the reduced row echelon form of the Macaulay matrix $\mathcal{M}_d$ *is of the form* $\left(\begin{array}{c|c} I & X \end{array} \right)$, *then* $\mathcal{I}$ *is reverse lexicographic.*

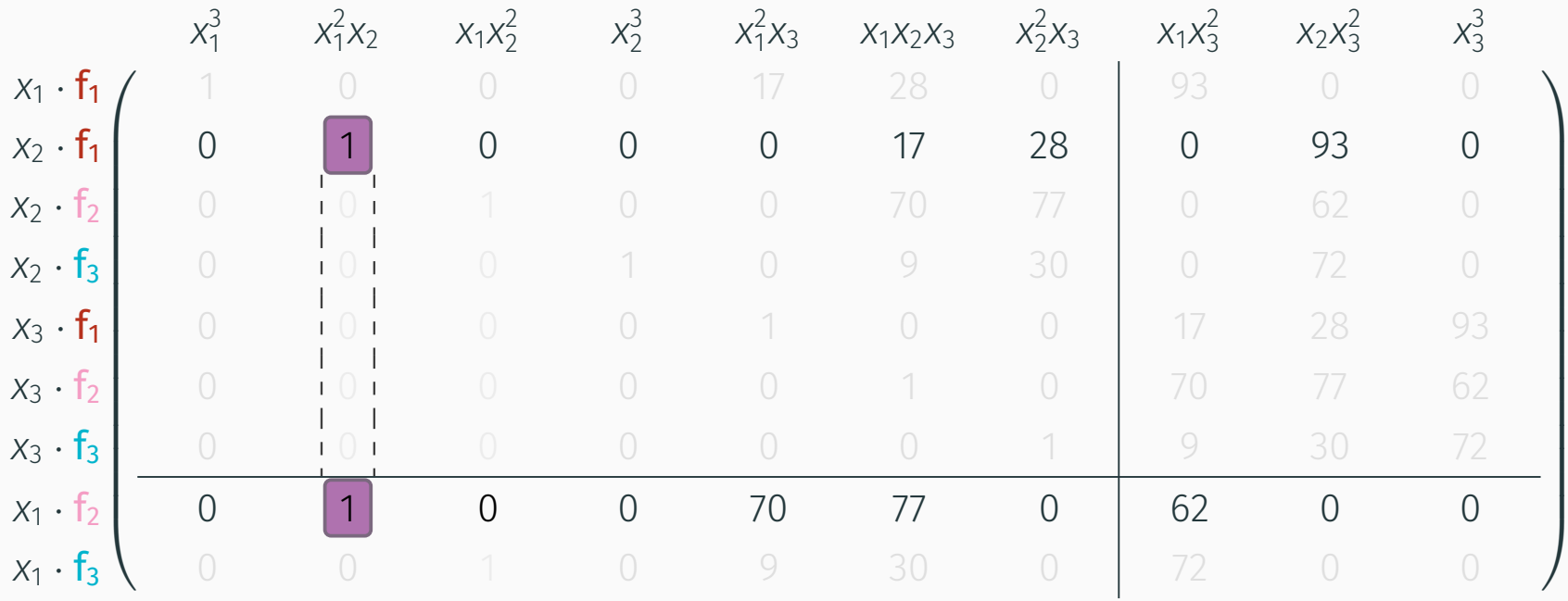
Bounds on the size of the reduced grevlex Gröbner basis

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	17	28	0	93	0	0
$x_2 \cdot f_1$	0	1	0	0	0	17	28	0	93	0
$x_2 \cdot f_2$	0	0	1	0	0	70	77	0	62	0
$x_2 \cdot f_3$	0	0	0	1	0	9	30	0	72	0
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0

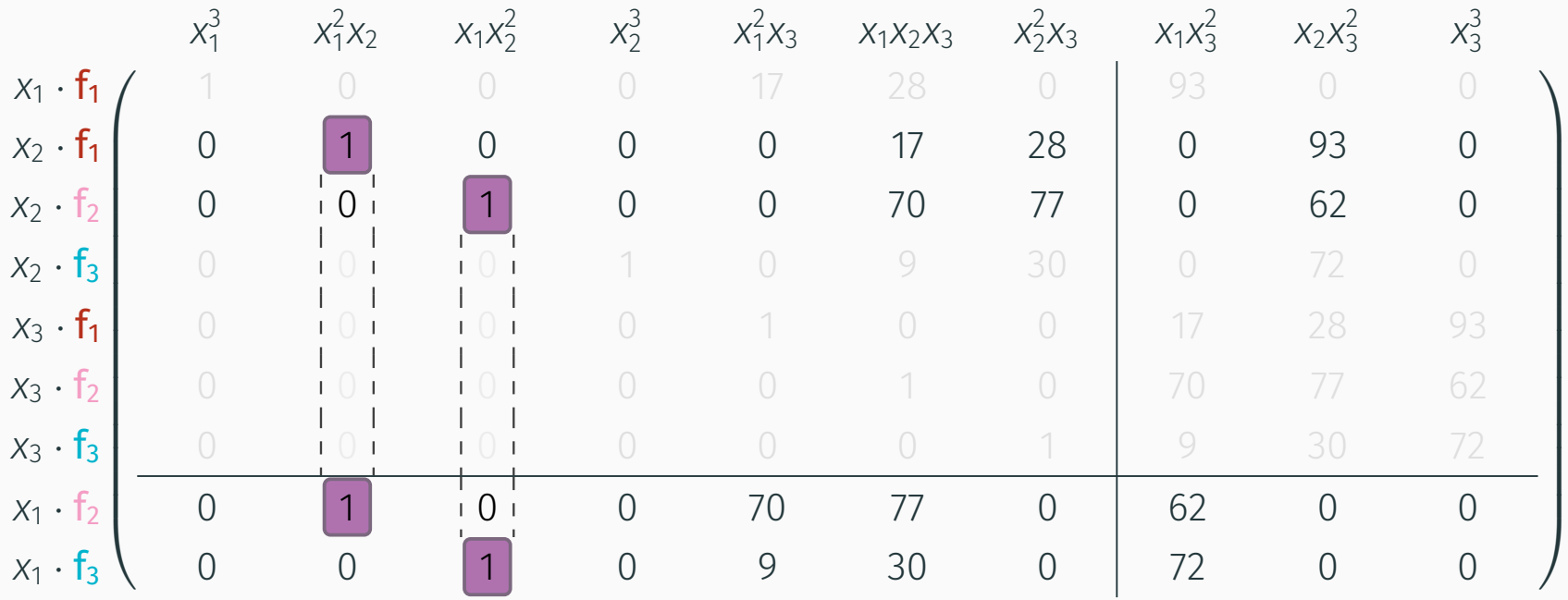
Bounds on the size of the reduced grevlex Gröbner basis

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	17	28	0	93	0	0
$x_2 \cdot f_1$	0	1	0	0	0	17	28	0	93	0
$x_2 \cdot f_2$	0	0	1	0	0	70	77	0	62	0
$x_2 \cdot f_3$	0	0	0	1	0	9	30	0	72	0
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0

Bounds on the size of the reduced grevlex Gröbner basis



Bounds on the size of the reduced grevlex Gröbner basis



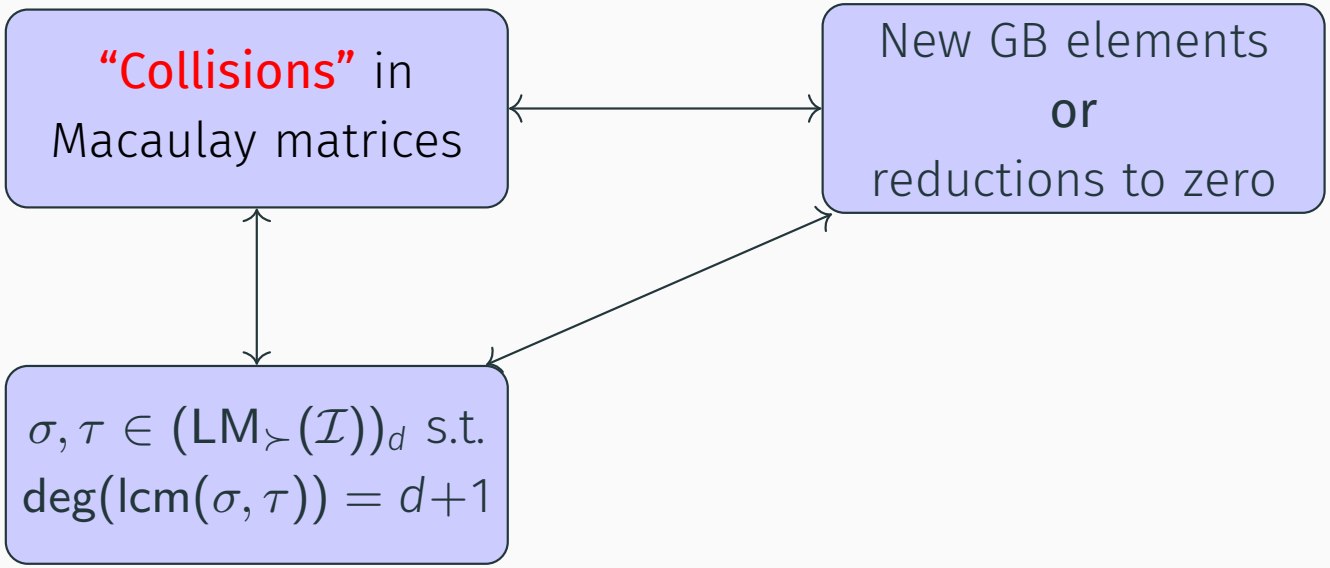
Bounds on the size of the reduced grevlex Gröbner basis

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	17	28	0	93	0	0
$x_2 \cdot f_1$	0	1	0	0	0	17	28	0	93	0
$x_2 \cdot f_2$	0	0	1	0	0	70	77	0	62	0
$x_2 \cdot f_3$	0	0	0	1	0	9	30	0	72	0
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0

"Collisions" in Macaulay matrices ⟷ New GB elements **or** reductions to zero

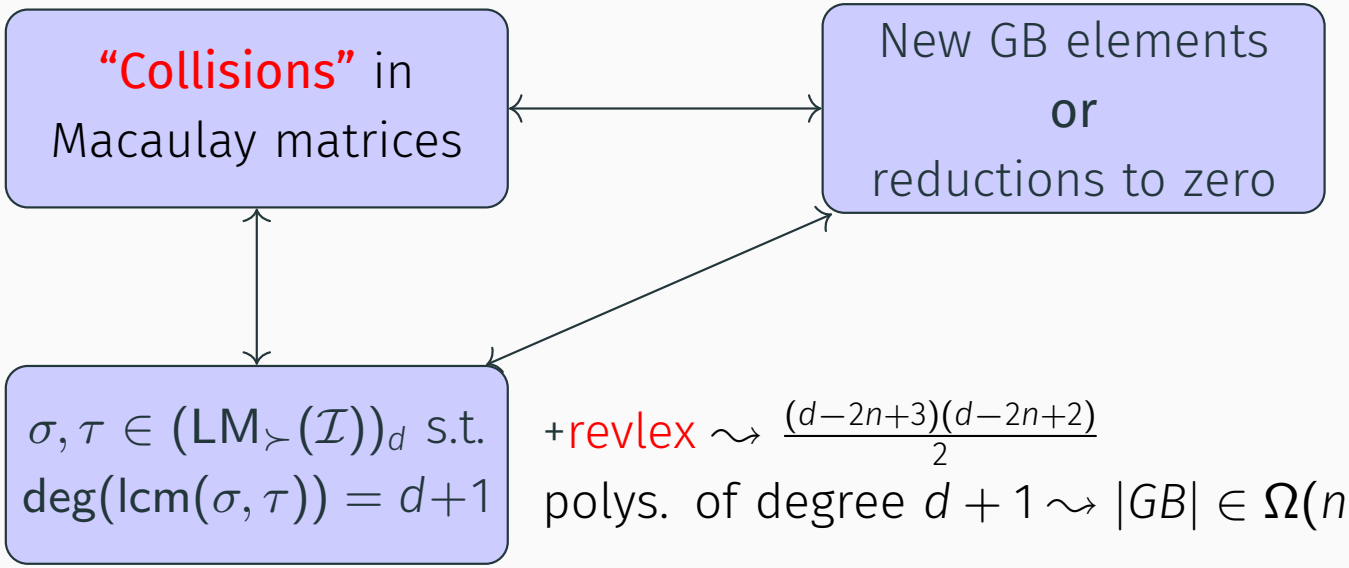
Bounds on the size of the reduced grevlex Gröbner basis

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	17	28	0	93	0	0
$x_2 \cdot f_1$	0	1	0	0	0	17	28	0	93	0
$x_2 \cdot f_2$	0	0	1	0	0	70	77	0	62	0
$x_2 \cdot f_3$	0	0	0	1	0	9	30	0	72	0
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0



Bounds on the size of the reduced grevlex Gröbner basis

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	17	28	0	93	0	0
$x_2 \cdot f_1$	0	1	0	0	0	17	28	0	93	0
$x_2 \cdot f_2$	0	0	1	0	0	70	77	0	62	0
$x_2 \cdot f_3$	0	0	0	1	0	9	30	0	72	0
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0



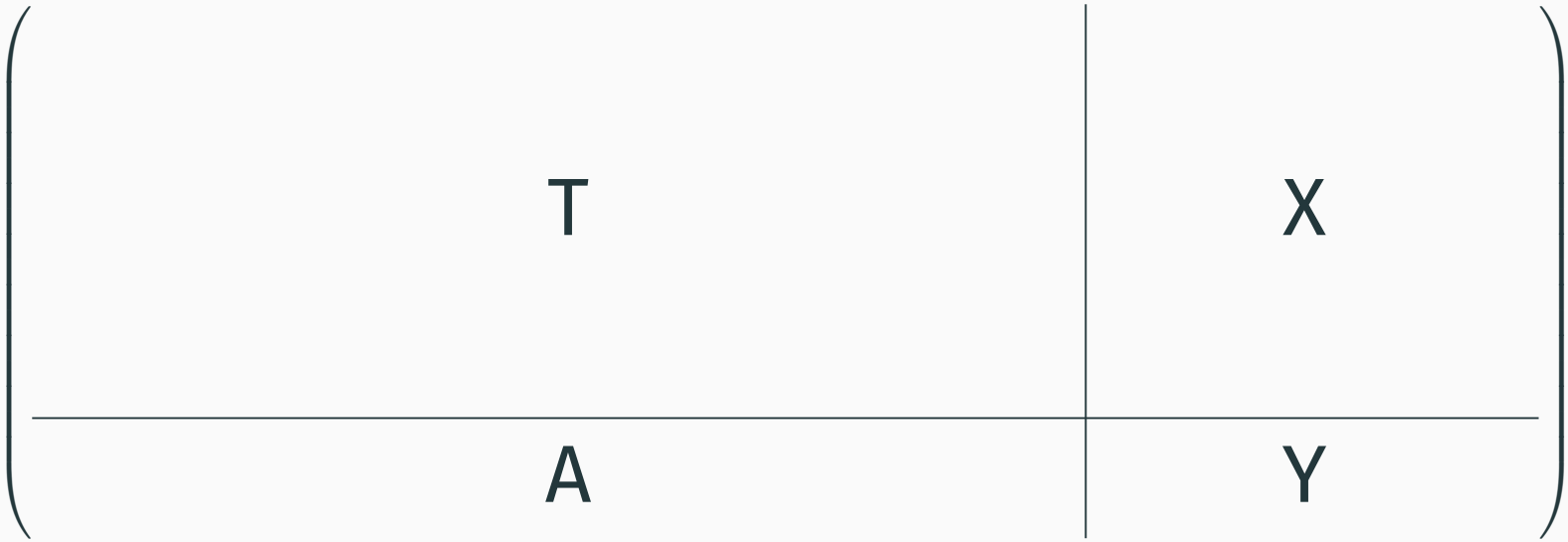
Upper bounds

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
$x_1 \cdot f_1$	1	0	0	0	17	28	0	93	0	0
$x_2 \cdot f_1$	0	1	0	0	0	17	28	0	93	0
$x_2 \cdot f_2$	0	0	1	0	0	70	77	0	62	0
$x_2 \cdot f_3$	0	0	0	1	0	9	30	0	72	0
$x_3 \cdot f_1$	0	0	0	0	1	0	0	17	28	93
$x_3 \cdot f_2$	0	0	0	0	0	1	0	70	77	62
$x_3 \cdot f_3$	0	0	0	0	0	0	1	9	30	72
$x_1 \cdot f_2$	0	1	0	0	70	77	0	62	0	0
$x_1 \cdot f_3$	0	0	1	0	9	30	0	72	0	0

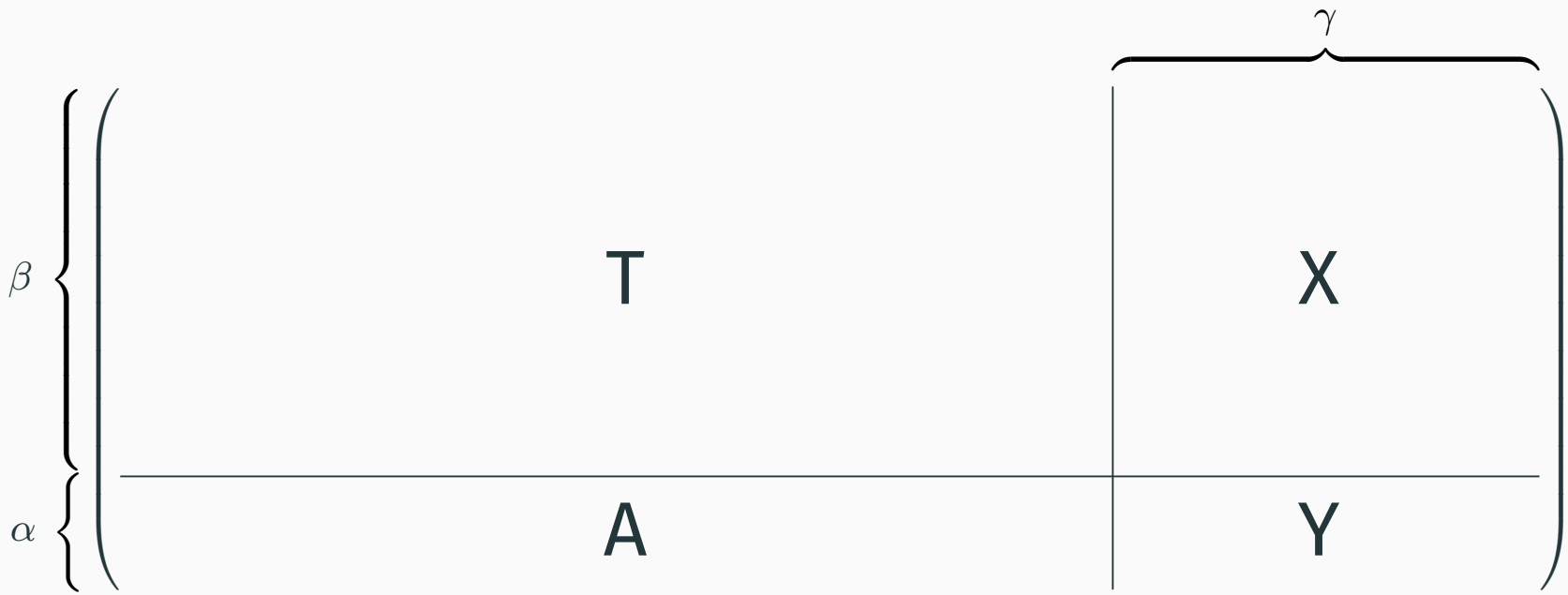
Upper bounds

$$\left(\begin{array}{ccccccc|ccc} 1 & 0 & 0 & 0 & 17 & 28 & 0 & 93 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 17 & 28 & 0 & 93 & 0 \\ 0 & 0 & 1 & 0 & 0 & 70 & 77 & 0 & 62 & 0 \\ 0 & 0 & 0 & 1 & 0 & 9 & 30 & 0 & 72 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 17 & 28 & 93 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 70 & 77 & 62 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 9 & 30 & 72 \\ \hline 0 & 1 & 0 & 0 & 70 & 77 & 0 & 62 & 0 & 0 \\ 0 & 0 & 1 & 0 & 9 & 30 & 0 & 72 & 0 & 0 \end{array}\right)$$

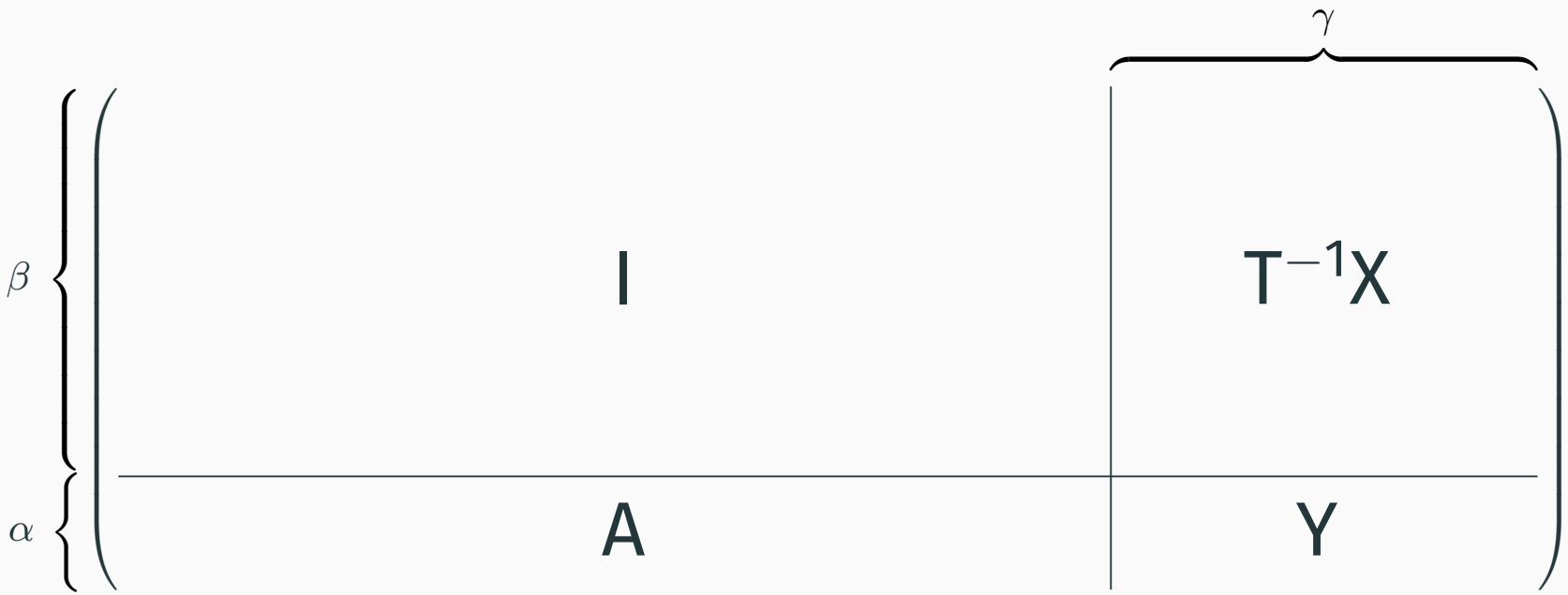
Upper bounds



Upper bounds



Upper bounds



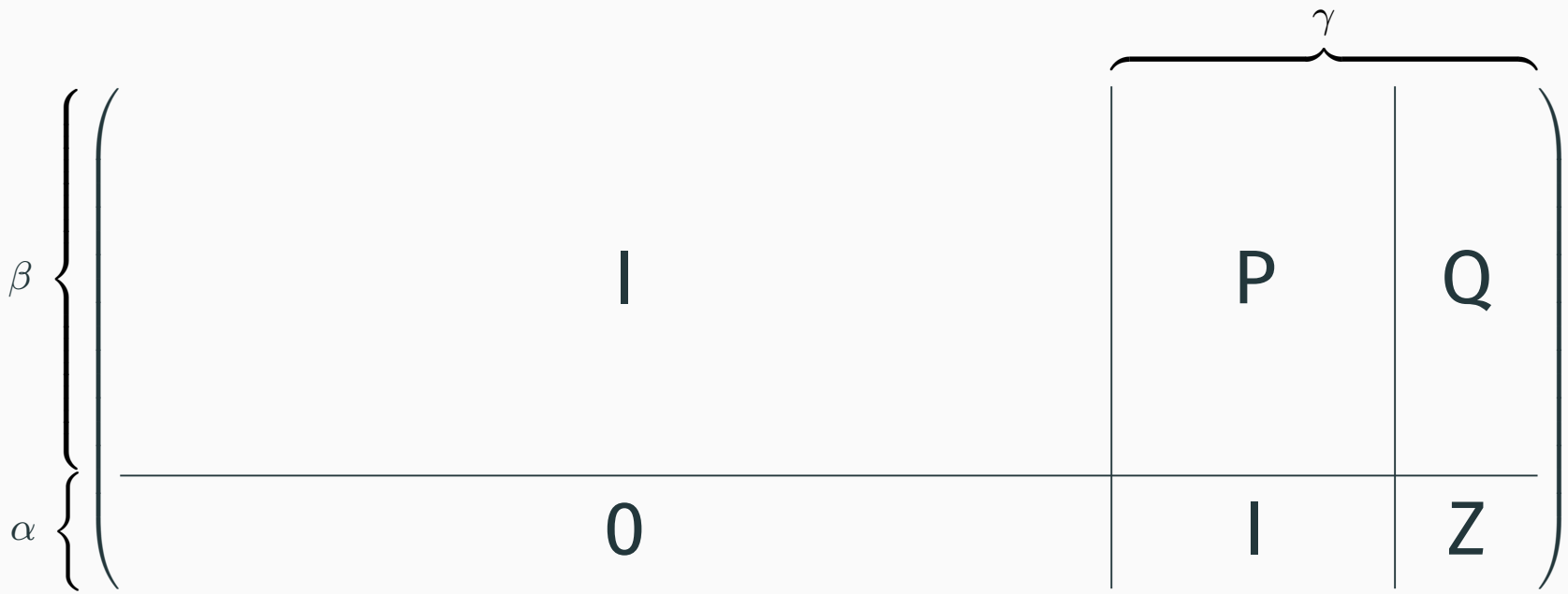
Step 1. Echelonize $(\mathsf{T} \mid \mathsf{X})$: $O(\beta^2\gamma^{\omega-2})$ [Jeannerod, Pernet, Storjohann, 2013]

Upper bounds

$$\begin{array}{c} \\ \beta \\ \alpha \end{array} \overbrace{\left(\begin{array}{c|c} I & T^{-1}X \\ \hline 0 & Y - AT^{-1}X \end{array}\right)}^{\gamma}$$

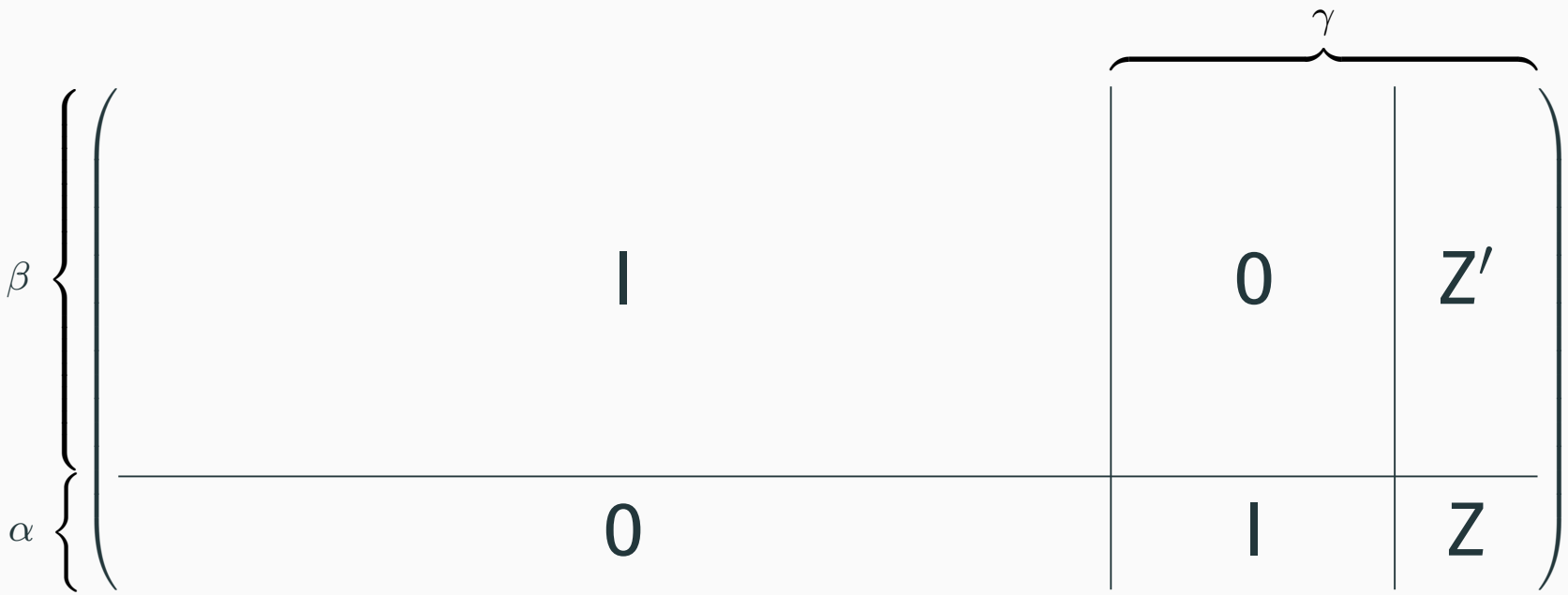
Step 1. Echelonize $(\mathsf{T} \mid \mathsf{X})$:	$O(\beta^2\gamma^{\omega-2})$	[Jeannerod, Pernet, Storjohann, 2013]
Step 2. Eliminate $(\mathsf{A} \mid \mathsf{Y})$:	$O(\alpha^{\omega-2}\beta\gamma)$	[Knight, 1995]

Upper bounds



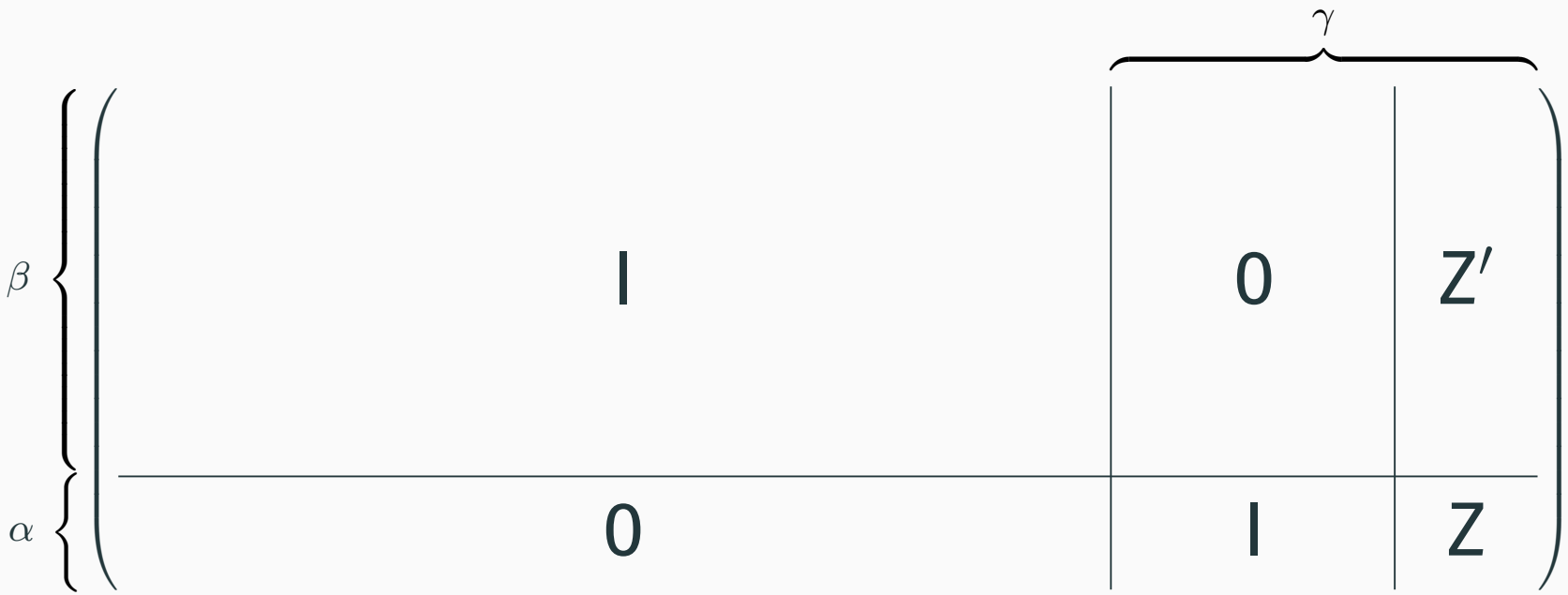
Step 1. Echelonize $(\mathsf{T} \mid \mathsf{X})$:	$O(\beta^2\gamma^{\omega-2})$	[Jeannerod, Pernet, Storjohann, 2013]
Step 2. Eliminate $(\mathsf{A} \mid \mathsf{Y})$:	$O(\alpha^{\omega-2}\beta\gamma)$	[Knight, 1995]
Step 3. Echelonize $\mathsf{Y} - \mathsf{A}\mathsf{T}^{-1}\mathsf{X}$:	$O(\alpha^{\omega-1}\gamma)$	[Storjohann, 2000]

Upper bounds



Step 1. Echelonize $(\mathsf{T} \mid \mathsf{X})$:	$O(\beta^2\gamma^{\omega-2})$	[Jeannerod, Pernet, Storjohann, 2013]
Step 2. Eliminate $(\mathsf{A} \mid \mathsf{Y})$:	$O(\alpha^{\omega-2}\beta\gamma)$	[Knight, 1995]
Step 3. Echelonize $\mathsf{Y} - \mathsf{A}\mathsf{T}^{-1}\mathsf{X}$:	$O(\alpha^{\omega-1}\gamma)$	[Storjohann, 2000]
Step 4. Eliminate P:	$O(\alpha^{\omega-2}\beta\gamma)$	[Knight, 1995]

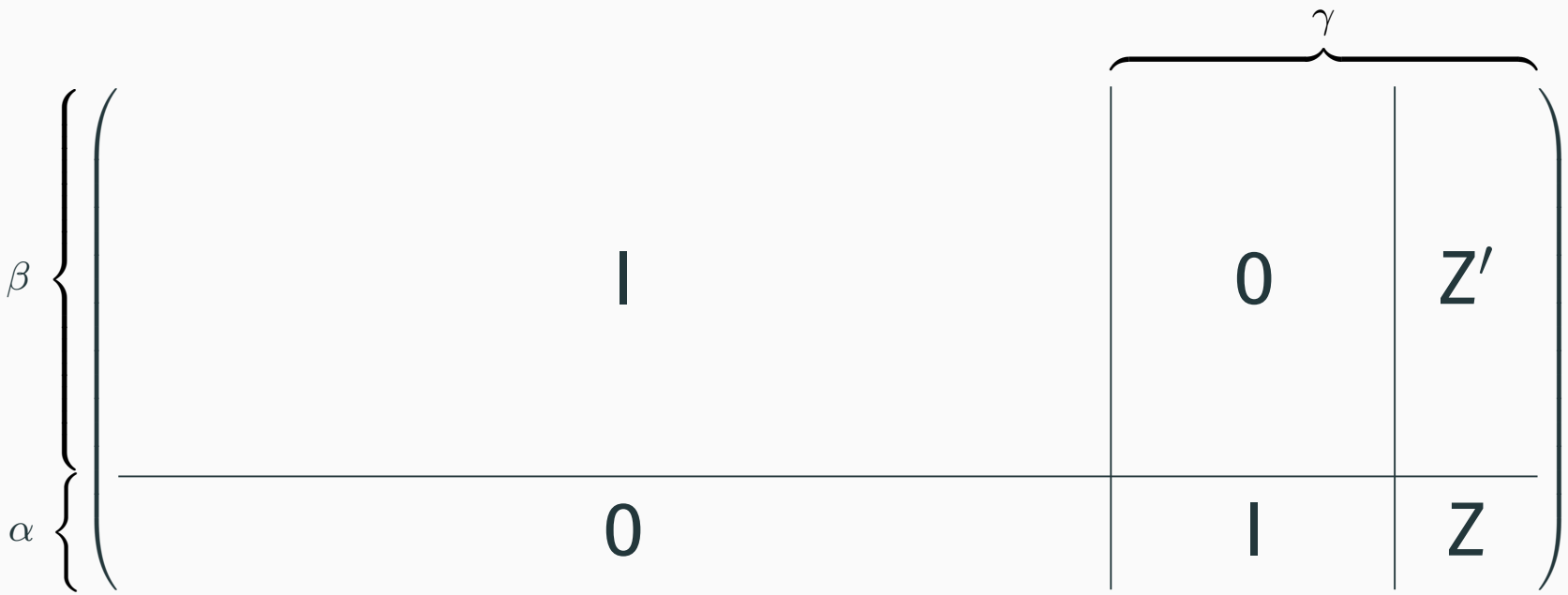
Upper bounds



Step 1. Echelonize $(\mathsf{T} \mid \mathsf{X})$:	$O(\beta^2\gamma^{\omega-2})$	[Jeannerod, Pernet, Storjohann, 2013]
Step 2. Eliminate $(\mathsf{A} \mid \mathsf{Y})$:	$O(\alpha^{\omega-2}\beta\gamma)$	[Knight, 1995]
Step 3. Echelonize $\mathsf{Y} - \mathsf{A}\mathsf{T}^{-1}\mathsf{X}$:	$O(\alpha^{\omega-1}\gamma)$	[Storjohann, 2000]
Step 4. Eliminate P:	$O(\alpha^{\omega-2}\beta\gamma)$	[Knight, 1995]

Cost per degree: $O(\alpha^{\omega-2}\beta\gamma + \beta^2\gamma^{\omega-2})$

Upper bounds



Step 1. Echelonize $(\mathsf{T} \mid \mathsf{X})$:	$O(\beta^2\gamma^{\omega-2})$	[Jeannerod, Pernet, Storjohann, 2013]
Step 2. Eliminate $(\mathsf{A} \mid \mathsf{Y})$:	$O(\alpha^{\omega-2}\beta\gamma)$	[Knight, 1995]
Step 3. Echelonize $\mathsf{Y} - \mathsf{A}\mathsf{T}^{-1}\mathsf{X}$:	$O(\alpha^{\omega-1}\gamma)$	[Storjohann, 2000]
Step 4. Eliminate P:	$O(\alpha^{\omega-2}\beta\gamma)$	[Knight, 1995]

Cost per degree: $O(\alpha^{\omega-2}\beta\gamma + \beta^2\gamma^{\omega-2})$ $\rightsquigarrow$ **Final complexity:** $O(n^{2\omega+3})$

Experimental results

n	r	k	D	d	rank	Std. F_5	Det. F_5
8	6	4	13	7	64	64	64
				8	130	256	130
				9	200	322	200
				10	276	385	276
				11	360	471	360
				12	454	559	454
				13	560	650	560
9	7	4	15	8	81	81	81
				9	164	324	164
				10	251	401	251
				11	344	486	344
				12	445	584	445
				13	556	675	556
				14	679	813	679
				15	816	931	816

n	r	k	D	d	rank	Std. F_5	Det. F_5
4	1	9	4	2	36	36	36
				3	164	324	164
				4	495	582	582
5	2	9	7	3	100	100	100
				4	450	900	450
				5	1278	1956	1956
				6	3002	3546	3546
				7	6435	6685	6685
6	3	9	6	4	225	225	225
				5	1017	2025	1017
				6	2838	4715	4715
7	4	9	6	5	441	441	441
				6	2009	3969	2009

n	r	k	D	d	rank	Std. F_5	Det. F_5
5	1	16	4	2	100	100	100
				3	800	1600	800
				4	3875	4662	4662
6	2	16	4	3	400	400	400
				4	3250	6400	3250

$k =$ number of variables.
$D =$ highest degree appearing in the (reduced) grevlex Gröbner basis for $F_r(M)$.

- When $r = n - 2$, all Macaulay matrices are full rank.
- When $r < n - 2$, the Macaulay matrix in degree $r + 2$ is full rank
- Many reductions to zero remain in higher degrees

Experimental results

n	r	k	D	d	rank	Std. F_5	Det. F_5
8	6	4	13	7	64	64	64
				8	130	256	130
				9	200	322	200
				10	276	385	276
				11	360	471	360
				12	454	559	454
				13	560	650	560
9	7	4	15	8	81	81	81
				9	164	324	164
				10	251	401	251
				11	344	486	344
				12	445	584	445
				13	556		
				14	679		
				15	816		

n	r	k	D	d	rank	Std. F_5	Det. F_5
4	1	9	4	2	36	36	36
				3	164	324	164
				4	495	582	582
5	2	9	7	3	100	100	100
				4	450	900	450
				5	1278	1956	1956
				6	3002	3546	3546
				7	6435	6685	6685
6	3	9	6	4	225	225	225
				5	1017	2025	1017

n	r	k	D	d	rank	Std. F_5	Det. F_5
5	1	16	4	2	100	100	100
				3	800	1600	800
				4	3875	4662	4662
6	2	16	4	3	400	400	400
				4	3250	6400	3250

$\sim 30\%$ of reductions to zero removed in general case

$k =$ number of variables.

$D =$ highest degree appearing in the (reduced) grevlex Gröbner basis for $F_r(M)$.

- When $r = n - 2$, all Macaulay matrices are full rank.
- When $r < n - 2$, the Macaulay matrix in degree $r + 2$ is full rank
- Many reductions to zero remain in higher degrees

Conclusions and perspectives

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.
- In the case $r = n - 2$:

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.
- In the case $r = n - 2$:
  - New algorithm which avoids **all** reductions to zero.

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.
- In the case $r = n - 2$:
  - New algorithm which avoids **all** reductions to zero.
  - Bound on the size of the Gröbner basis: asymptotically n^6 assuming reverse lex property

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.
- In the case $r = n - 2$:
  - New algorithm which avoids **all** reductions to zero.
  - Bound on the size of the Gröbner basis: asymptotically n^6 assuming reverse lex property
  - Subquadratic complexity upper bound: $O(n^{2\omega+3})$ assuming reverse lex property

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.
- In the case $r = n - 2$:
  - New algorithm which avoids **all** reductions to zero.
  - Bound on the size of the Gröbner basis: asymptotically n^6 assuming reverse lex property
  - Subquadratic complexity upper bound: $O(n^{2\omega+3})$ assuming reverse lex property
- Experimental data suggests improved complexity even for $r < n - 2$.

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.
- In the case $r = n - 2$:
  - New algorithm which avoids **all** reductions to zero.
  - Bound on the size of the Gröbner basis: asymptotically n^6 assuming reverse lex property
  - Subquadratic complexity upper bound: $O(n^{2\omega+3})$ assuming reverse lex property
- Experimental data suggests improved complexity even for $r < n - 2$.

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.
- In the case $r = n - 2$:
  - New algorithm which avoids **all** reductions to zero.
  - Bound on the size of the Gröbner basis: asymptotically n^6 assuming reverse lex property
  - Subquadratic complexity upper bound: $O(n^{2\omega+3})$ assuming reverse lex property
- Experimental data suggests improved complexity even for $r < n - 2$.

Future works

- Second syzygies in the general case. [Ma, 1994]

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.
- In the case $r = n - 2$:
  - New algorithm which avoids **all** reductions to zero.
  - Bound on the size of the Gröbner basis: asymptotically n^6 assuming reverse lex property
  - Subquadratic complexity upper bound: $O(n^{2\omega+3})$ assuming reverse lex property
- Experimental data suggests improved complexity even for $r < n - 2$.

Future works

- Second syzygies in the general case. [Ma, 1994]
- Free resolutions of determinantal ideals. [Lascoux, 1978]

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.
- In the case $r = n - 2$:
  - New algorithm which avoids **all** reductions to zero.
  - Bound on the size of the Gröbner basis: asymptotically n^6 assuming reverse lex property
  - Subquadratic complexity upper bound: $O(n^{2\omega+3})$ assuming reverse lex property
- Experimental data suggests improved complexity even for $r < n - 2$.

Future works

- Second syzygies in the general case. [Ma, 1994]
- Free resolutions of determinantal ideals. [Lascoux, 1978]
- The maximal minor case. [Eagon, Northcott, 1962]

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.
- In the case $r = n - 2$:
  - New algorithm which avoids **all** reductions to zero.
  - Bound on the size of the Gröbner basis: asymptotically n^6 assuming reverse lex property
  - Subquadratic complexity upper bound: $O(n^{2\omega+3})$ assuming reverse lex property
- Experimental data suggests improved complexity even for $r < n - 2$.

Future works

- Second syzygies in the general case. [Ma, 1994]
- Free resolutions of determinantal ideals. [Lascoux, 1978]
- The maximal minor case. [Eagon, Northcott, 1962]
- Implications of sharper complexity results for cryptography schemes.

Conclusions and perspectives

Summary

- New F_5-type criteria to identify and avoid reductions to zero for determinantal systems.
- In the case $r = n - 2$:
  - New algorithm which avoids **all** reductions to zero.
  - Bound on the size of the Gröbner basis: asymptotically n^6 assuming reverse lex property
  - Subquadratic complexity upper bound: $O(n^{2\omega+3})$ assuming reverse lex property
- Experimental data suggests improved complexity even for $r < n - 2$.

Future works

- Second syzygies in the general case. [Ma, 1994]
- Free resolutions of determinantal ideals. [Lascoux, 1978]
- The maximal minor case. [Eagon, Northcott, 1962]
- Implications of sharper complexity results for cryptography schemes.
- Efficient implementations of new algorithms.

Thanks. Questions?