Refined F_5 algorithms for ideals of minors of square matrices

SIAM AG '23: Applications of Algebraic Geometry to Post-Quantum Cryptology - Part I of IV

Sriram Gopalakrishnan, Vincent Neiger, Mohab Safey El Din

July 10, 2023

Sorbonne Université, CNRS, LIP6, France

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

$$\begin{pmatrix} f_{11} & f_{12} & \text{[redacted]} & \text{[redacted]} \\ f_{21} & f_{22} & \text{[redacted]} & \text{[redacted]} \end{pmatrix}$$

$$\Downarrow$$

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

Determinantal systems

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

$$\Downarrow$$

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

Determinantal systems

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

$$\Big\Downarrow$$

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

Determinantal systems

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

$$\Downarrow$$

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

Determinantal systems

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

$$\Downarrow$$

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

Determinantal systems

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

$$\Downarrow$$

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

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 $\mathbb{k}[x_1, \dots, x_k]$.

Find $\boldsymbol{a} \in \overline{\mathbb{k}}^k$ with $\mathsf{rank}(M(\boldsymbol{a})) \leq r$.

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 $\mathsf{rank}(M(\boldsymbol{a})) \leq r$.

Determinantal systems

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

$$\Big\Downarrow$$

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

- HFE
- OV

- GeMSS
- Rainbow

The MinRank Problem

$f_{i,j}$ are **linear forms** in $\mathbb{k}[x_1, \dots, x_k]$.

Find $\boldsymbol{a} \in \overline{\mathbb{k}}^k$ with $\mathbf{rank}(M(\boldsymbol{a})) \leq r$.

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

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 ↔ 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 $\mathbf{rank}(M(\boldsymbol{a})) \leq r$.

Macaulay matrices - linearization

Assume F homogeneous.

Macaulay matrices - linearization

Assume F homogeneous.

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

$$\begin{array}{cccc} x^3 & x^2y & xy^2 & y^3 \\ \left(\begin{array}{cccc} & & & \\ & & & \\ & & & \end{array}\right) \end{array}$$

Macaulay matrices - linearization

Assume F homogeneous.

$$\begin{cases} \mathbf{f}_1 = 2x^2 + 11xy - y^2 \\ \mathbf{f}_2 = 4x^2 + xy - 2y^2 \\ \mathbf{f}_3 = -6x^2 - xy + y^2 \end{cases} \xrightarrow{\cdot x} \begin{array}{c|cccc} & x^3 & x^2y & xy^2 & y^3 \\ \hline x\mathbf{f}_1 & 2 & 11 & -1 & 0 \end{array}$$

Macaulay matrices - linearization

Assume F homogeneous.

$$\begin{cases} \mathbf{f}_1 = 2x^2 + 11xy - y^2 \\ \mathbf{f}_2 = 4x^2 + xy - 2y^2 \\ \mathbf{f}_3 = -6x^2 - xy + y^2 \end{cases} \xrightarrow[\cdot y]{\cdot x} \begin{array}{c|cccc} & x^3 & x^2y & xy^2 & y^3 \\ \hline x\mathbf{f}_1 & 2 & 11 & -1 & 0 \\ y\mathbf{f}_1 & 0 & 2 & 11 & -1 \\ & & & & \\ & & & & \end{array}$$

Macaulay matrices - linearization

Assume F homogeneous.

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

$$\begin{tikzcd} f_1 \arrow[r, bend left, "\cdot x"] \arrow[r, "\cdot y"] & x f_1, \; y f_1 \\ f_2 \arrow[r, "\cdot x"] & x f_2 \end{tikzcd}$$

$$\begin{array}{c|cccc} & x^3 & x^2y & xy^2 & y^3 \\ \hline x f_1 & 2 & 11 & -1 & 0 \\ y f_1 & 0 & 2 & 11 & -1 \\ x f_2 & 4 & 1 & -2 & 0 \\ & & & & \\ & & & & \end{array}$$

Macaulay matrices - linearization

Assume F homogeneous.

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

$$\begin{tikzcd} f_1 \arrow[r, bend left, "\cdot x"] \arrow[dr, "\cdot y"] & xf_1 \\ & yf_1 \\ f_2 \arrow[r, "\cdot x"] \arrow[dr, "\cdot y"'] & xf_2 \\ & yf_2 \end{tikzcd}$$

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

Macaulay matrices - linearization

Assume F homogeneous.

$$\begin{tikzcd}
 & xf_1 \\
f_1 = 2x^2 + 11xy - y^2 \arrow[ur, bend left, "\cdot x"] \arrow[r, "\cdot y"] & yf_1 \\
 & xf_2 \\
f_2 = 4x^2 + xy - 2y^2 \arrow[ur, "\cdot x"] \arrow[r, "\cdot y"'] & yf_2 \\
f_3 = -6x^2 - xy + y^2 \arrow[r, "\cdot x"'] & xf_3
\end{tikzcd}$$

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

Macaulay matrices - linearization

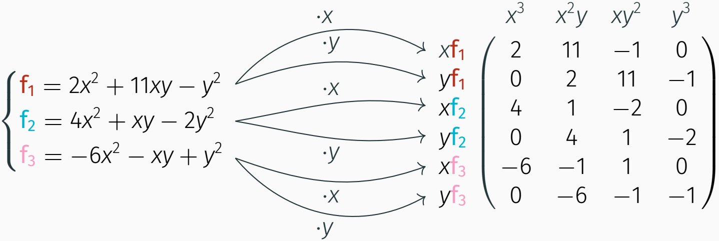
Assume F homogeneous.

$$\begin{tikzcd}
 & xf_1 \\
f_1 = 2x^2 + 11xy - y^2 \arrow[ur, bend left, "\cdot x"] \arrow[r, bend left, "\cdot y"] & yf_1 \\
 & xf_2 \\
f_2 = 4x^2 + xy - 2y^2 \arrow[ur, "\cdot x"] \arrow[r, bend right, "\cdot y"'] & yf_2 \\
f_3 = -6x^2 - xy + y^2 \arrow[r, bend right, "\cdot x"] \arrow[dr, bend right, "\cdot y"'] & xf_3 \\
 & yf_3
\end{tikzcd}$$

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

Macaulay matrices - linearization

Assume F homogeneous.



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

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

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.

$$\begin{tikzcd}
f_1 = 2x^2 + 11xy - y^2 \arrow[r, bend left, "\cdot x"] \arrow[d, phantom] & xf_1 \\
 \arrow[ur, phantom] \arrow[r, phantom] & yf_1 \arrow[from=1-1, "\cdot y"'] \\
f_2 = 4x^2 + xy - 2y^2 \arrow[r, "\cdot x"] \arrow[dr, "\cdot y"'] & xf_2 \\
 & yf_2 \\
f_3 = -6x^2 - xy + y^2 \arrow[r, "\cdot x"] \arrow[dr, bend right, "\cdot y"'] & xf_3 \\
 & yf_3
\end{tikzcd}$$

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

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.

$$\begin{tikzcd}
 & xf_1 \\
f_1 = 2x^2 + 11xy - y^2 \arrow[ur, bend left, "\cdot x"] \arrow[r, "\cdot y"] & yf_1 \\
f_2 = 4x^2 + xy - 2y^2 \arrow[r, "\cdot x"] \arrow[dr, "\cdot y"'] & xf_2 \\
 & yf_2 \\
f_3 = -6x^2 - xy + y^2 \arrow[r, "\cdot y"] \arrow[dr, bend right, "\cdot x"] & xf_3 \\
 & yf_3
\end{tikzcd}$$

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

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

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

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.

$\cdot x$

$\cdot y$

$$\begin{cases} f_1 = 2x \\ f_2 = 4x \\ f_3 = - \end{cases}$$

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

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

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

↑ algebraic property: regularity

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.

$\cdot x$

$\cdot y$

$$\begin{cases} f_1 = 2x \\ f_2 = 4x \\ f_3 = - \end{cases}$$

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

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

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 $\Bbbk = \mathbb{F}_7$, $\succ =$ 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.

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

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

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

The F_5 algorithm ([Faugère, 2002])

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

$$
\begin{aligned}
f_1 &= 5x^2 + 5xy + 3y^2 + 5xz + 5yz + 6z^2\\
f_2 &= 2x^2 + xy + 4y^2 + 2xz + 4z^2\\
f_3 &= 4x^2 + xy + 4y^2 + 3xz + 5yz + 2z^2
\end{aligned}
$$

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

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

$$\mathcal{M}_4$$

$$
\begin{array}{c|ccccccccccccccc}
 & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4\\
\hline
(1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0\\
(1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0\\
(1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0\\
(1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0\\
(1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0\\
(1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6\\
(2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0\\
(2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0\\
(2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0\\
(2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0\\
(2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0\\
(2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4\\
(3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0\\
(3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0\\
(3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0\\
(3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0\\
(3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0\\
(3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2
\end{array}
$$

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

$$\mathcal{M}_4$$

$$\begin{array}{c|ccccccccccccccc}
 & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\
\hline
(1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\
(1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\
(1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\
(1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\
(1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\
(1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\
(2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
(2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\
(2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\
(2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\
(2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\
(2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\
(3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
(3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
(3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\
(3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\
(3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\
(3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2
\end{array}$$

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

$$\mathcal{M}_4$$

$$\begin{array}{c|ccccccccccccccc}
 & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\
\hline
(1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\
(1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\
(1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\
(1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\
(1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\
(1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\
(2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
(2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\
(2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\
(2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\
(2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\
(2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\
(3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
(3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
(3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\
(3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\
(3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\
(3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2
\end{array}$$

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

$$\mathcal{M}_4$$

$$\begin{array}{c|ccccccccccccccc} & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\ \hline (1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\ (1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ (1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\ (1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\ (1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\ (1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\ (2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ (2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ (2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ (2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\ (2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\ (2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\ (3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ (3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ (3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\ (3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\ (3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\ (3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2 \end{array}$$

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

$$\mathcal{M}_4$$

$$\begin{array}{c|ccccccccccccccc}
 & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\
\hline
(1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\
(1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\
(1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\
(1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\
(1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\
(1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\
(2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
(2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\
(2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\
(2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\
(2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\
(2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\
(3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
(3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
(3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\
(3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\
(3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\
(3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2
\end{array}$$

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

$$\mathcal{M}_4$$

$$\begin{array}{c|ccccccccccccccc}
 & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\
\hline
(1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\
(1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\
(1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\
(1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\
(1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\
(1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\
(2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
(2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\
(2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\
(2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\
(2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\
(2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\
(3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
(3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
(3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\
(3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\
(3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\
(3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2
\end{array}$$

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

Lazard: $\mathcal{M}_4$ is 18×15.

$$\mathcal{M}_4$$

$$\begin{array}{c|ccccccccccccccc}
 & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\
\hline
(1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\
(1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\
(1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\
(1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\
(1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\
(1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\
(2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
(2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\
(2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\
(2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\
(2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\
(2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\
(3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
(3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
(3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\
(3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\
(3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\
(3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2
\end{array}$$

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

Lazard: $\mathcal{M}_4$ is 18×15.

F$_5$: $\mathcal{M}_4$ is 15×15 and full rank!

$$\mathcal{M}_4$$

$$\begin{array}{c|ccccccccccccccc}
 & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\
(1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\
(1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\
(1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\
(1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\
(1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\
(1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\
(2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
(2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\
(2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\
(2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\
(2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\
(2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\
(3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
(3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
(3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\
(3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\
(3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\
(3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2
\end{array}$$

The F_5 algorithm ([Faugère, 2002])

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

$(f_1, \ldots, f_m)$ generic

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

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

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

Lazard: $\mathcal{M}_4$ is 18 × 15.

F$_5$: $\mathcal{M}_4$ is 15 × 15 and full rank!

$$\mathcal{M}_4$$

$$\begin{array}{c|ccccccccccccccc} & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\ \hline (1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\ (1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ (1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\ (1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\ (1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\ (1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\ (2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ (2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ (2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ (2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\ (2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\ (2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\ (3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ (3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ (3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\ (3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\ (3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\ (3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2 \end{array}$$

The F_5 algorithm ([Faugère, 2002])

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

$(f_1, \ldots, f_m)$ generic

$$\Downarrow$$

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

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

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

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

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

Lazard: $\mathcal{M}_4$ is 18×15.

F$_5$: $\mathcal{M}_4$ is 15×15 and full rank!

$$\mathcal{M}_4$$

$$\begin{array}{c|ccccccccccccccc} & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\ \hline (1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\ (1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ (1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\ (1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\ (1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\ (1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\ (2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ (2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ (2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ (2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\ (2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\ (2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\ (3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ (3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ (3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\ (3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\ (3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\ (3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2 \end{array}$$

The F_5 algorithm ([Faugère, 2002])

Let $\Bbbk = \mathbb{F}_7$, $\succ =$ 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

$$\Downarrow$$

$\Big\{$ **No** reductions to zero.

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

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

Lazard: $\mathcal{M}_4$ is 18×15.

F$_5$: $\mathcal{M}_4$ is 15×15 and full rank!

$$\mathcal{M}_4$$

$$\begin{array}{c|ccccccccccccccc}
 & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\
\hline
(1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\
(1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\
(1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\
(1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\
(1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\
(1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\
(2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
(2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\
(2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\
(2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\
(2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\
(2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\
(3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
(3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
(3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\
(3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\
(3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\
(3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2
\end{array}$$

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

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

Lazard: $\mathcal{M}_4$ is 18×15.

F$_5$: $\mathcal{M}_4$ is 15×15 and full rank!

$(f_1, \dots, f_m)$ generic

$$\Downarrow$$

$$\begin{cases} \textbf{No} \text{ reductions to zero.} \\ \text{Precise complexity analysis [1]} \end{cases}$$

$$\mathcal{M}_4$$

$$\begin{array}{c|ccccccccccccccc}
 & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\
\hline
(1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\
(1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\
(1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\
(1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\
(1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\
(1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\
(2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
(2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\
(2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\
(2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\
(2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\
(2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\
(3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
(3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
(3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\
(3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\
(3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\
(3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2
\end{array}$$

[1] [Bardet, Faugère, Salvy, 2015]

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

$(f_1, \ldots, f_m)$ generic

$$\Downarrow$$

zero.

y analysis [1]

Determinantal systems are not generic!

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

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

Lazard: $\mathcal{M}_4$ is 18 × 15.

F$_5$: $\mathcal{M}_4$ is 15 × 15 and full rank!

$$\begin{array}{c|ccccccccccccccc} & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\ \hline (1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\ (1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ (1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\ (1,xz) & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 & 0 \\ (1,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 0 & 5 & 5 & 0 & 6 & 0 \\ (1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\ (2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ (2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ (2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ (2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\ (2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\ (2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\ (3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ (3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ (3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\ (3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\ (3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\ (3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2 \end{array}$$

[1] [Bardet, Faugère, Salvy, 2015]

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

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

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

Lazard: $\mathcal{M}_4$ is 18×15.

F$_5$: $\mathcal{M}_4$ is 15×15 and full rank!

$(f_1, \ldots, f_m)$ generic

$\Downarrow$

zero.

y analysis [1]

Determinantal systems are not generic!

How do we remove reductions to zero?

$$\begin{array}{c|ccccccccccccccc} & x^4 & x^3y & x^2y^2 & xy^3 & y^4 & x^3z & x^2yz & xy^2z & y^3z & x^2z^2 & xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \\ \hline (1,x^2) & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\ (1,xy) & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ (1,y^2) & 0 & 0 & 5 & 5 & 3 & 0 & 0 & 5 & 5 & 0 & 0 & 6 & 0 & 0 & 0 \\ & & & & & & & & & & 5 & 5 & 0 & 6 & 0 & 0 \\ & & & & & & & & & & 0 & 5 & 5 & 0 & 6 & 0 \\ (1,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 3 & 5 & 5 & 6 \\ (2,x^2) & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ (2,xy) & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ (2,y^2) & 0 & 0 & 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ (2,xz) & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\ (2,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 0 & 2 & 0 & 0 & 4 & 0 \\ (2,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 2 & 0 & 4 \\ (3,x^2) & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ (3,xy) & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ (3,y^2) & 0 & 0 & 4 & 1 & 4 & 0 & 0 & 3 & 5 & 0 & 0 & 2 & 0 & 0 & 0 \\ (3,xz) & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 & 0 \\ (3,yz) & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 0 & 3 & 5 & 0 & 2 & 0 \\ (3,z^2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 3 & 5 & 2 \end{array}$$

[1] [Bardet, Faugère, Salvy, 2015]

Contributions - to appear in the proceedings of ISSAC ’23

Contributions - to appear in the proceedings of ISSAC '23

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 - to appear in the proceedings of ISSAC ’23

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 - to appear in the proceedings of ISSAC ’23

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 - to appear in the proceedings of ISSAC '23

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 - to appear in the proceedings of ISSAC ’23

M is an $n \times n$ matrix of generic linear forms over $\Bbbk[x_1, \dots, x_k]$, $r \leq n-1$. 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 - to appear in the proceedings of ISSAC ’23

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: $O(n^{4\omega-1}) \rightsquigarrow \begin{array}{c} O(n^{2\omega+3}) \\ \Omega(n^6) \end{array}$

Preprint Coming Soon

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

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 $f_1, \ldots, f_m$.

Syzygies

Definition (Syzygy)

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

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

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

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)

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

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

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

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)

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

$$\Downarrow$$

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

Syzygies

Definition (Syzygy)

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

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

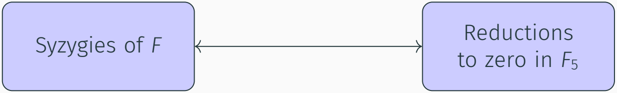
is called a **syzygy** of $f_1, \dots, f_m$.

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)

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

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

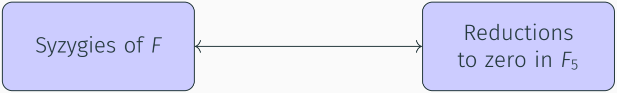
is called a **syzygy** of $f_1, \dots, f_m$.

Example (Koszul syzygies)

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

$$\Downarrow$$

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



Syzygies of F

Reductions to zero in F_5

Theorem ([Hilbert, 1890])

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

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

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.

$$\begin{tikzcd}
& \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ \times & \times & \times & \times \end{pmatrix} \\
\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix} \arrow[ur, "\text{Type I}"] &
\end{tikzcd}$$

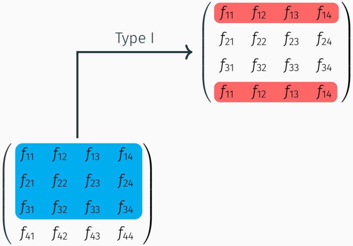
The Gulliksen-Negård complex

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

$$\begin{tikzcd}
 & \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ \times & \times & \times & \times \end{pmatrix} \\
\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix} \arrow[ur, "\text{Type I}"] &
\end{tikzcd}$$

The Gulliksen-Negård complex

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



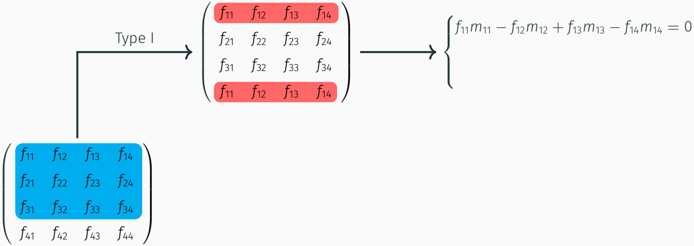
Type I

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

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

The Gulliksen-Negård complex

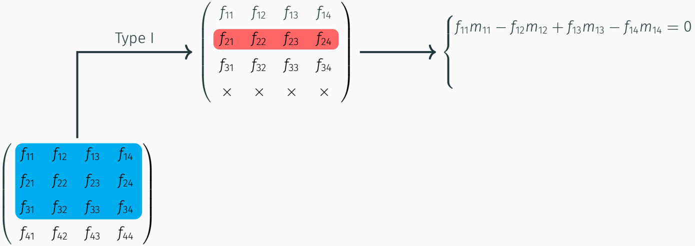
m_{ij} = determinant of submatrix of M given by deleting i-th row, j-th column.



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

The Gulliksen-Negård complex

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



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

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

The Gulliksen-Negård complex

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

$$\begin{tikzcd}
 & \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{21} & f_{22} & f_{23} & f_{24} \end{pmatrix} \arrow[r] & \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ \\ \end{cases} \\
\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix} \arrow[ur, "\text{Type I}"] & &
\end{tikzcd}$$

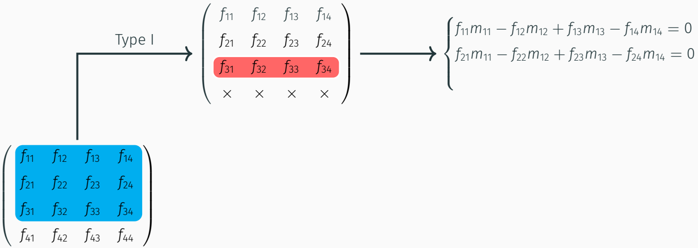
The Gulliksen-Negård complex

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

$$\begin{tikzcd}
 & \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{21} & f_{22} & f_{23} & f_{24} \end{pmatrix} \arrow[r] & \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ \end{cases} \\
\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix} \arrow[ur, "\text{Type I}"] & &
\end{tikzcd}$$

The Gulliksen-Negård complex

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



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

The Gulliksen-Negård complex

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

$$\begin{tikzcd}
 & \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{31} & f_{32} & f_{33} & f_{34} \end{pmatrix} \arrow[r] & \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ \end{cases} \\
\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix} \arrow[ur, "\text{Type I}"] & &
\end{tikzcd}$$

The Gulliksen-Negård complex

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

$$\begin{tikzcd}[ampersand replacement=\&]
 \& \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{31} & f_{32} & f_{33} & f_{34} \end{pmatrix} \arrow[r] \& \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ f_{31}m_{11} - f_{32}m_{12} + f_{33}m_{13} - f_{34}m_{14} = 0 \end{cases} \\
\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix} \arrow[ur, "\text{Type I}"] \& \&
\end{tikzcd}$$

The Gulliksen-Negård complex

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

$$\begin{tikzcd}
 & \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ \times & \times & \times & \times \end{pmatrix} \arrow[r] & \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ f_{31}m_{11} - f_{32}m_{12} + f_{33}m_{13} - f_{34}m_{14} = 0 \end{cases} \\
\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix} \arrow[ur, "\text{Type I}"] & &
\end{tikzcd}$$

The Gulliksen-Negård complex

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

$$\begin{tikzcd}
 & \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ \times & \times & \times & \times \end{pmatrix} \arrow[r] & \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ f_{31}m_{11} - f_{32}m_{12} + f_{33}m_{13} - f_{34}m_{14} = 0 \end{cases} \\
\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix} \arrow[ur, "\text{Type I}"] & &
\end{tikzcd}$$

The Gulliksen-Negård complex

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

$$\begin{tikzcd}[ampersand replacement=\&]
 \& \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ \times & \times & \times & \times \end{pmatrix} \arrow[r] \& \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ f_{31}m_{11} - f_{32}m_{12} + f_{33}m_{13} - f_{34}m_{14} = 0 \end{cases} \\
\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix} \arrow[ur, "\text{Type I}"] \arrow[dr, "\text{Type II}"'] \& \& \\
 \& f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} \&
\end{tikzcd}$$

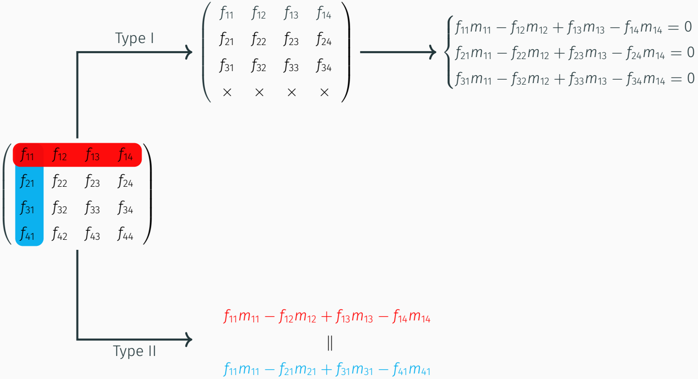
The Gulliksen-Negård complex

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

$$\begin{tikzcd}
& \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ \times & \times & \times & \times \end{pmatrix} \arrow[r] & \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ f_{31}m_{11} - f_{32}m_{12} + f_{33}m_{13} - f_{34}m_{14} = 0 \end{cases} \\
\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ f_{41} & f_{42} & f_{43} & f_{44} \end{pmatrix} \arrow[ur, "\text{Type I}"] \arrow[dr, "\text{Type II}"'] & & \\
& f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} &
\end{tikzcd}$$

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

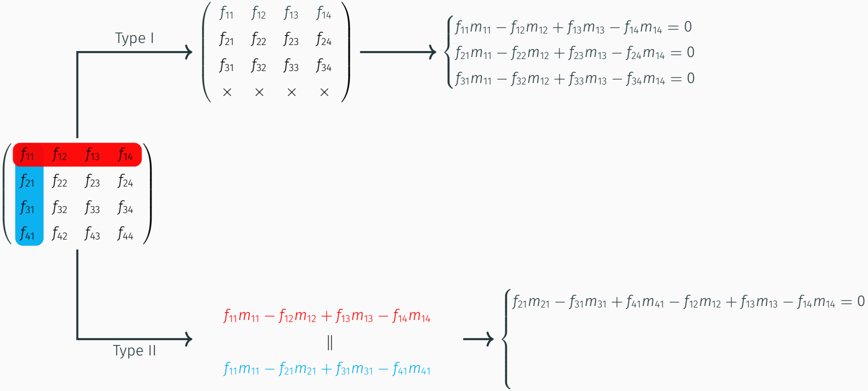
$$f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14}$$

$$\|$$

$$f_{11}m_{11} - f_{21}m_{21} + f_{31}m_{31} - f_{41}m_{41}$$

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

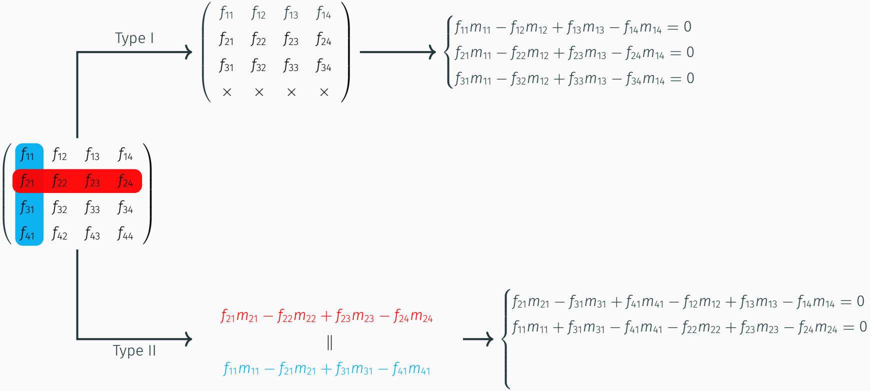
$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ \times & \times & \times & \times \end{pmatrix} \longrightarrow \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} +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

Type II

$$\begin{array}{c} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} \\ \| \\ f_{11}m_{11} - f_{21}m_{21} + f_{31}m_{31} - f_{41}m_{41} \end{array} \longrightarrow \begin{cases} f_{21}m_{21} - f_{31}m_{31} + f_{41}m_{41} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ \\ \\ \end{cases}$$

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

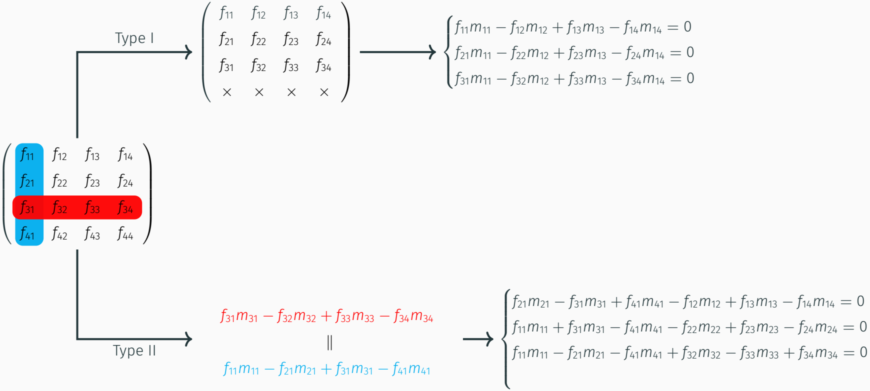
$$\begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ f_{31} & f_{32} & f_{33} & f_{34} \\ \times & \times & \times & \times \end{pmatrix} \longrightarrow \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} +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

Type II

$$\begin{array}{c} f_{21}m_{21} - f_{22}m_{22} + f_{23}m_{23} - f_{24}m_{24} \\ \| \\ f_{11}m_{11} - f_{21}m_{21} + f_{31}m_{31} - f_{41}m_{41} \end{array} \longrightarrow \begin{cases} f_{21}m_{21} - f_{31}m_{31} + f_{41}m_{41} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{11}m_{11} + f_{31}m_{31} - f_{41}m_{41} - f_{22}m_{22} + f_{23}m_{23} - f_{24}m_{24} = 0 \\ \\ \end{cases}$$

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

$$f_{31}m_{31} - f_{32}m_{32} + f_{33}m_{33} - f_{34}m_{34}$$

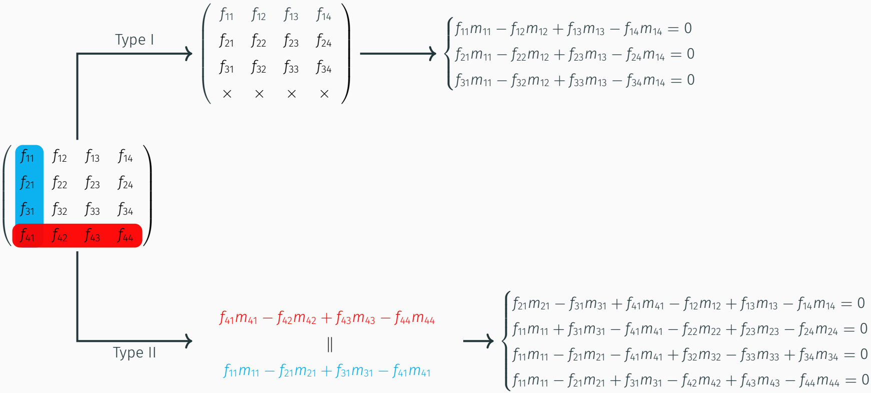
$$\|$$

$$f_{11}m_{11} - f_{21}m_{21} + f_{31}m_{31} - f_{41}m_{41}$$

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

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

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

The Gulliksen-Negård complex

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

$$\begin{tikzcd}[ampersand replacement=\&]
 \& \begin{pmatrix} f_{11} \& f_{12} \& f_{13} \& f_{14} \\ f_{21} \& f_{22} \& f_{23} \& f_{24} \\ f_{31} \& f_{32} \& f_{33} \& f_{34} \\ \times \& \times \& \times \& \times \end{pmatrix} \arrow[r] \& \begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ f_{31}m_{11} - f_{32}m_{12} + f_{33}m_{13} - f_{34}m_{14} = 0 \end{cases} \\
\begin{pmatrix} f_{11} \& f_{12} \& f_{13} \& f_{14} \\ f_{21} \& f_{22} \& f_{23} \& f_{24} \\ f_{31} \& f_{32} \& f_{33} \& f_{34} \\ f_{41} \& f_{42} \& f_{43} \& f_{44} \end{pmatrix} \arrow[ur, "\text{Type I}"] \arrow[dr, "\text{Type II}"'] \& \& \\
 \& \begin{matrix} \textcolor{red}{f_{41}m_{41} - f_{42}m_{42} + f_{43}m_{43} - f_{44}m_{44}} \\ \| \\ \textcolor{cyan}{f_{11}m_{11} - f_{21}m_{21} + f_{31}m_{31} - f_{41}m_{41}} \end{matrix} \arrow[r] \& \begin{cases} f_{21}m_{21} - f_{31}m_{31} + f_{41}m_{41} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{11}m_{11} + f_{31}m_{31} - f_{41}m_{41} - f_{22}m_{22} + f_{23}m_{23} - f_{24}m_{24} = 0 \\ f_{11}m_{11} - f_{21}m_{21} - f_{41}m_{41} + f_{32}m_{32} - f_{33}m_{33} + f_{34}m_{34} = 0 \\ f_{11}m_{11} - f_{21}m_{21} + f_{31}m_{31} - f_{42}m_{42} + f_{43}m_{43} - f_{44}m_{44} = 0 \end{cases}
\end{tikzcd}$$

Theorem ([Kurano, 1989])

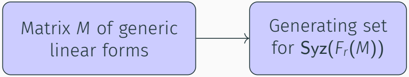
The syzygies between the $(r+1)$-minors of M are generated by the syzygies between the $(r+1)$ minors of the $(r+2) \times (r+2)$ submatrices of M.

New F_5 algorithms - the general case

New F_5 algorithms - the general case

Matrix M of generic linear forms

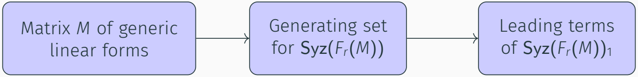
New F_5 algorithms - the general case



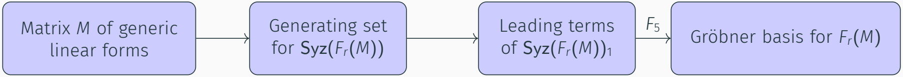
Matrix M of generic linear forms

Generating set for $\mathrm{Syz}(F_r(M))$

New F_5 algorithms - the general case


Matrix M of generic linear forms
Generating set for $\mathrm{Syz}(F_r(M))$
Leading terms of $\mathrm{Syz}(F_r(M))_1$

New F_5 algorithms - the general case



Matrix M of generic linear forms

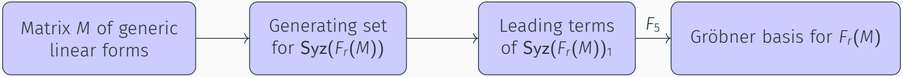
Generating set for $\mathrm{Syz}(F_r(M))$

Leading terms of $\mathrm{Syz}(F_r(M))_1$

F_5

Gröbner basis for $F_r(M)$

New F_5 algorithms - the general case



Matrix M of generic linear forms

Generating set for $\mathrm{Syz}(F_r(M))$

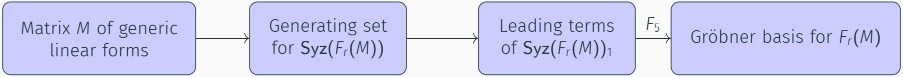
Leading terms of $\mathrm{Syz}(F_r(M))_1$

F_5

Gröbner basis for $F_r(M)$

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

New F_5 algorithms - the general case



Matrix M of generic linear forms

Generating set for $\mathrm{Syz}(F_r(M))$

Leading terms of $\mathrm{Syz}(F_r(M))_1$

F_5

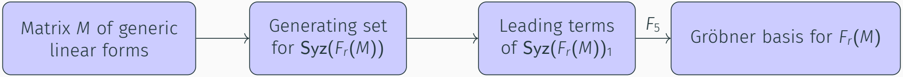
Gröbner basis for $F_r(M)$

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

Theorem ([Eagon, Hochster, 1971])

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

New F_5 algorithms - the general case



Matrix M of generic linear forms

Generating set for $\mathrm{Syz}(F_r(M))$

Leading terms of $\mathrm{Syz}(F_r(M))_1$

F_5

Gröbner basis for $F_r(M)$

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

Theorem ([Eagon, Hochster, 1971])

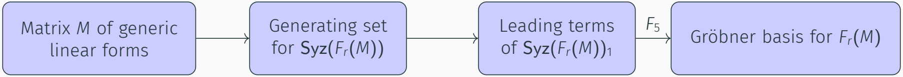
$F_r(M)$ has a free resolution of length $(n-r)^2$.

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

for

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

New F_5 algorithms - the general case



Matrix M of generic linear forms

Generating set for $\mathrm{Syz}(F_r(M))$

Leading terms of $\mathrm{Syz}(F_r(M))_1$

F_5

Gröbner basis for $F_r(M)$

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

Theorem ([Eagon, Hochster, 1971])

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

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

for

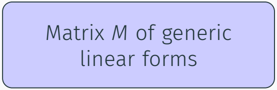
$1 < k < (n-r)^2$.

$\Longrightarrow$

Cannot efficiently compute a Gröbner basis for $\mathrm{Syz}(F_r(M))$

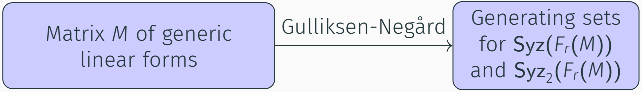
New F_5 algorithms - the case $r = n - 2$

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



Matrix M of generic linear forms

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

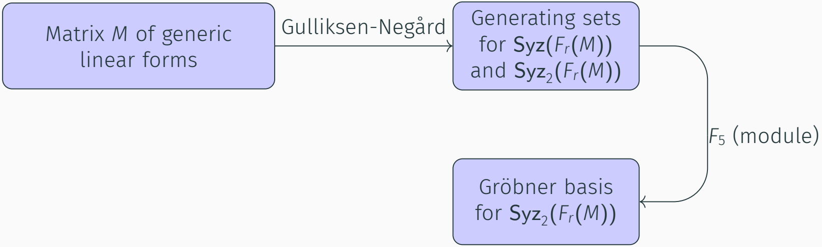


Matrix M of generic linear forms

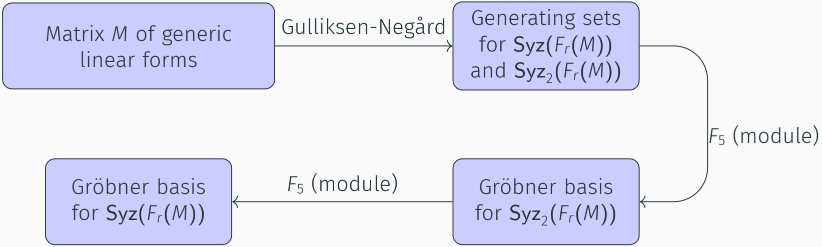
Gulliksen-Negård

Generating sets for $\mathrm{Syz}(F_r(M))$ and $\mathrm{Syz}_2(F_r(M))$

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


Matrix M of generic linear forms
Gulliksen-Negård
Generating sets for $\mathrm{Syz}(F_r(M))$ and $\mathrm{Syz}_2(F_r(M))$
F_5 (module)
Gröbner basis for $\mathrm{Syz}_2(F_r(M))$

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



Matrix M of generic linear forms

Gulliksen-Negård

Generating sets for $\mathrm{Syz}(F_r(M))$ and $\mathrm{Syz}_2(F_r(M))$

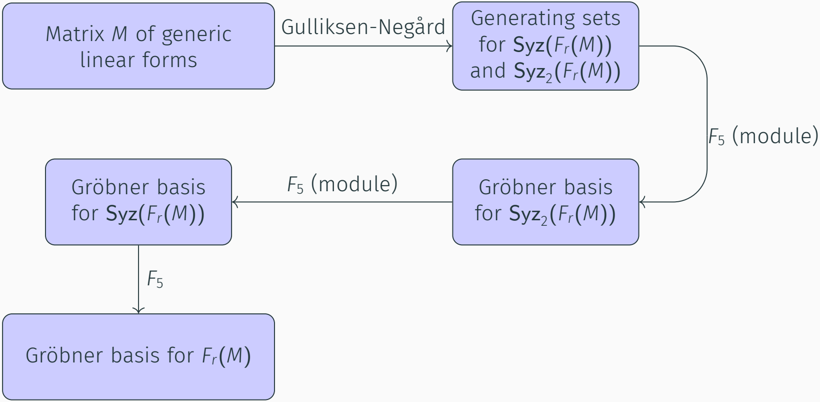
F_5 (module)

Gröbner basis for $\mathrm{Syz}_2(F_r(M))$

F_5 (module)

Gröbner basis for $\mathrm{Syz}(F_r(M))$

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



Matrix M of generic linear forms

Gulliksen-Negård

Generating sets for $\mathrm{Syz}(F_r(M))$ and $\mathrm{Syz}_2(F_r(M))$

F_5 (module)

Gröbner basis for $\mathrm{Syz}_2(F_r(M))$

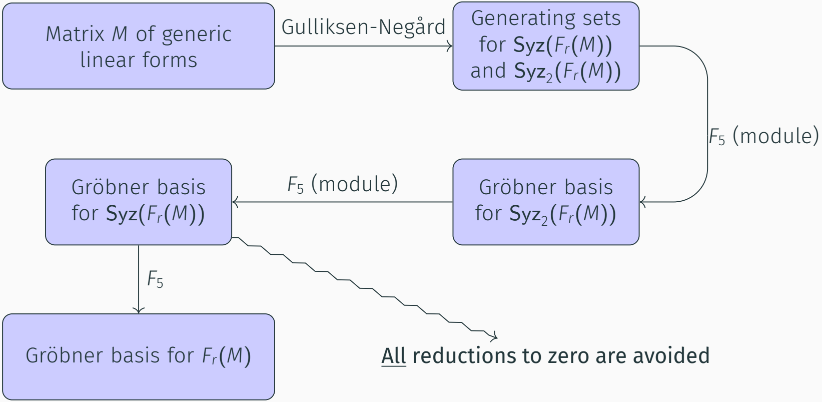
F_5 (module)

Gröbner basis for $\mathrm{Syz}(F_r(M))$

F_5

Gröbner basis for $F_r(M)$

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



Matrix M of generic linear forms

Gulliksen-Negård

Generating sets for $\mathrm{Syz}(F_r(M))$ and $\mathrm{Syz}_2(F_r(M))$

F_5 (module)

Gröbner basis for $\mathrm{Syz}_2(F_r(M))$

F_5 (module)

Gröbner basis for $\mathrm{Syz}(F_r(M))$

F_5

Gröbner basis for $F_r(M)$

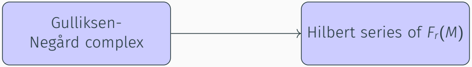
All reductions to zero are avoided

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

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

Gulliksen-Negård complex

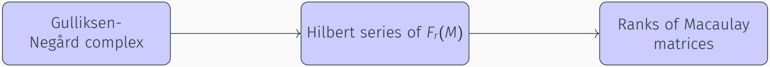
A complexity analysis in the case $r = n - 2$



Gulliksen-Negård complex

Hilbert series of $F_r(M)$

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

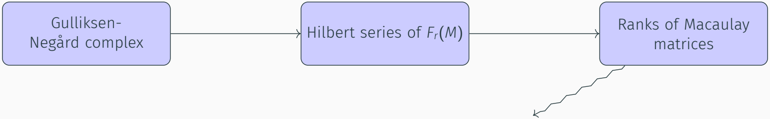


Gulliksen-Negård complex

Hilbert series of $F_r(M)$

Ranks of Macaulay matrices

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

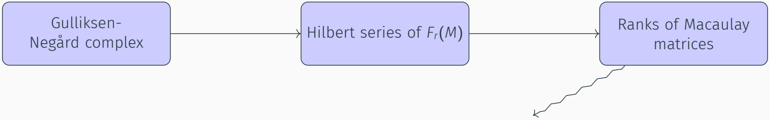


Theorem ([G., Neiger, Safey, 2023])

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

$$O\left(\left(\sum_{d=n-1}^{2n-3} \frac{(d^2 + (-2n+4)d + 4n^2 - 4n + 3)(2 + d - n)}{3}\right)^{\omega - 1} \binom{2n+1}{5}\right).$$

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



Gulliksen-Negård complex

Hilbert series of $F_r(M)$

Ranks of Macaulay matrices

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

$$O\left(\left(\sum_{d=n-1}^{2n-3} \frac{(d^2+(-2n+4)d+4n^2-4n+3)(2+d-n)}{3}\right)^{\omega-1}\binom{2n+1}{5}\right).$$

Asymptotically:

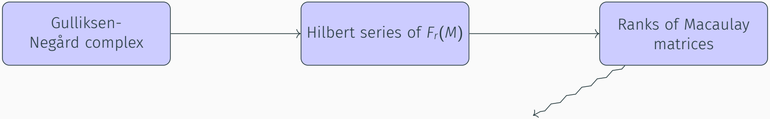
[Faugère, Safey, Spaenlehauer, 2013]

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

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

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

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



Gulliksen-Negård complex

Hilbert series of $F_r(M)$

Ranks of Macaulay matrices

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

$$O\left(\left(\sum_{d=n-1}^{2n-3} \frac{(d^2 + (-2n+4)d + 4n^2 - 4n + 3)(2 + d - n)}{3}\right)^{\omega-1} \binom{2n+1}{5}\right).$$

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 $O(n^{2\omega+3})$ and established lower bound $\Omega(n^6)$.

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	[illegible]	[illegible]
				14	679	[illegible]	[illegible]
				15	816	[illegible]	[illegible]

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 future works

Conclusions and future works

Summary

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

Conclusions and future works

Summary

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

Conclusions and future works

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 future works

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.
  - Explicit Hilbert series leading to new complexity bound.

Conclusions and future works

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.
  - Explicit Hilbert series leading to new complexity bound.
- Experimental data suggests improved complexity in general.

Conclusions and future works

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.
    - Explicit Hilbert series leading to new complexity bound.
- Experimental data suggests improved complexity in general.

Conclusions and future works

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.
  - Explicit Hilbert series leading to new complexity bound.
- Experimental data suggests improved complexity in general.

Future works

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

Conclusions and future works

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.
  - Explicit Hilbert series leading to new complexity bound.
- Experimental data suggests improved complexity in general.

Future works

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

Conclusions and future works

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.
    - Explicit Hilbert series leading to new complexity bound.
- Experimental data suggests improved complexity in general.

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 future works

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.
  - Explicit Hilbert series leading to new complexity bound.
- Experimental data suggests improved complexity in general.

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 future works

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.
  - Explicit Hilbert series leading to new complexity bound.
- Experimental data suggests improved complexity in general.

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?

Sharper complexity bounds

$$\begin{array}{cc}
 & \begin{matrix} x_1^2 & x_1x_2 & \cdots & x_ax_b & \cdots & x_{k-1}x_k & x_k^2 \end{matrix} \\
\begin{matrix} f_1 \\ f_2 \\ \vdots \\ f_m \end{matrix} & \begin{pmatrix} 1 & 0 & \cdots & 0 & \times & \times & \times \\ 0 & 1 & \cdots & 0 & \vdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \times & \times & \times \\ 0 & 0 & \cdots & 1 & \times & \times & \times \end{pmatrix} \\
 & \begin{matrix} \underbrace{\hphantom{x_1^2 \quad x_1x_2 \quad \cdots \quad x_ax_b}}_{\substack{\text{Identity block} \\ \text{(reverse lexicographic ideal)}}} & \underbrace{\hphantom{\cdots \quad x_{k-1}x_k \quad x_k^2}}_{\text{Dense block}} \end{matrix}
\end{array}$$

Sharper complexity bounds

$$\begin{array}{c|ccccccc}
 & x_1^2 & x_1x_2 & \cdots & x_ax_b & \cdots & x_{k-1}x_k & x_k^2 \\
\hline
f_1 & 1 & 0 & \cdots & 0 & \times & \times & \times \\
f_2 & 0 & 1 & \cdots & 0 & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \times & \times & \times \\
f_m & 0 & 0 & \cdots & 1 & \times & \times & \times \\
 & \multicolumn{4}{c}{\underbrace{\hphantom{1\quad 0\quad \cdots\quad 0}}_{\substack{\text{Identity block}\\ \text{(reverse lexicographic ideal)}}}} & \multicolumn{3}{c}{\underbrace{\hphantom{\times\quad \times\quad \times}}_{\text{Dense block}}}
\end{array}$$

$$\begin{array}{c|ccccccc}
 & x_1^3 & x_1^2x_2 & \cdots & x_kx_ax_b & \cdots & x_{k-1}x_k^2 & x_k^3 \\
\hline
x_1f_1 & 1 & 0 & \cdots & 0 & \times & \times & \times \\
x_2f_1 & 0 & 1 & \cdots & 0 & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
x_1f_2 & 0 & 1 & \cdots & 0 & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \times & \times & \times \\
x_kf_m & 0 & 0 & \cdots & 1 & \times & \times & \times
\end{array}$$

Sharper complexity bounds

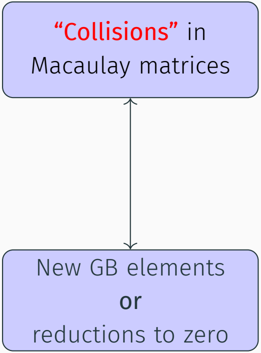
$$\begin{array}{cc}
 & \begin{array}{ccccccc} x_1^2 & x_1x_2 & \cdots & x_ax_b & \cdots & x_{k-1}x_k & x_k^2 \end{array} \\
\begin{array}{c} f_1 \\ f_2 \\ \vdots \\ f_m \end{array} & \left(\underbrace{\begin{array}{cccc} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{array}}_{\substack{\text{Identity block} \\ \text{(reverse lexicographic ideal)}}} \; \underbrace{\begin{array}{ccc} \times & \times & \times \\ \vdots & \vdots & \vdots \\ \times & \times & \times \\ \times & \times & \times \end{array}}_{\text{Dense block}} \right)
\end{array}$$

$$\begin{array}{c|ccccccc}
 & x_1^3 & x_1^2x_2 & \cdots & x_kx_ax_b & \cdots & x_{k-1}x_k^2 & x_k^3 \\
\hline
x_1f_1 & 1 & 0 & \cdots & 0 & \times & \times & \times \\
x_2f_1 & 0 & \boxed{1} & \cdots & 0 & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
x_1f_2 & 0 & \boxed{1} & \cdots & 0 & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \times & \times & \times \\
x_kf_m & 0 & 0 & \cdots & 1 & \times & \times & \times
\end{array}$$

Sharper complexity bounds

$$\begin{array}{cccccccc}
 & x_1^2 & x_1x_2 & \cdots & x_ax_b & \cdots & x_{k-1}x_k & x_k^2 \\
f_1 & 1 & 0 & \cdots & 0 & \times & \times & \times \\
f_2 & 0 & 1 & \cdots & 0 & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \times & \times & \times \\
f_m & 0 & 0 & \cdots & 1 & \times & \times & \times \\
 & \multicolumn{4}{c}{\underbrace{\hphantom{xxxxxxxxxxxxxxxx}}_{\text{Identity block (reverse lexicographic ideal)}}} & \multicolumn{3}{c}{\underbrace{\hphantom{xxxxxxxxxxxx}}_{\text{Dense block}}}
\end{array}$$

$$\begin{array}{cccccccc}
 & x_1^3 & x_1^2x_2 & \cdots & x_kx_ax_b & \cdots & x_{k-1}x_k^2 & x_k^3 \\
x_1f_1 & 1 & 0 & \cdots & 0 & \times & \times & \times \\
x_2f_1 & 0 & \boxed{1} & \cdots & 0 & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
x_1f_2 & 0 & \boxed{1} & \cdots & 0 & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \times & \times & \times \\
x_kf_m & 0 & 0 & \cdots & 1 & \times & \times & \times
\end{array}$$


"Collisions" in Macaulay matrices

New GB elements
or
reductions to zero

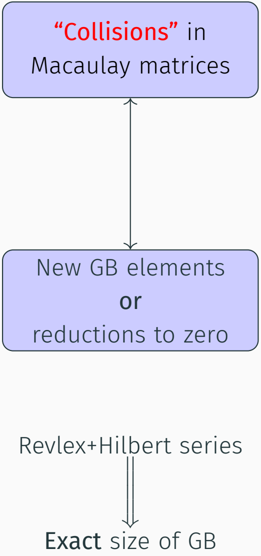
Sharper complexity bounds

$$\begin{array}{c|ccccccc}
 & x_1^2 & x_1x_2 & \cdots & x_ax_b & \cdots & x_{k-1}x_k & x_k^2 \\
\hline
f_1 & 1 & 0 & \cdots & 0 & \times & \times & \times \\
f_2 & 0 & 1 & \cdots & 0 & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \times & \times & \times \\
f_m & 0 & 0 & \cdots & 1 & \times & \times & \times
\end{array}$$

Identity block
(reverse lexicographic ideal)

Dense block

$$\begin{array}{c|ccccccc}
 & x_1^3 & x_1^2x_2 & \cdots & x_kx_ax_b & \cdots & x_{k-1}x_k^2 & x_k^3 \\
\hline
x_1f_1 & 1 & 0 & \cdots & 0 & \times & \times & \times \\
x_2f_1 & 0 & \boxed{1} & \cdots & 0 & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
x_1f_2 & 0 & \boxed{1} & \cdots & 0 & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \times & \times & \times \\
x_kf_m & 0 & 0 & \cdots & 1 & \times & \times & \times
\end{array}$$



"Collisions" in Macaulay matrices

New GB elements **or** reductions to zero

Revlex+Hilbert series

$\Downarrow$

Exact size of GB