Refined F_5 algorithms for ideals of minors of square matrices

Sriram Gopalakrishnan, Vincent Neiger, Mohab Safey El Din

JNCF, April 15, 2024

Sorbonne Université

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

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

$$\Downarrow$$

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

Determinantal systems

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

$$\Downarrow$$

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

Determinantal systems

$$\begin{pmatrix} f_{11} & \text{[redacted]} & \text{[redacted]} & f_{14} \\ f_{21} & \text{[redacted]} & \text{[redacted]} & f_{24} \end{pmatrix}$$

$$\Downarrow$$

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

Determinantal systems

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

$$\Downarrow$$

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

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

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

$$\Big\Downarrow$$

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

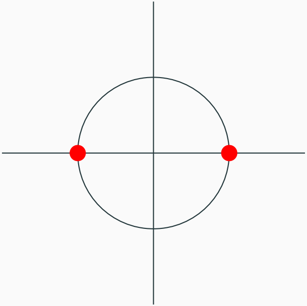
Determinantal systems

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

$$\Downarrow$$

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

Critical points of f ↔ Solutions to maximal minors of $\mathsf{Jac}(f)$



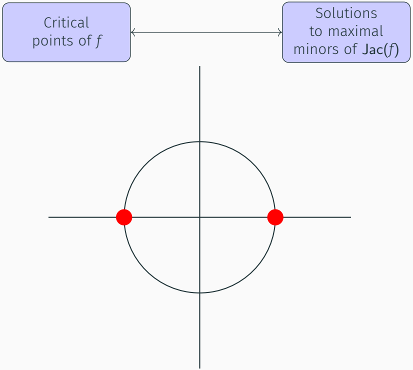
Determinantal systems

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

$$\Downarrow$$

$$\left\{\begin{array}{l} f_{11}f_{22} - f_{12}f_{21} \\ f_{11}f_{23} - f_{13}f_{21} \\ f_{11}f_{24} - f_{14}f_{21} \\ f_{12}f_{23} - f_{13}f_{22} \\ f_{12}f_{24} - f_{14}f_{22} \\ f_{13}f_{24} - f_{14}f_{23} \end{array}\right.$$

Post-quantum crypto (multivariate and code-based cryptography)


Critical points of f ↔ Solutions to maximal minors of $\mathsf{Jac}(f)$

The MinRank Problem

$f_{i,j}$ are **linear forms** in $\Bbbk[x_1, \ldots, x_k]$.

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

Gröbner bases

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

Gröbner bases

$F \subseteq \Bbbk[x_1, \dots, x_k]$ a polynomial system.

Definition (Gröbner bases)

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

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 $g_1, \ldots, g_m$.

Gröbner bases

$F \subseteq \Bbbk[x_1, \ldots, x_k]$ 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

Worst case is doubly exponential in the number of variables. [Mayr, Mayer, 1982]

Gröbner bases

$F \subseteq \Bbbk[x_1, \ldots, x_k]$ 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

Worst case is doubly exponential in the number of variables. [Mayr, Mayer, 1982]

For zero-dimensional systems:

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

Macaulay matrices

Assume F homogeneous.

Macaulay matrices

Assume F homogeneous.

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

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

Macaulay matrices

Assume F homogeneous.

$$\begin{cases} 2x^2 + 11xy - y^2 \\ 4x^2 + xy - 2y^2 \\ -6x^2 - xy + y^2 \end{cases} \xrightarrow{\cdot x} \begin{array}{c} \\ (1, x) \\ \\ \\ \\ \end{array} \begin{array}{cccc} x^3 & x^2y & xy^2 & y^3 \end{array} \hspace{-12em} \begin{array}{c} \\ \left(\begin{array}{cccc} 2 & 11 & -1 & 0 \\ & & & \\ & & & \\ & & & \end{array}\right) \end{array}$$

Macaulay matrices

Assume F homogeneous.

$$\begin{tikzcd}[row sep=tiny]
 & (1,x) \\
\left\{ 2x^2+11xy-y^2 \right. \arrow[ur, bend left, "\cdot x"] \arrow[r, bend left, "\cdot y"] & (1,y) \\
4x^2+xy-2y^2 & \\
-6x^2-xy+y^2 &
\end{tikzcd}$$

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

$$\begin{pmatrix}
2 & 11 & -1 & 0 \\
0 & 2 & 11 & -1 \\
 & & & \\
 & & & \\
 & & &
\end{pmatrix}$$

Macaulay matrices

Assume F homogeneous.

$$\begin{tikzcd}
 & (1,x) \\
2x^2+11xy-y^2 \arrow[ru, bend left, "\cdot x"] \arrow[r, "\cdot y"] & (1,y) \\
4x^2+xy-2y^2 \arrow[ru, "\cdot x"] & (2,x) \\
-6x^2-xy+y^2 &
\end{tikzcd}$$

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

Macaulay matrices

Assume F homogeneous.

$$\begin{tikzcd}
 & (1,x) \\
2x^2+11xy-y^2 \arrow[ur, bend left, "\cdot x"] \arrow[r, bend left, "\cdot y"] & (1,y) \\
4x^2+xy-2y^2 \arrow[r, bend left, "\cdot x"] \arrow[dr, bend right, "\cdot y"'] & (2,x) \\
-6x^2-xy+y^2 & (2,y)
\end{tikzcd}$$

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

Macaulay matrices

Assume F homogeneous.

$$\begin{tikzcd}
 & (1,x) \\
2x^2+11xy-y^2 \arrow[ur, bend left, "\cdot x"] \arrow[r, bend left, "\cdot y"] & (1,y) \\
 & (2,x) \\
4x^2+xy-2y^2 \arrow[ur, bend left, "\cdot x"] \arrow[r, bend right, "\cdot y"] & (2,y) \\
-6x^2-xy+y^2 \arrow[r, bend right, "\cdot x"'] & (3,x)
\end{tikzcd}$$

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

$$\left(\begin{array}{cccc}
2 & 11 & -1 & 0 \\
0 & 2 & 11 & -1 \\
4 & 1 & -2 & 0 \\
0 & 4 & 1 & -2 \\
-6 & -1 & 1 & 0 \\
\end{array}\right)$$

Macaulay matrices

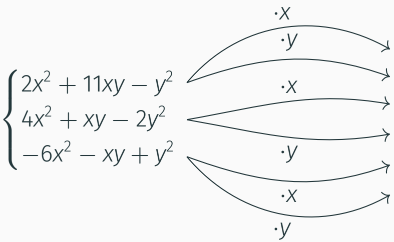
Assume F homogeneous.

$$\begin{tikzcd}
 & (1,x) \\
2x^2+11xy-y^2 \arrow[ur, bend left, "\cdot x"] \arrow[r, "\cdot y"] & (1,y) \\
4x^2+xy-2y^2 \arrow[r, "\cdot x"] \arrow[dr, "\cdot y"'] & (2,x) \\
 & (2,y) \\
-6x^2-xy+y^2 \arrow[r, "\cdot x"'] \arrow[dr, bend right, "\cdot y"'] & (3,x) \\
 & (3,y)
\end{tikzcd}$$

$$\begin{array}{c|cccc}
 & x^3 & x^2y & xy^2 & y^3 \\
\hline
(1,x) & 2 & 11 & -1 & 0 \\
(1,y) & 0 & 2 & 11 & -1 \\
(2,x) & 4 & 1 & -2 & 0 \\
(2,y) & 0 & 4 & 1 & -2 \\
(3,x) & -6 & -1 & 1 & 0 \\
(3,y) & 0 & -6 & -1 & -1
\end{array}$$

Macaulay matrices

Assume F homogeneous.



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

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

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

Macaulay matrices

Assume F homogeneous.

$$\begin{tikzcd}
2x^2+11xy-y^2 \arrow[r, bend left, "\cdot x"] \arrow[dr, bend left, "\cdot y"] & (1,x) \\
 & (1,y) \\
4x^2+xy-2y^2 \arrow[r, bend left, "\cdot x"] \arrow[dr, bend right, "\cdot y"] & (2,x) \\
 & (2,y) \\
-6x^2-xy+y^2 \arrow[r, bend right, "\cdot y"] \arrow[dr, bend right, "\cdot x"'] & (3,x) \\
 & (3,y)
\end{tikzcd}$$

$$\begin{array}{c|cccc}
 & x^3 & x^2y & xy^2 & y^3 \\
\hline
(1,x) & 2 & 11 & -1 & 0 \\
(1,y) & 0 & 2 & 11 & -1 \\
(2,x) & 4 & 1 & -2 & 0 \\
(2,y) & 0 & 4 & 1 & -2 \\
(3,x) & -6 & -1 & 1 & 0 \\
(3,y) & 0 & -6 & -1 & -1
\end{array}$$

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

Theorem (Macaulay bound, [Lazard, 1983])

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

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

Gröbner bases - linear algebra

Gröbner bases - linear algebra

The F_4 algorithm ([Faugère, 1999])

- Perform multiple S-pair reductions at once using fast linear algebra.

Gröbner bases - linear algebra

The F_4 algorithm ([Faugère, 1999])

- Perform multiple S-pair reductions at once using fast linear algebra.
- Make good S-pair choices.

Gröbner bases - linear algebra

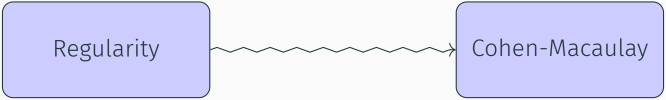
The F_4 algorithm ([Faugère, 1999])

- Perform multiple S-pair reductions at once using fast linear algebra.
- Make good S-pair choices.

Gröbner bases - linear algebra

The F_4 algorithm ([Faugère, 1999])

- Perform multiple S-pair reductions at once using fast linear algebra.
- Make good S-pair choices.



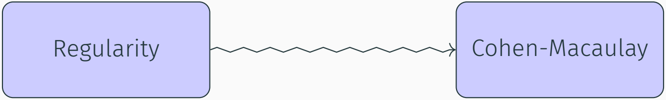
Regularity

Cohen-Macaulay

Gröbner bases - linear algebra

The F_4 algorithm ([Faugère, 1999])

- Perform multiple S-pair reductions at once using fast linear algebra.
- Make good S-pair choices.



Regularity

Cohen-Macaulay

⇝ initial complexity analysis of generalized MinRank:

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

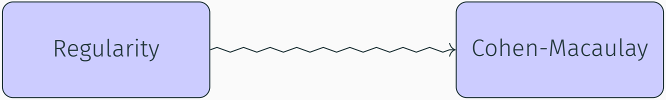
Computing a grevlex Gröbner basis of the $(r+1)$-minors of an $n \times m$ matrix of generic polynomials of degree D in k variables has arithmetic complexity

$$O\left(\binom{n}{r+1}\binom{m}{r+1}\binom{Dr(m-r)+(D-1)k+1+k}{k}^{\omega}\right).$$

Gröbner bases - linear algebra

The F_4 algorithm ([Faugère, 1999])

- Perform multiple S-pair reductions at once using fast linear algebra.
- Make good S-pair choices.



$\rightsquigarrow$ initial complexity analysis of generalized MinRank:

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

Computing a grevlex Gröbner basis of the $(r+1)$-minors of an $n \times m$ matrix of generic polynomials of degree D in k variables has arithmetic complexity

$$O\left(\binom{n}{r+1}\binom{m}{r+1}\binom{Dr(m-r)+(D-1)k+1+k}{k}^{\omega}\right).$$

Matrices computed by F_4 are generically rank-deficient

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.

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

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

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

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

$$\mathcal{M}_4$$

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

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

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

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

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

$$\mathcal{M}_4$$

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

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.

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

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

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

Lazard: $\mathcal{M}_4$ is 18×15.

$$\mathcal{M}_4$$

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

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

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

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

$(f_1, \ldots, f_m)$ regular sequence

$$\mathcal{M}_4$$

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

The F_5 algorithm ([Faugère, 2002])

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

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

$(f_1, \ldots, f_m)$ regular sequence

$$\Downarrow$$

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

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

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

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

$(f_1, \ldots, f_m)$ regular sequence

$$\Downarrow$$

$\Big\{$ **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.

F₅: $\mathcal{M}_4$ 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.

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

$(f_1, \ldots, f_m)$ regular sequence

$$\Downarrow$$

$$\left\{\begin{array}{l}\textbf{No} \text{ reductions to zero.}\\ \text{Precise complexity analysis}^{1}\end{array}\right.$$

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

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

Lazard: $\mathcal{M}_4$ is 18×15.

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

$\mathcal{M}_4$

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

[1] [Bardet, Faugère, Salvy, 2015]

The F_5 algorithm ([Faugère, 2002])

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

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

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

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

$(f_1, \ldots, f_m)$ regular sequence

$\Downarrow$

zero.

y analysis [1]

Determinantal systems are not regular sequences!

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

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

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

Lazard: $\mathcal{M}_4$ is 18×15.

F_5: $\mathcal{M}_4$ is 15×15 and full rank!

[1] [Bardet, Faugère, Salvy, 2015]

The F_5 algorithm ([Faugère, 2002])

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

$(f_1, \ldots, f_m)$ regular sequence

$$\Downarrow$$

$\{$ zero.

y analysis [1]

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

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

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

Determinantal systems are not regular sequences!

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

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

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

How do we remove reductions to zero?

Lazard: $\mathcal{M}_4$ is 18 × 15.

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

[1] [Bardet, Faugère, Salvy, 2015]

Contributions

Contributions

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

M is an $n \times n$ matrix of generic linear forms over $\mathbb{k}[x_1, \dots, x_k]$, $r \leq n-1$. 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 $r+2$

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

Contributions

M is an $n \times n$ matrix of generic linear forms over $\Bbbk[x_1, \ldots, x_k]$, $r \le n-1$. 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

M is an $n \times n$ matrix of generic linear forms over $\mathbb{k}[x_1, \dots, x_k]$, $r \leq n-1$. 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.

Contributions

M is an $n \times n$ matrix of generic linear forms over $\Bbbk[x_1, \ldots, x_k]$, $r \leq n-1$. 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, 2023])

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

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

Syzygies

Definition (Syzygy)

A sequence $(a_1, \ldots, a_m) \in \Bbbk[x_1, \ldots, x_k]^m$ such that

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

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

Syzygies

Definition (Syzygy)

A sequence $(a_1, \dots, a_m) \in \Bbbk[x_1, \dots, x_k]^m$ such that

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

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

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

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

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

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

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

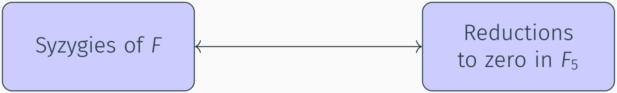
is called a **syzygy** of $f_1, \ldots, f_m$.

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 of F

Reductions to zero in F_5

Syzygies

Definition (Syzygy)

A sequence $(a_1, \dots, a_m) \in \mathbb{k}[x_1, \dots, x_k]^m$ such that

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

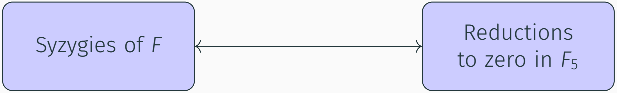
is called a **syzygy** of $f_1, \dots, f_m$.

Example (Koszul syzygies)

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

$$\Downarrow$$

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



Syzygies of F

Reductions to zero in F_5

Theorem ([Hilbert, 1890])

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

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

The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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

The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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

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

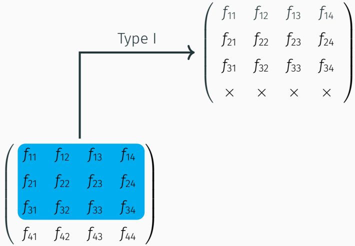
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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



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

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

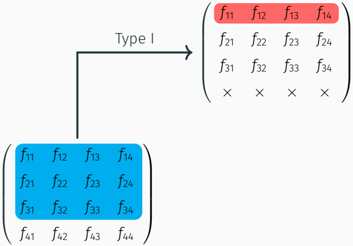
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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



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

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

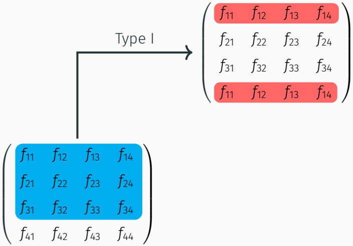
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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



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

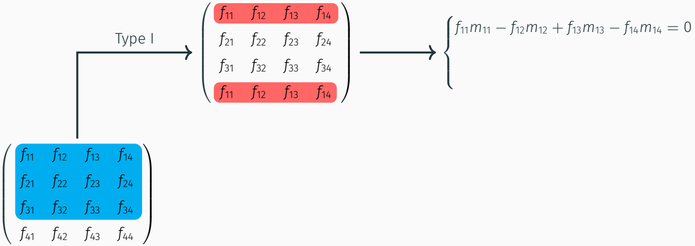
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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



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

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

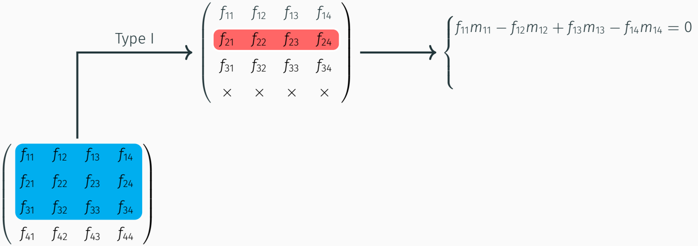
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

m_{ij} = determinant of submatrix of M obtained 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

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

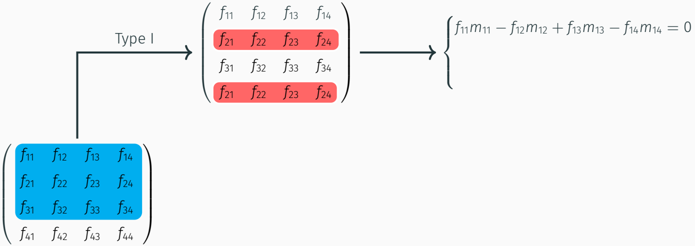
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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



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

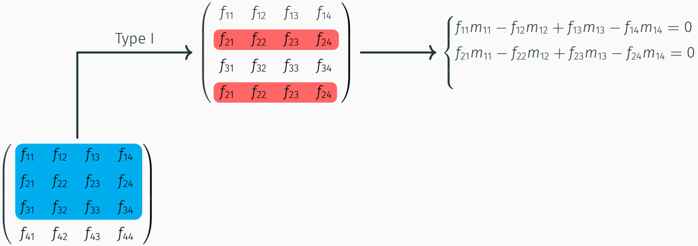
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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



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

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

$$\begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ \end{cases}$$

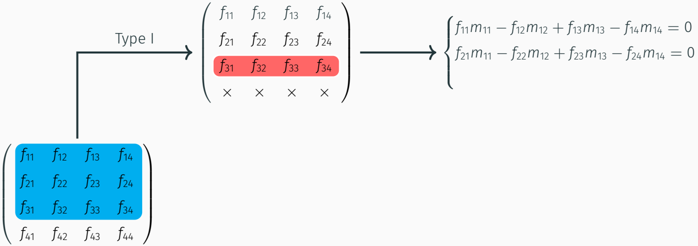
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

m_{ij} = determinant of submatrix of M obtained 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

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

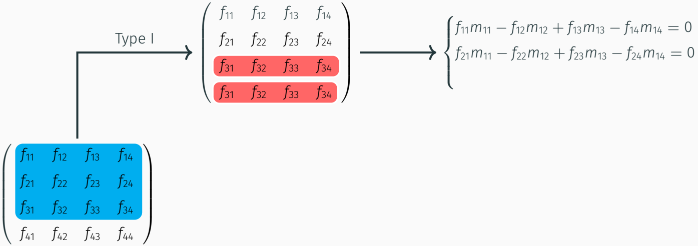
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

m_{ij} = determinant of submatrix of M obtained 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

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

$$\begin{cases} f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14} = 0 \\ f_{21}m_{11} - f_{22}m_{12} + f_{23}m_{13} - f_{24}m_{14} = 0 \\ \end{cases}$$

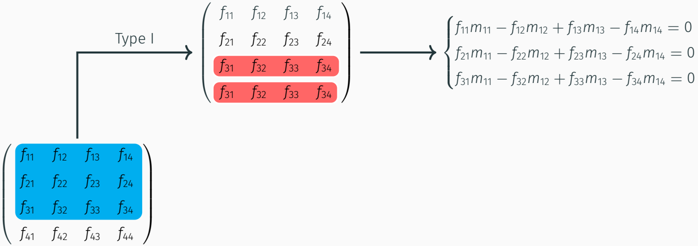
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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



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

The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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

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

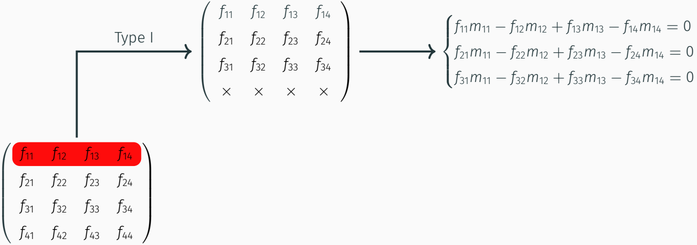
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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



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

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

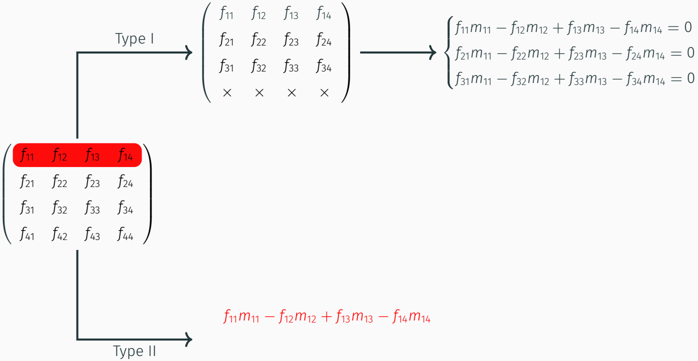
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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



Type I

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

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

Type II

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

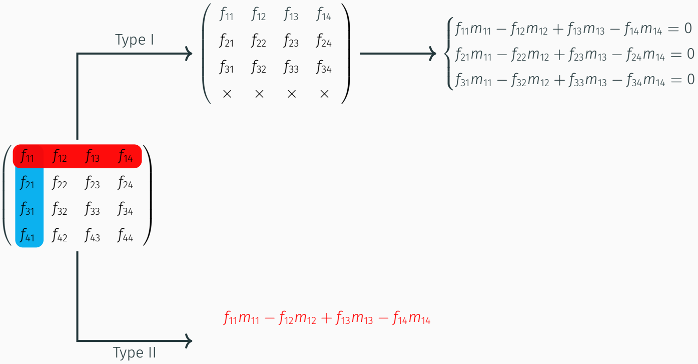
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

m_{ij} = determinant of submatrix of M obtained 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

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

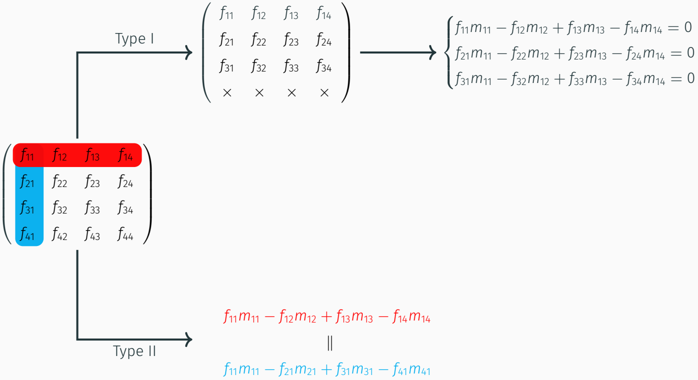
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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



Type I

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

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

Type II

$$f_{11}m_{11} - f_{12}m_{12} + f_{13}m_{13} - f_{14}m_{14}$$
$$\|$$
$$f_{11}m_{11} - f_{21}m_{21} + f_{31}m_{31} - f_{41}m_{41}$$

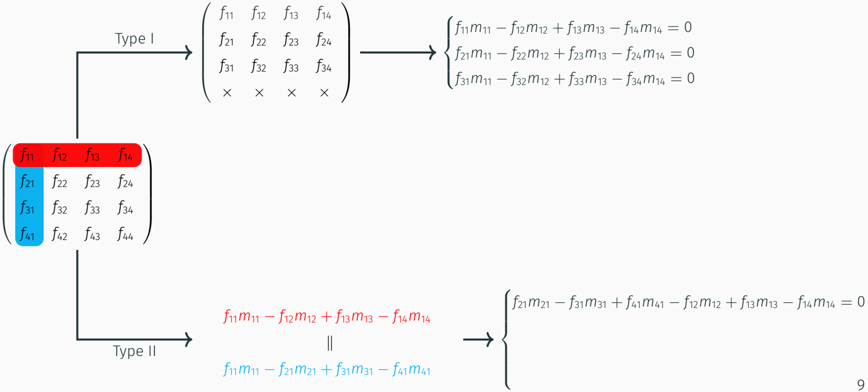
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

m_{ij} = determinant of submatrix of M obtained 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

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

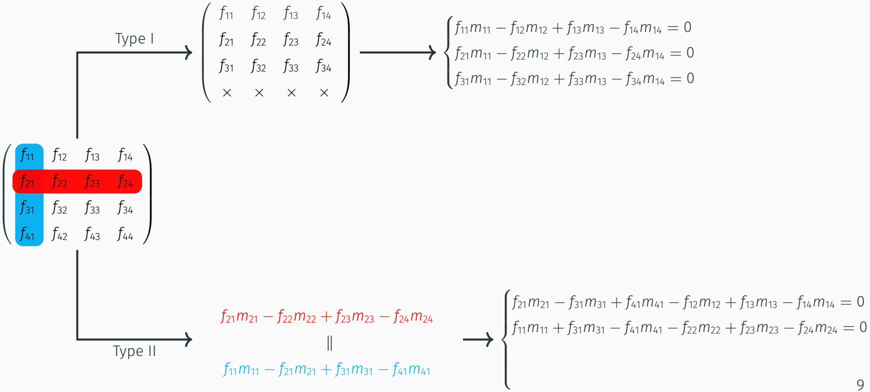
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

m_{ij} = determinant of submatrix of M obtained 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

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

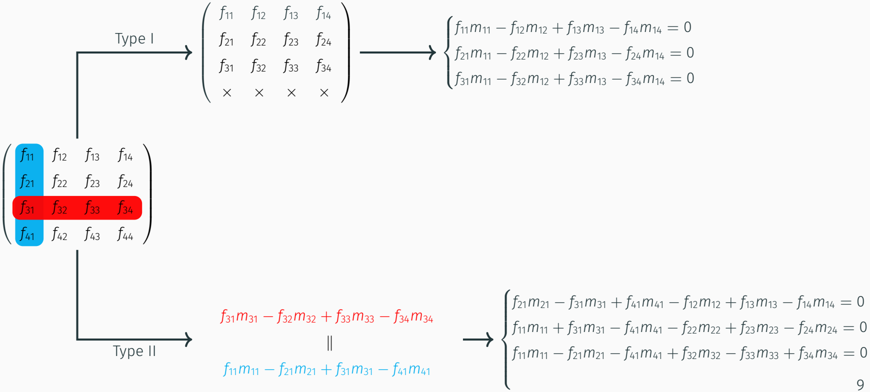
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

m_{ij} = determinant of submatrix of M obtained 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

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

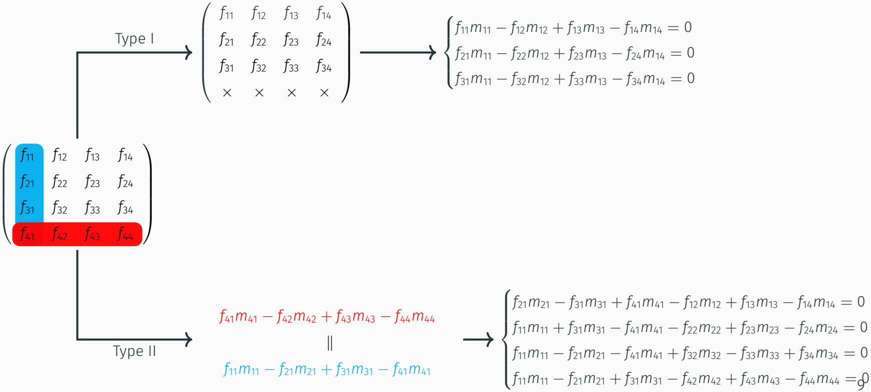
The Gulliksen-Negård complex

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

m_{ij} = determinant of submatrix of M obtained 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

Theorem ([Gulliksen, Negård, 1972])

$r = n - 2$, entries of M sufficiently generic $\rightsquigarrow$ free resolution:

$$0 \to \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \langle F_r(M) \rangle \to 0$$

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

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

Theorem ([Kurano, 1989])

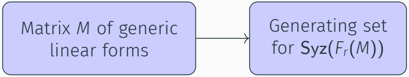
The syzygies between the $(r+1)$-minors of M are generated by the syzygies between the $(r+1)$ minors of the $(r+2) \times (r+2)$ submatrices of M.

New F_5 algorithms - the general case

New F_5 algorithms - the general case

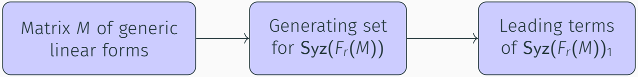
Matrix M of generic linear forms

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

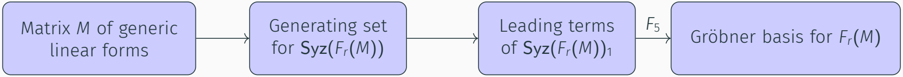


Matrix M of generic linear forms

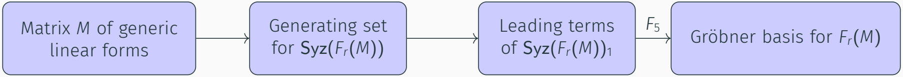
Generating set for $\mathrm{Syz}(F_r(M))$

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 $\mathrm{Syz}(F_r(M))$

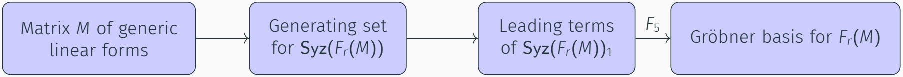
Leading terms of $\mathrm{Syz}(F_r(M))_1$

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

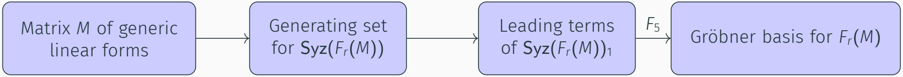
Gröbner basis for $F_r(M)$

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

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])

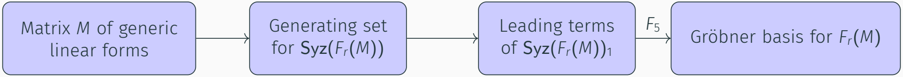
$F_r(M)$ has a free resolution of length $(n-r)^2$.

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

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 $(n-r)^2$.

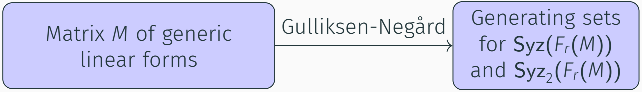
$$\mathrm{Syz}_k(F_r(M)) \neq 0 \text{ for } 1 < k < (n-r)^2. \quad \Longrightarrow \quad \text{Cannot efficiently compute a Gröbner basis for } \mathrm{Syz}(F_r(M))$$

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 $r = n - 2$

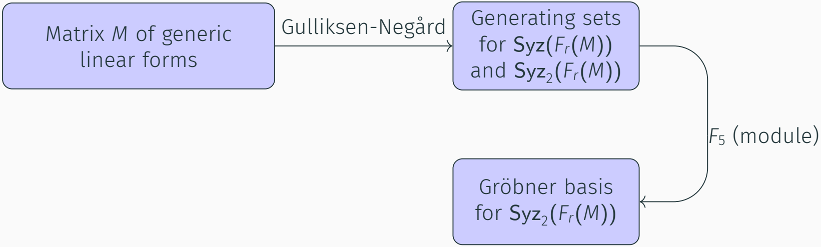


Matrix M of generic linear forms

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

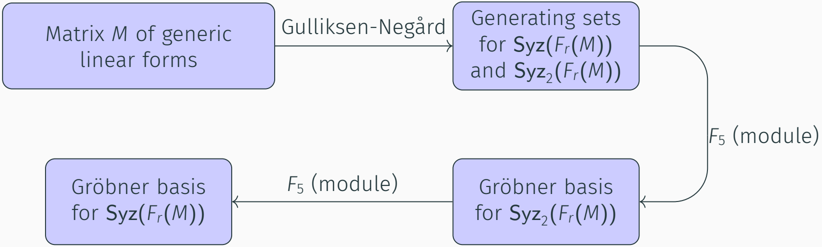
Gulliksen-Negård

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

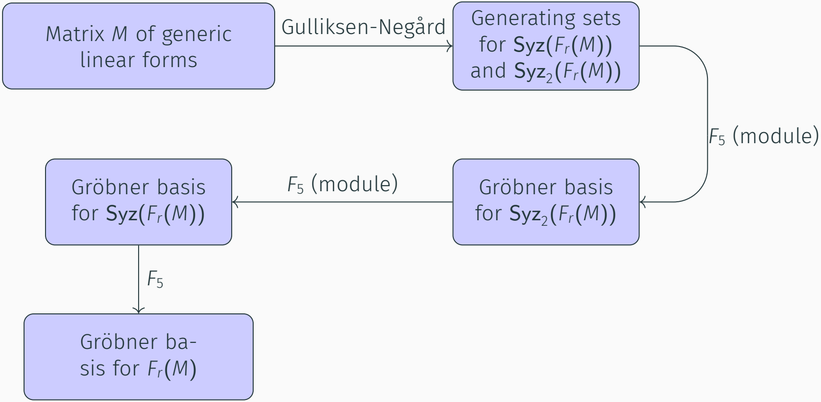
F_5 (module)

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

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 $\mathrm{Syz}_2(F_r(M))$

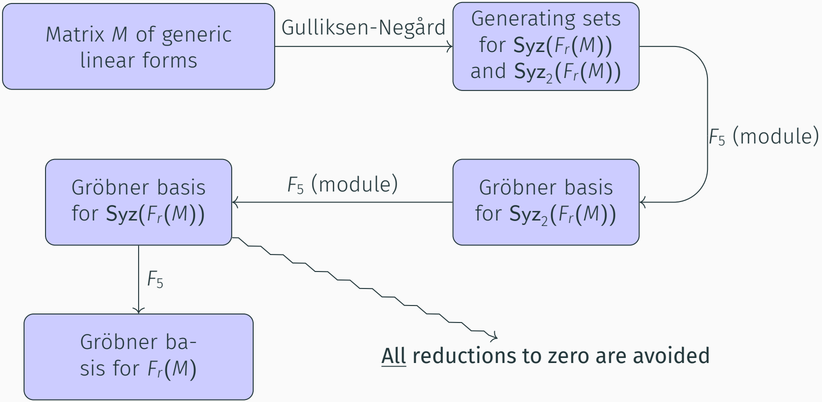
F_5 (module)

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 $F_r(M)$

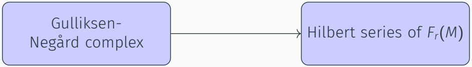
All reductions to zero are avoided

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

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

Gulliksen-Negård complex

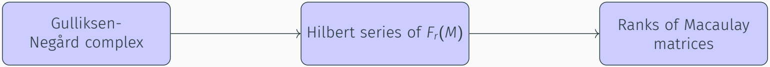
A complexity analysis in the case $r = n - 2$



Gulliksen-Negård complex

Hilbert series of $F_r(M)$

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

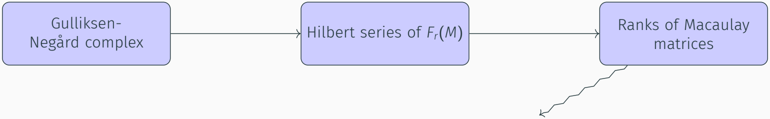


Gulliksen-Negård complex

Hilbert series of $F_r(M)$

Ranks of Macaulay matrices

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

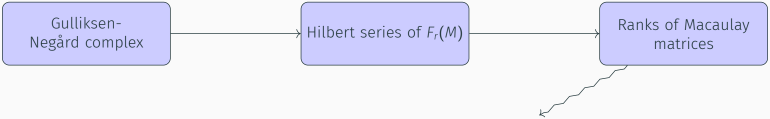


Theorem ([G., Neiger, Safey, 2023])

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

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

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

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

Asymptotically:

[Faugère, Safey, Spaenlehauer, 2013]

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

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

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

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

Conclusion and perspectives

Conclusion and perspectives

Summary

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

Conclusion and perspectives

Summary

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

Conclusion 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.

Conclusion 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.
  - Explicit Hilbert series leading to new complexity bound.

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

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

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

Future works

- Second syzygies in the general case.

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

Future works

- Second syzygies in the general case.[a]

[a] [Ma, 1994]

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

Future works

- Second syzygies in the general case.[a]
- Other free resolutions of determinantal ideals.

[a] [Ma, 1994]

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

Future works

- Second syzygies in the general case.[a]
- Other free resolutions of determinantal ideals.[b]

[a] [Ma, 1994]

[b] [Lascoux, 1978], [Eagon, Northcott, 1962],...

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

Future works

- Second syzygies in the general case.[a]
- Other free resolutions of determinantal ideals.[b]
- Sharper complexity analyses of new algorithms and implications for cryptography schemes.

[a] [Ma, 1994]

[b] [Lascoux, 1978], [Eagon, Northcott, 1962],...

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

Future works

- Second syzygies in the general case.[a]
- Other free resolutions of determinantal ideals.[b]
- Sharper complexity analyses of new algorithms and implications for cryptography schemes.
- Efficient implementations of new algorithms.

[a] [Ma, 1994]

[b] [Lascoux, 1978], [Eagon, Northcott, 1962],...

Thanks. Questions?