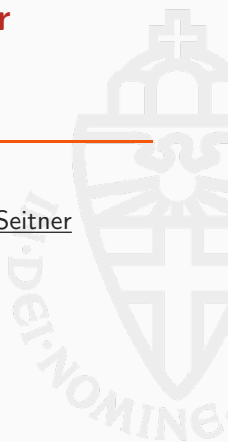


Smoothing the degree of regularity for polynomial systems

Samuel Jaques, Lars Ran, Simona Samardjiska and Melvin Seitner

August 11, 2026, Ohrid

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen



Macaulay Matrix

MQ problem:

$$\begin{aligned} f_1 &= X^2 + 3Y^2 + X + 2Y + 2 \\ f_2 &= 2X^2 + XY + 4X + 3Y + 1 \\ f_3 &= 3X^2 + 2XY + 4Y^2 + X + 1 \end{aligned}$$

Macaulay Matrix of degree d of $\mathcal{F} = (f_1, \dots, f_m)$

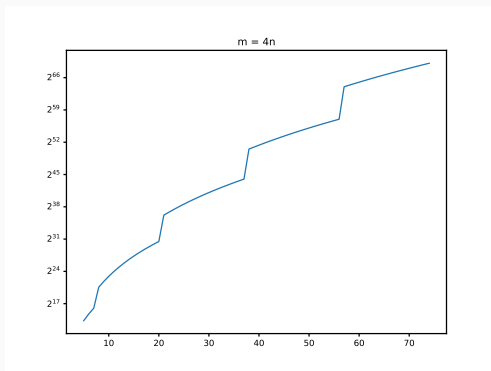
- Columns indexed by $\mu \in \mathcal{M}_d := \{\text{monomials of degree } \leq d\}$
- Rows indexed by (μ, f_i) , where $\mu \in \mathcal{M}_{d-2}$ and $f_i \in \mathcal{F}$, containing the coefficients of μf_i .

$$\text{Mac}^3(\mathcal{F}) = \begin{array}{c} \begin{matrix} Xf_1 \\ Xf_2 \\ Xf_3 \\ Yf_1 \\ Yf_2 \\ Yf_3 \\ f_1 \\ f_2 \\ f_3 \end{matrix} \begin{bmatrix} X^3 & X^2Y & XY^2 & Y^3 & Y^2 & XY & X^2 & Y & X & 1 \\ 1 & 0 & 3 & 0 & 1 & 2 & 0 & 2 & 0 & 0 \\ 2 & 1 & 0 & 0 & 4 & 3 & 0 & 1 & 0 & 0 \\ 3 & 2 & 4 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 & 1 & 2 & 0 & 2 & 0 \\ 0 & 2 & 1 & 0 & 0 & 4 & 3 & 0 & 1 & 0 \\ 0 & 3 & 2 & 4 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 4 & 3 & 1 \\ 0 & 0 & 0 & 0 & 3 & 2 & 4 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

Complexity Growth

Degree of regularity: Smallest d where we expect $\text{Mac}^d(\mathcal{F})$ to have a unique solution.

Width of Macaulay matrix: $|\mathcal{M}_d| = O(n^d)$



Our goal: make this smoother!

An intermediate step (example)

Another example: $n = 2$, $m = 4$

functions	monomials
$f_1 = X^2 + 3Y^2 + X + 2Y + 2$	
$f_2 = 2X^2 + XY + 4X + 3Y + 1$	$X, Y,$
$f_3 = 3X^2 + 2XY + 4Y^2 + X + 1$	X^2, XY, Y^2
$f_4 = 2X^2 + 2XY + 4Y^2 + 4Y$	
$Yf_1 = X^2Y + 3Y^3 + XY + 2Y^2 + 2Y$	
$Yf_2 = 2X^2Y + XY^2 + 4XY + 3Y^2 + Y$	
$Yf_3 = 3X^2Y + 2XY^2 + 4Y^3 + XY + Y$	
$Yf_4 = 2X^2Y + 2XY^2 + 4Y^3 + 4Y^2$	$X^3, X^2Y,$
$Xf_1 = X^3 + 3XY^2 + X^2 + 2XY + 2X$	XY^2, Y^3
$Xf_2 = 2X^3 + X^2Y + 4X^2 + 3XY + X$	
$Xf_3 = 3X^3 + 2X^2Y + 4XY^2 + X^2 + X$	
$Xf_4 = 2X^3 + 2X^2Y + 4XY^2 + 4XY$	

An intermediate step (example)

Another example: $n = 2$, $m = 4$

functions	monomials
$f_1 = X^2 + 3Y^2 + X + 2Y + 2$	
$f_2 = 2X^2 + XY + 4X + 3Y + 1$	$X, Y,$
$f_3 = 3X^2 + 2XY + 4Y^2 + X + 1$	X^2, XY, Y^2
$f_4 = 2X^2 + 2XY + 4Y^2 + 4Y$	
$Yf_1 = X^2Y + 3Y^3 + XY + 2Y^2 + 2Y$	
$Yf_2 = 2X^2Y + XY^2 + 4XY + 3Y^2 + Y$	$X^2Y,$
$Yf_3 = 3X^2Y + 2XY^2 + 4Y^3 + XY + Y$	XY^2, Y^3
$Yf_4 = 2X^2Y + 2XY^2 + 4Y^3 + 4Y^2$	
$Xf_1 = X^3 + 3XY^2 + X^2 + 2XY + 2X$	
$Xf_2 = 2X^3 + X^2Y + 4X^2 + 3XY + X$	
$Xf_3 = 3X^3 + 2X^2Y + 4XY^2 + X^2 + X$	
$Xf_4 = 2X^3 + 2X^2Y + 4XY^2 + 4XY$	

$$\text{Mac}^d = \left[\begin{array}{c|c|c} * & * & * \\ \hline 0 & * & * \\ \hline 0 & 0 & \text{Mac}^{d-1} \end{array} \right]$$

Core idea: Use submatrices of Mac^d involving fewer variables.

Narrowing down the submatrices

Which rows of $\text{Mac}^d(\mathcal{F})$? We want:

- Few supporting columns,
- Relatively many rows (as proxy for rank)

Let $\mu \in \mathcal{M}_{d-2}$.

$\forall i$, the expected support of $\mu \cdot f_i$ is $\mu \cdot \mathcal{M}_2$,

so the expected support of all of $\mu \cdot \mathcal{F}$ is also $\mu \cdot \mathcal{M}_2$.

We'll take a set of rows $\mathcal{S} \cdot \mathcal{F}$ for some $\mathcal{S} \subseteq \mathcal{M}_{d-2}$. The support is

$$\partial^2 \mathcal{S} := \mathcal{S} \cdot \mathcal{M}_2$$

We want $\mathcal{S} \subseteq \mathcal{M}_{d-2}$ to satisfy:

$$|\partial^2 \mathcal{S}| = \min_{|\mathcal{T}|=|\mathcal{S}|} |\partial^2 \mathcal{T}|$$

The `grevlex` ordering of the monomials $\mathcal{M}$:

- Sort monomials based on degree first
- Write monomials as sorted lists of variables, e.g.

$$ZX^2 \rightarrow (X, X, Z)$$

then sort lexicographically, i.e. alphabetically

We want a set $\mathcal{S} \subseteq \mathcal{M}$ that satisfies

$$|\partial^2 \mathcal{S}| = \min_{|T|=|\mathcal{S}|} |\partial^2 T|$$

Clements-Lindström, 1969: This property is satisfied by initial segments of the `grevlex` monomial ordering.

$$\mathcal{S} = \{\text{monomial } \mu \mid \mu \leq \max(\mathcal{S})\}$$

Example
in $X < Y < Z$

1	XXX
X	XXY
Y	XXZ
Z	XYY
XX	XYZ
XY	XZZ
XZ	YYY
YY	YYZ
YZ	YZZ
ZZ	ZZZ

Macaulay Matrix of grevlex-initial segment $\mathcal{S} \subseteq \mathcal{M}$

- Columns indexed $\mu \in \partial^2 \mathcal{S}$
- Rows indexed by (μ, f_i) for $\mu \in \mathcal{S}$, with the coefficients of μf_i .

$$\text{Mac}^d = \left[\begin{array}{c|c} * & * \\ \hline 0 & \text{Mac}^{\mathcal{S}} \end{array} \right] = \left[\begin{array}{c|c|c} * & * & * \\ \hline 0 & * & * \\ \hline 0 & 0 & \text{Mac}^{d-1} \end{array} \right]$$

if $\mathcal{M}_{d-3} \subseteq \mathcal{S} \subseteq \mathcal{M}_{d-2}$

Note that

- $\mathcal{M}_{d-2}$ is an initial segment of $\mathcal{M}$, with
- $\partial^2 \mathcal{M}_{d-2} = \mathcal{M}_d$
- $\text{Mac}^{\mathcal{M}_{d-2}}(\mathcal{F}) = \text{Mac}^d(\mathcal{F})$

Trivial Syzygies

Trivial syzygies: Let $f, g \in \mathcal{F}$ with $f = \sum_{\mu \in \mathcal{M}_2} \alpha_\mu \mu$ and $g = \sum_{\mu \in \mathcal{M}_2} \beta_\mu \mu$ and let $\nu \in \mathcal{M}_{d-4}$

$$\begin{aligned}\nu fg &= \nu gf \\ \sum_{\mu \in \mathcal{M}_2} \alpha_\mu \cdot \nu \mu g &= \sum_{\mu \in \mathcal{M}_2} \beta_\mu \cdot \nu \mu f \\ \sum_{\mu \in \mathcal{M}_2} \alpha_\mu \cdot \text{row}(\nu \mu, g) &= \sum_{\mu \in \mathcal{M}_2} \beta_\mu \cdot \text{row}(\nu \mu, f) = \text{coeffs}(\nu fg)\end{aligned}$$

The **Relation Matrix** $\text{Rel}^d(\mathcal{F})$ is defined as:

- Columns indexed by (μ, f_i) , where $\mu \in \mathcal{M}_{d-2}$ and $f_i \in \mathcal{F}$
- Rows indexed by $(\nu, \{f_i, f_j\})$ with $\nu \in \mathcal{M}_{d-4}$ and $f_i \neq f_j \in \mathcal{F}$.

So that $\text{Rel}^d(\mathcal{F}) \cdot \text{Mac}^d(\mathcal{F}) = 0$.

Higher order syzygies: $\text{Rel}^d(\mathcal{F})$ itself has trivial syzygies $\text{Rel}_2^d(\mathcal{F})$, which then has trivial syzygies $\text{Rel}_3^d(\mathcal{F})$, etc.

$$\text{nul}(\text{Mac}^d(\mathcal{F})) = \sum_{c>1} (-1)^c \binom{m}{c} |\mathcal{M}_{d-2c}|$$

Semi-regularity: Up to the degree of regularity, all syzygies of Mac^d are trivial, i.e. linear combinations of the $(fg = gf)$ -syzygies

$$\text{Mac}^d = \left[\begin{array}{c|c} * & * \\ \hline 0 & \text{Mac}^S \end{array} \right]$$

$$\{\text{syzygies of } \text{Mac}^S(\mathcal{F})\} = \left\{ \begin{array}{l} \text{Syzygies on the} \\ \text{rows of } \text{Mac}^d(\mathcal{F}) \\ \text{indexed by } \mathcal{S} \times \mathcal{F} \end{array} \right\}$$

$$\left\{ \begin{array}{l} \text{Trivial syzygies} \\ \text{of } \text{Mac}^S(\mathcal{F}) \end{array} \right\} := \left\{ \begin{array}{l} \text{Syzygies} \\ \text{of } \text{Mac}^S(\mathcal{F}) \end{array} \right\} \cap \left\{ \begin{array}{l} \text{Trivial syzygies} \\ \text{of } \text{Mac}^d(\mathcal{F}) \end{array} \right\}$$

Monomial semi-regularity: Up to the first $\mathcal{S}$ where $\text{null}(\text{Mac}^S) = 0$, all syzygies of Mac^S are trivial syzygies of Mac^d .

Partitioning the relation Matrix

Write $\max(\mathcal{S}) = X_{a_{d-2}} \cdots X_{a_1}$, where $a_{d-2} > \cdots > a_1$.

Let $\mathcal{F}_i$ be the system $\mathcal{F}(X_1, X_2, \dots, X_{a_i-1}, 0, \dots, 0)$ in $a_i - 1$ variables.

The standard relation matrix can be partitioned as follows:

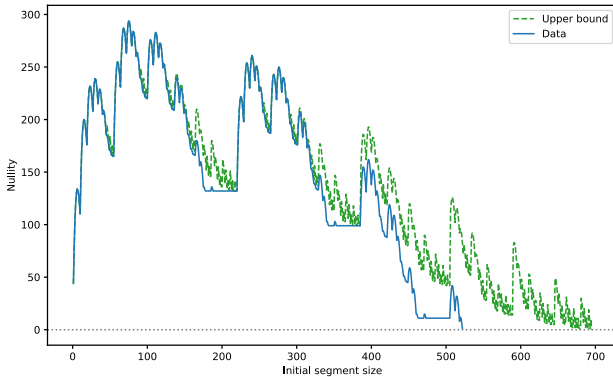
$$\text{Rel}^d(\mathcal{F}) = \left[\begin{array}{c|c|c|c|c} \text{Rel}^d(\mathcal{F}_{d-2}) & * & * & * & * \\ \hline 0 & \text{Rel}^{d-1}(\mathcal{F}_{d-3}) & * & * & * \\ \hline 0 & 0 & \ddots & * & * \\ \hline 0 & 0 & 0 & \text{Rel}^3(\mathcal{F}_1) & * \\ \hline 0 & 0 & 0 & 0 & * \end{array} \right]$$

$\underbrace{\hspace{10em}}_{\mathcal{S} \times \mathcal{F}}$

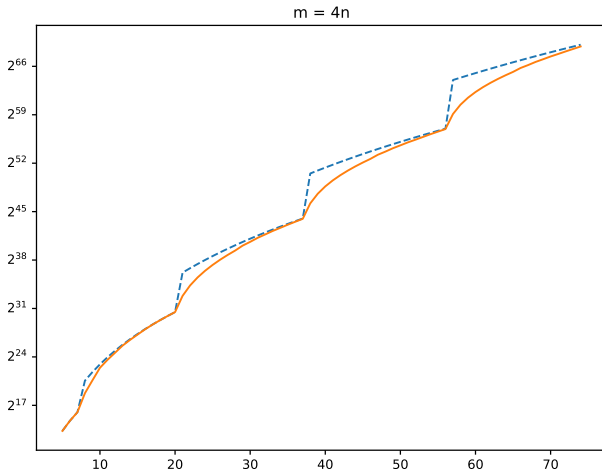
So the dimension of the trivial syzygies on $\text{Mac}^{\mathcal{S}}$ is at most

$$\text{rank Rel}^d(\mathcal{F}) - \sum_{i=0}^{d-2} \text{rank Rel}^{i+2}(\mathcal{F}_i)$$

Nullity Predictions



Complexity Comparison



Thank you for listening!

