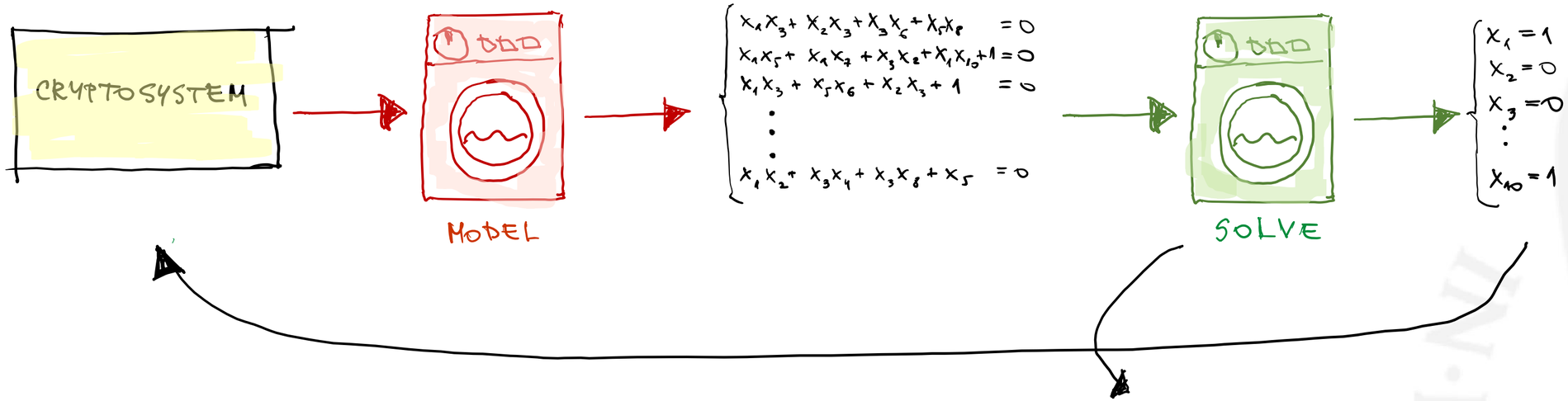
iCIS | Digital Security
Radboud University

Smoothing the degree of regularity for polynomial systems

(joint work with Samuel Jaques, Lars Ran, Melvin Seitner)

Simona Samardjiska
Department of Digital Security – Radboud University
simona.samardjiska@ru.nl

Algebraic models



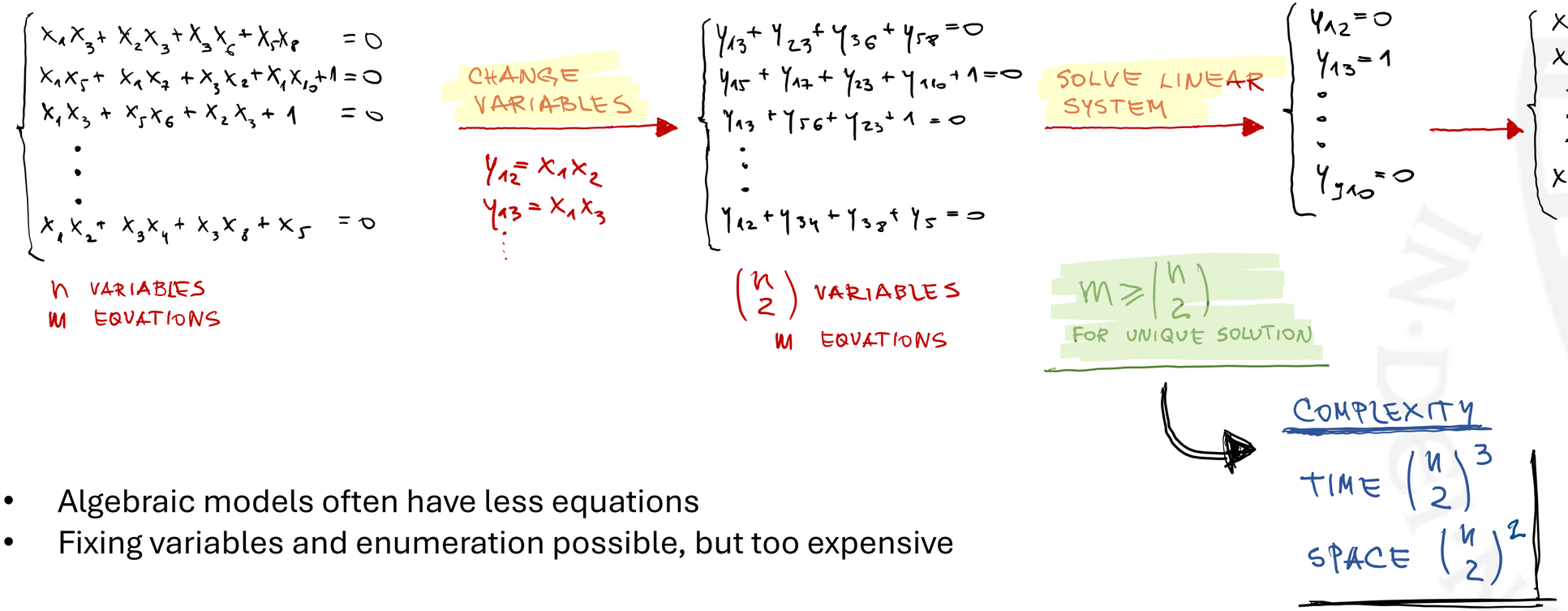
- Message recovery attack
- Signature forgery
- Key-recovery attack

Non-trivial methods for

- Solving
- Complexity estimates

Solving algebraic systems

Simplest method - linearization



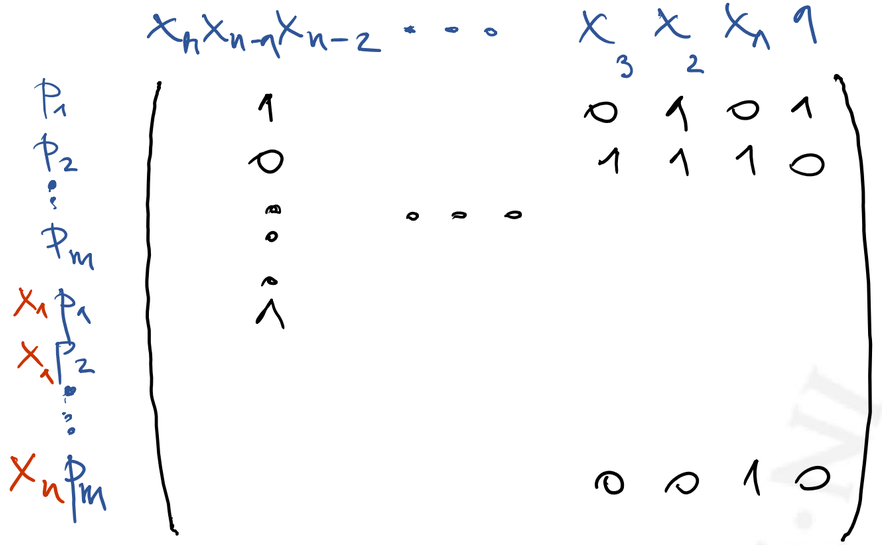
- Algebraic models often have less equations
- Fixing variables and enumeration possible, but too expensive

Solving algebraic systems

General principle F4, XL, Joux-Vitse

$$\begin{cases} p_1(x_1, \ldots, x_n) = 0 \\ p_2(x_1, \ldots, x_n) = 0 \\ \quad \ldots \\ p_m(x_1, \ldots, x_n) = 0 \end{cases}$$

Form Macaulay matrix of degree d



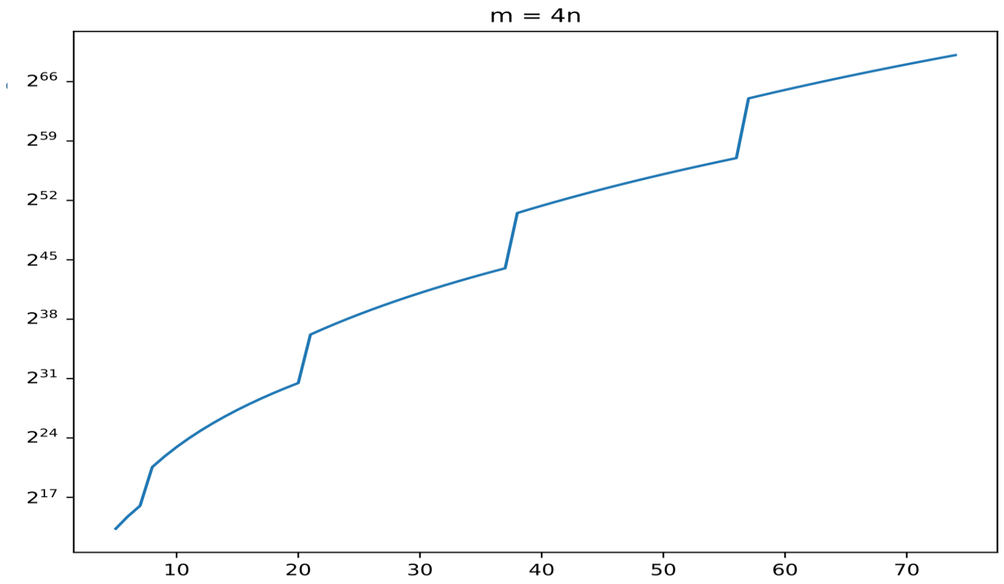
- Gauss reduce if enough independent rows, otherwise **repeat** for d+1

COMPLEXITY $\binom{n}{D}^3$

For some minimum D - ***degree of regularity***

Pitfall of XL algorithm

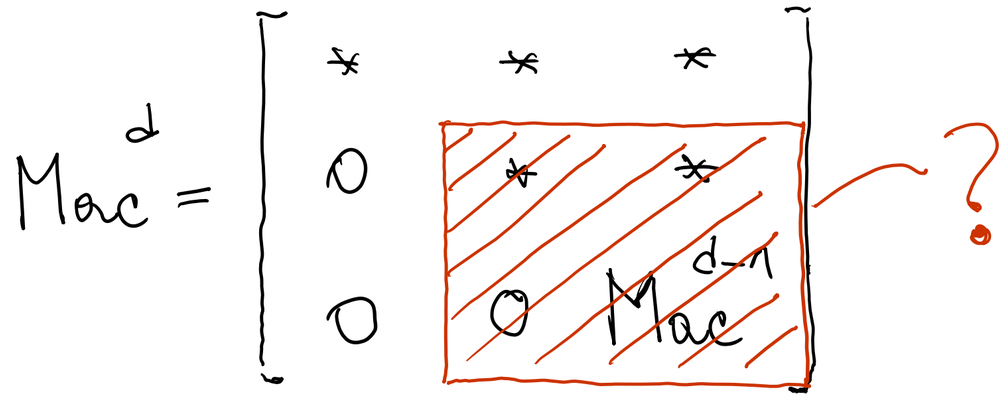
- Complexity directly depends on size of Macaulay matrix
- Going from *d* to *d+1* increases sharply the complexity
- Often there is **unnecessary overhead**



- **Can we remove this overhead in a provable manner**?

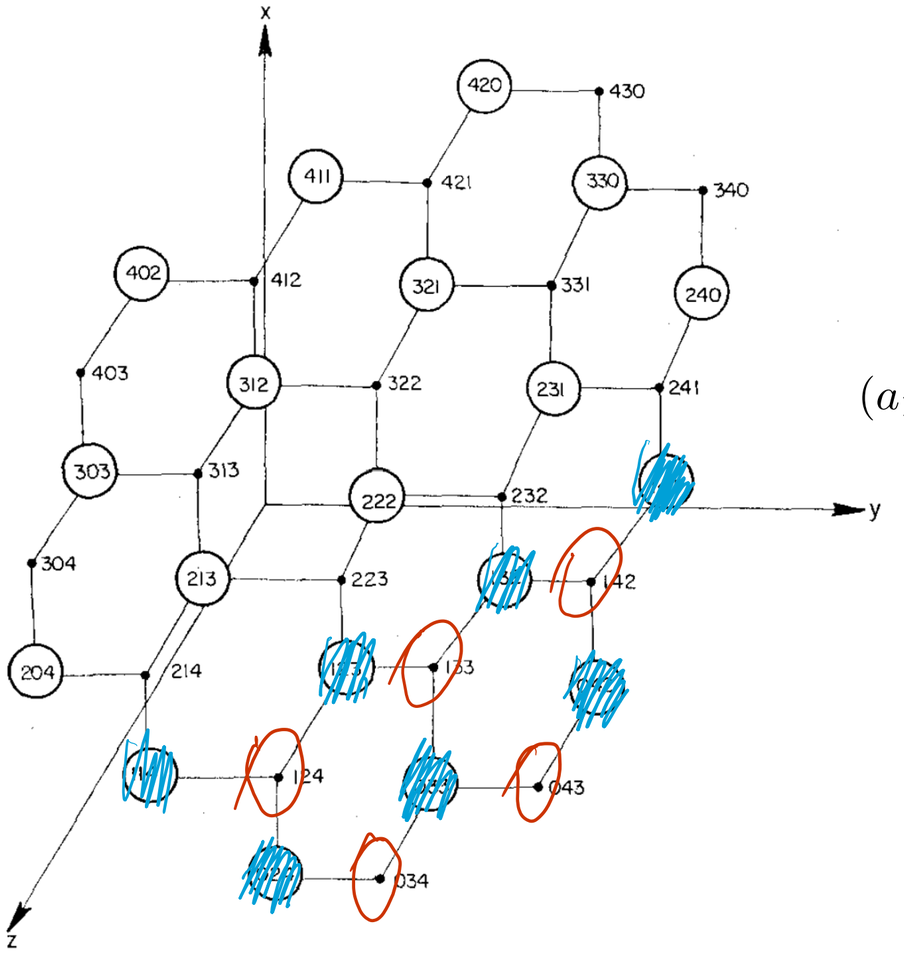
A natural solution

- Consider only a submatrix of Macaulay matrix (up to some row and column reordering)



- How to find the best (or close to best) choice of a submatrix?
  - We want the optimal, **minimal possible**

A prelude:
An old combinatorics result (Clements-Lindström ‘69, Kruskal-Katona‘66)



Which ***m* buttons (dots)** should we press **to minimize** the number of **lights (circles)** that turn on?

- a button turns all lights according to

$$(a_1, \ldots, a_n) \mapsto \{(a_1 - 1, \ldots, a_n), (a_1, a_2 - 1, \ldots, a_n), \ldots, (a_1, \ldots, a_n - 1)\}$$

Solution: The first ***m*** buttons in lexicographical order

This result nicely applies to our situation ☺

iCIS | Digital Security
Radboud University

Grevlex ordering, supports and shadows

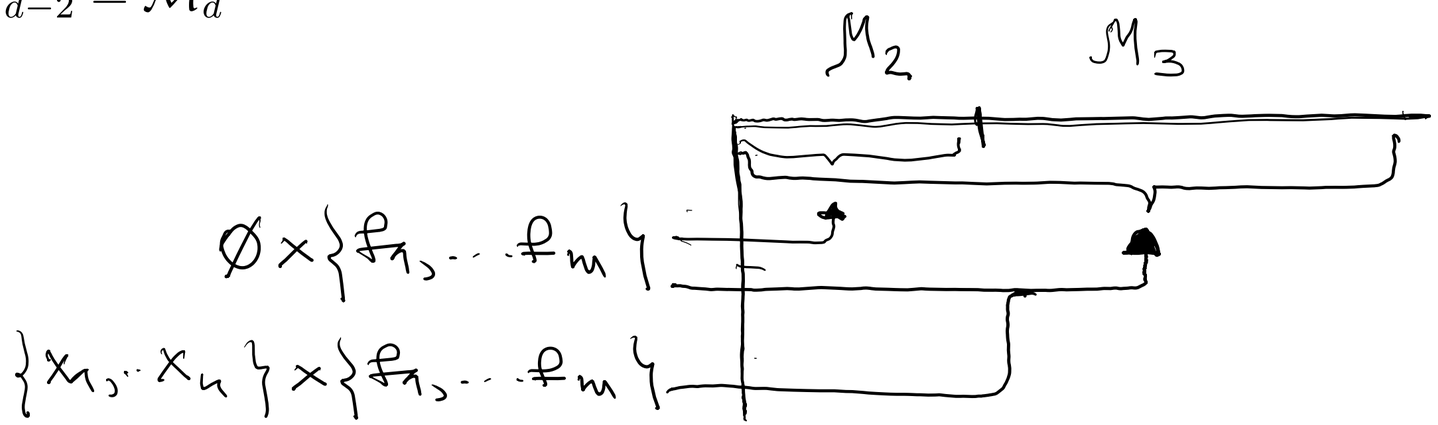
- **Grevlex** monomial ordering

$$X_1^3 > X_2X_1^2 > X_2^2X_1 > X_2^3 > X_3X_1^2 > X_3X_2X_1 > X_3X_2^2 > \cdots X_n^3 > \\ > X_1^2 > X_2X_1 > X_2^2 > X_3X_1 > X_3X_2 > \cdots > X_1 > X_2 > \cdots X_n > 1$$

- **Support** of a row in Macaulay matrix Mac^d – all columns containing nonzero coefficients
- **Shadow** of $S \in \mathcal{M}_{d-2}$, for $S \times \{f_1, \ldots, f_m\}$ - index set of rows

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

- Note $\partial^2 \mathcal{M}_{d-2} = \mathcal{M}_d$



Initial segments and Clements-Lindström for Macaulay matrices

- **Initial segment** $\mathcal{S}_{\leq \mu} = \{\nu \in \mathcal{M} \text{ where } \nu \leq \mu\}.$
  - for monomial $X_3X_1^2$

$$X_3X_1^2 > X_3X_2X_2 > X_3X_2^2 > \cdots > X_3X_2 > \cdots > X_1 > X_2 > \cdots X_n > 1$$

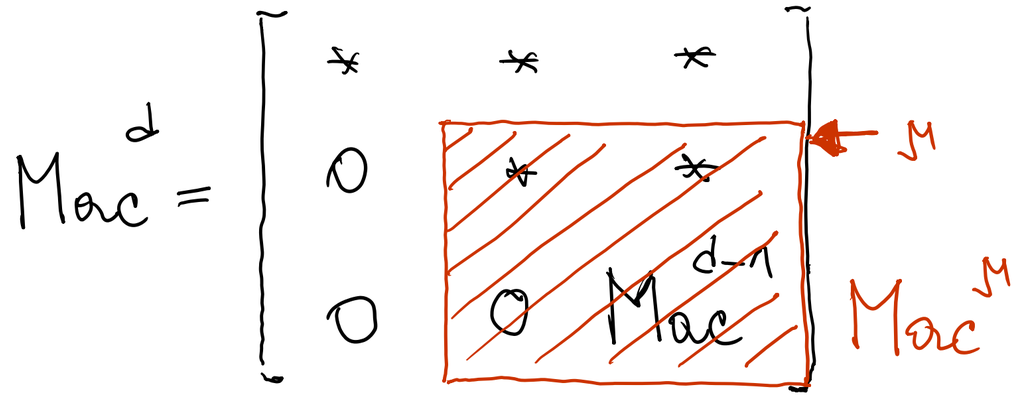
- Intuitively, we want the second shadow to map a number of rows to the least possible columns
- **Clements-Lindström** implies $\partial\big(\text{init}(S)\big) \subseteq \text{init}\big(\partial(S)\big).$
- **=> for initial segments** $\left|\partial^2(\mathcal{S})\right| = \min_{\substack{T \subseteq \mathcal{M}_d \\ |T|=|\mathcal{S}|}} \left|\partial^2(T)\right|.$

If S is initial segment in grevlex order, then it maps to the least number of columns compared to any other T of the same size

Let's attach a Macaulay matrix to the initial segment

Macaulay matrix Mac^{μ} for initial segment $\mathcal{S}_{\leq \mu}, \quad \mu \in \mathcal{M}_{d-2}$

- defined not by degree but by monomial
- Rows indexed by $(\nu, f_i), \quad \nu \in \mathcal{S},$ and columns indexed by $\nu \in \partial^2 \mathcal{S}$



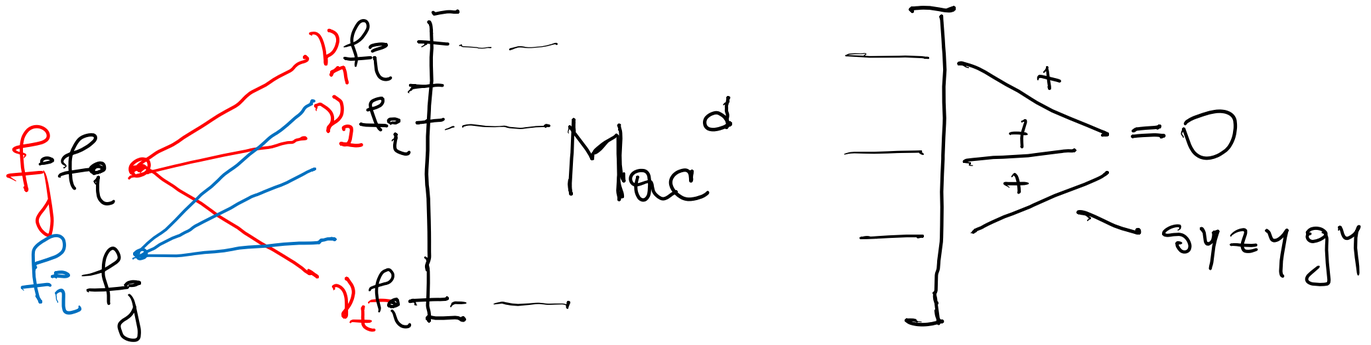
- Since $\mathrm{Mac}^{X_1^{d-2}} = \mathrm{Mac}^{d}$

=> Monomial Macaulay matrix generalizes Macaulay matrix

Initial segment Macaulay is optimal with respect to size

- **Matrix size is not the same as matrix rank**
- But good enough proxy
- Still, no guarantee for optimality with respect to rank (**open problem**)
- But good enough to show smoothing appears ☺
- What remains is to **predict the nullity of the initial segment Macaulay matrix**

Nullity of Macaulay matrix for semi-regular systems

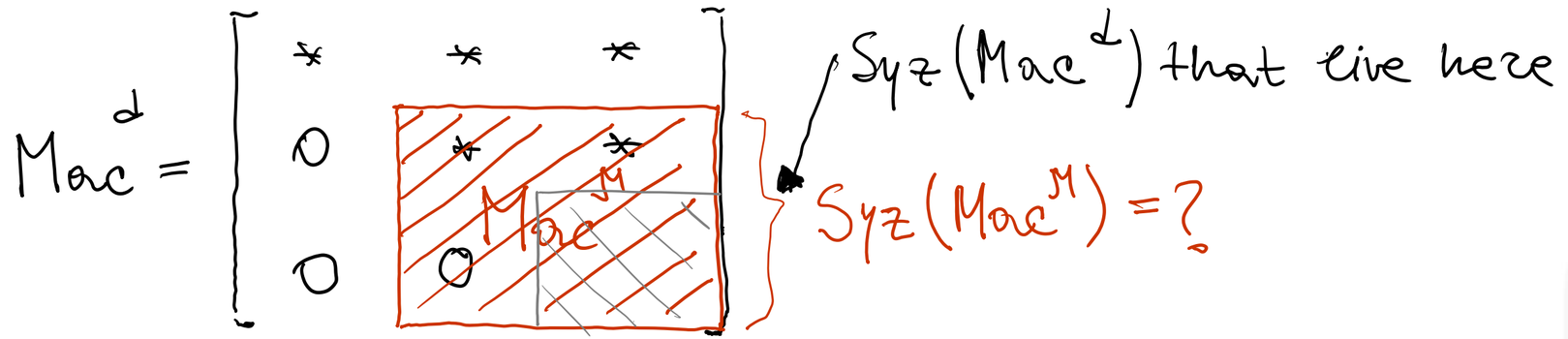


- **Trivial syzygies** – generated by $f_i \cdot f_j - f_j \cdot f_i = 0$
- **Semi regular sequence** [BFS04] – up to the degree of regularity **all syzygies are trivial**
- We can calculate the nullity of the Macaulay matrix by inclusion-exclusion

$$\text{null } \text{Mac}^d = \sum_{c=0}^{m} (-1)^{c+1} \binom{m}{c} |\mathcal{M}_{d-2c}|.$$

- corresponds to Hilbert series $\mathcal{H}(t) = \left[\frac{\prod_{i=1}^{m} (1 - t^{\deg f_i})}{(1-t)^n} \right]$

How to estimate the nullity of a monomial Macaulay matrix?



- We want (some sort of) a semi-regularity assumption
- **Monomial semi-regularity**
  - Up to the first μ where Mac^{μ} is solvable, all syzygies of Mac^{μ} are trivial syzygies of Mac^{d} .
  - This first μ - **monomial of regularity**

- More fine grained, but monomial semi-regularity does not imply semi-regularity ☹
  - Happens if $\deg(\mu_{reg}) < d_{reg}$

- **Conjecture:** Monomial semi-regularity is generic property.

Estimating the nullity of a monomial Macaulay matrix

- A useful toolbox - **anti-shadows** (inverse of shadows)

$$\partial^{-c}\mathcal{S} = \{\mu \mid \mu \cdot \mathcal{M}_c \subseteq \mathcal{S}\}$$

- Inclusion-exclusion to calculate the nullity of Mac^{μ}

$$\text{null } \mathrm{Mac}^{\mu} \approx \sum_{c \geq 0} (-1)^{c+1} \binom{m}{c} \left|\partial^{2-2c}(\mathcal{S})\right|.$$

- How to compute the size of anti-shadows?
  - rather technical (see paper)

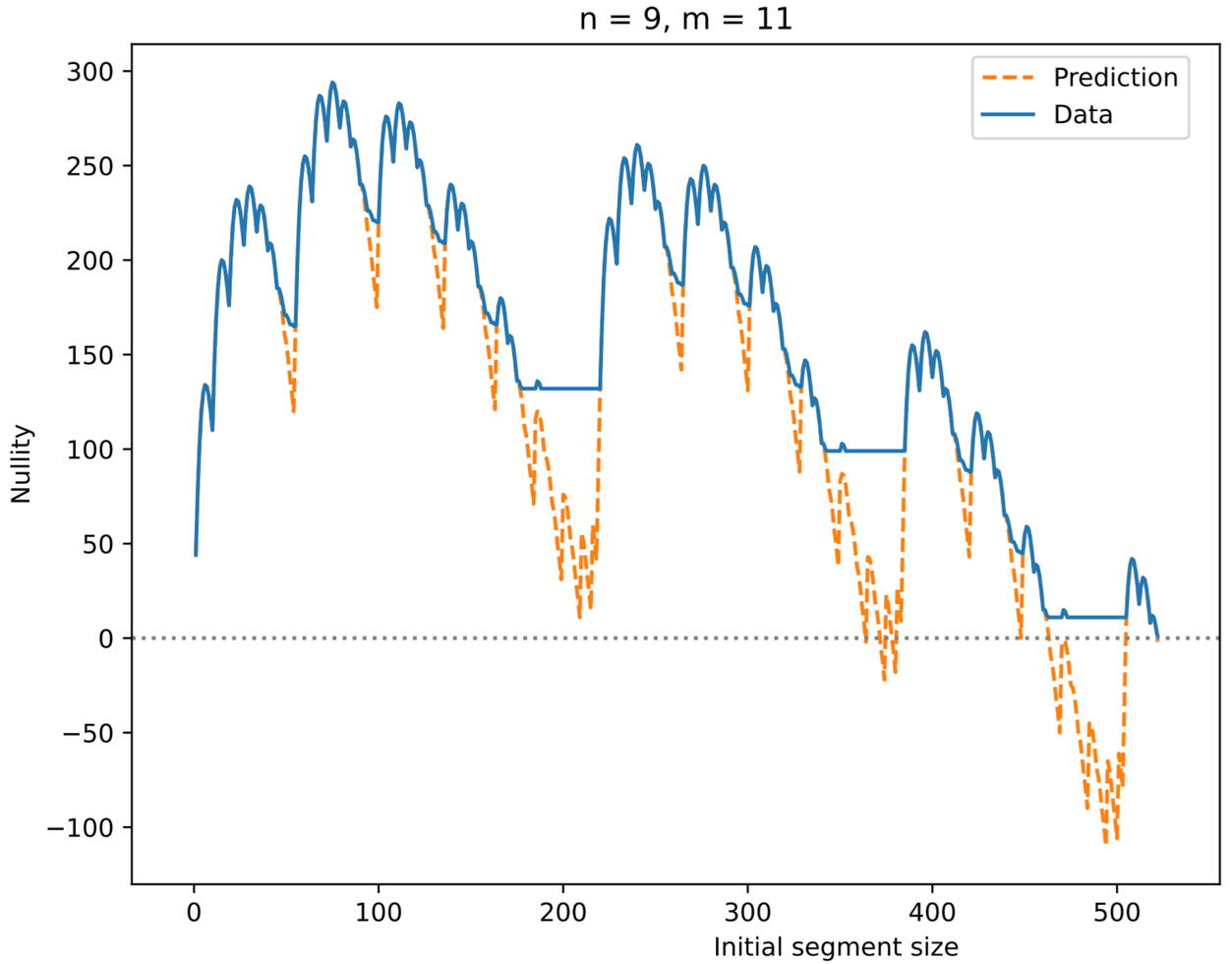
$$\text{for } \mu = X_{a_d} \cdots X_{a_{\ell+1}} \cdot X_1^{\ell}, \quad a_d \geq \cdots \geq a_{t+1} > 1$$

$$\text{null } \mathrm{Mac}^{\mu} \approx \sum_{c \geq 0} (-1)^{c+1} \binom{m}{c} \left(\left(\binom{n}{d-2c} \right) - \sum_{k=1}^{d-\ell} \left(\binom{a_k - 1}{k+2-2c} \right) \right)$$

Estimating the nullity of a monomial Macaulay matrix

$$\text{null } \text{Mac}^{\mu} \approx \sum_{c \geq 0} (-1)^{c+1} \binom{m}{c} \left| \partial^{2-2c}(\mathcal{S}) \right|.$$

- Not always equality ☹
- Correct for a great portion of monomials μ
- Let's try to estimate
  - When it is correct
  - If not, provide a more useful upper bound



Relations matrices for Macaulay matrices

- Let $\mathcal{R}_d = \langle \mathcal{M}_d \rangle_{\mathbb{F}}$
- Define relation matrices $\mathrm{Rel}_c^d(\mathcal{F}) : \mathcal{R}_{d-2c}^{\binom{m}{c}} \to \mathcal{R}_{d-2-2c}^{\binom{m}{c+1}}$
  - $\mathrm{Rel}_0^d(\mathcal{F}) = \mathrm{Mac}^d(\mathcal{F})$
  - $\mathrm{Rel}_c^d(\mathcal{F})$ encodes the trivial syzygies of $\mathrm{Rel}_{c-1}^d(\mathcal{F})$

$$\mathrm{Rel}_c^d(\mathcal{F}) \circ \mathrm{Rel}_{c-1}^d(\mathcal{F}) = 0$$

  - Space of all syzygies and Koszul (trivial) syzygies

$$\mathrm{Syz}_c^d = \mathrm{left\_ker}\, \mathrm{Rel}_{c-1}^d(\mathcal{F}) \quad \wedge \quad \mathrm{KSyz}_c^d = \mathrm{rowspace}\, \mathrm{Rel}_c^d(\mathcal{F}).$$

$$\mathrm{KSyz}_c^d \subseteq \mathrm{Syz}_c^d\,.$$

  - **For semi-regular sequences** $\mathrm{KSyz}_c^d = \mathrm{Syz}_c^d\,.$
  - (this is why our inclusion-exclusion argument works!)

Taking the analog for monomial Macaulay matrices

- **Which elements of** $\mathrm{KSyz}_c^d = \mathrm{rowspace}\,\mathrm{Rel}_c^d$ **define trivial syzygies of** $\mathrm{Mac}^\mu(\mathcal{F})$ **?**
- Define $\mathrm{sRel}_c^\mu(\mathcal{F})$ - submatrix of $\mathrm{Rel}_c^d(\mathcal{F})$
  - Rows indexed by $\partial^{-2c}(\mathcal{S}) \times \mathrm{Subsets}_{c+1}([m])$
  - Columns indexed by $\partial^{2-2c}(\mathcal{S}) \times \mathrm{Subsets}_c([m])$
  - Again $\mathrm{sRel}_0^\mu(\mathcal{F}) = \mathrm{Mac}^\mu(\mathcal{F})$ and $\mathrm{sRel}_c^\mu(\mathcal{F}) \circ \mathrm{sRel}_{c-1}^\mu(\mathcal{F}) = 0$
  - ∂ **- trivial syzygies of** $\mathrm{Mac}^\mu(\mathcal{F})$**:** $\mathrm{rowspace}(\mathrm{sRel}^\mu)$
  - So far so good, but $\mathrm{rowspace}(\mathrm{sRel}_c^\mu) \neq$ All trivial syzygies of sRel_{c-1}^μ
  - **For monomial semi-regular sequences**

$$\mathrm{rowspace}(\mathrm{sRel}_c^\mu) \neq \mathrm{left\_ker}(\mathrm{sRel}_{c-1}^\mu)$$

  - (this is why our inclusion-exclusion argument does not work!)

iCIS | Digital Security
Radboud University

Partitioning the relation matrix

- So we have $\mathrm{KSyz}_c^{\mu} \supseteq \mathrm{rowspace}\, \mathrm{sRel}_c^{\mu}$.
- But we want to estimate the **dimension of the entire set of trivial syzygies**
- For

$$\begin{array}{rrl} \mu & (= & X_{a_{d-2}} \cdots \quad X_{a_2} X_{a_1}) \\ \leq \mu_1 & (= & X_{a_{d-2}} \cdots \quad X_{a_2} X_1) \\ \leq \mu_2 & (= & X_{a_{d-2}} \cdots X_{a_3} X_1^2) \\ \leq \mu_{d-2} & (= & X_1^{d-2}) \end{array}$$

- **=> A partition:** (where $\mathrm{Rel}_c^{\ell+2}(\pi_{a_\ell - 1}\mathcal{F})$ is a relation matrix on the projection to $\mathbb{F}[X_1, \ldots, X_{a_\ell - 1}]$)

$$\mathrm{sRel}_c^{\mu_\ell} = \left[\begin{array}{c|c} \mathrm{Rel}_c^{\ell+2}(\pi_{a_\ell - 1}\mathcal{F}) & * \\ \hline 0 & \mathrm{sRel}_c^{\mu_{\ell-1}} \end{array}\right] \quad \Rightarrow \quad \dim \mathrm{KSyz}^{\mu_\ell} - \dim \mathrm{KSyz}^{\mu_{\ell-1}} \geq \dim \mathrm{KSyz}^{\ell+2}(\pi_{a_\ell - 1}\mathcal{F})$$

A more accurate nullity bound

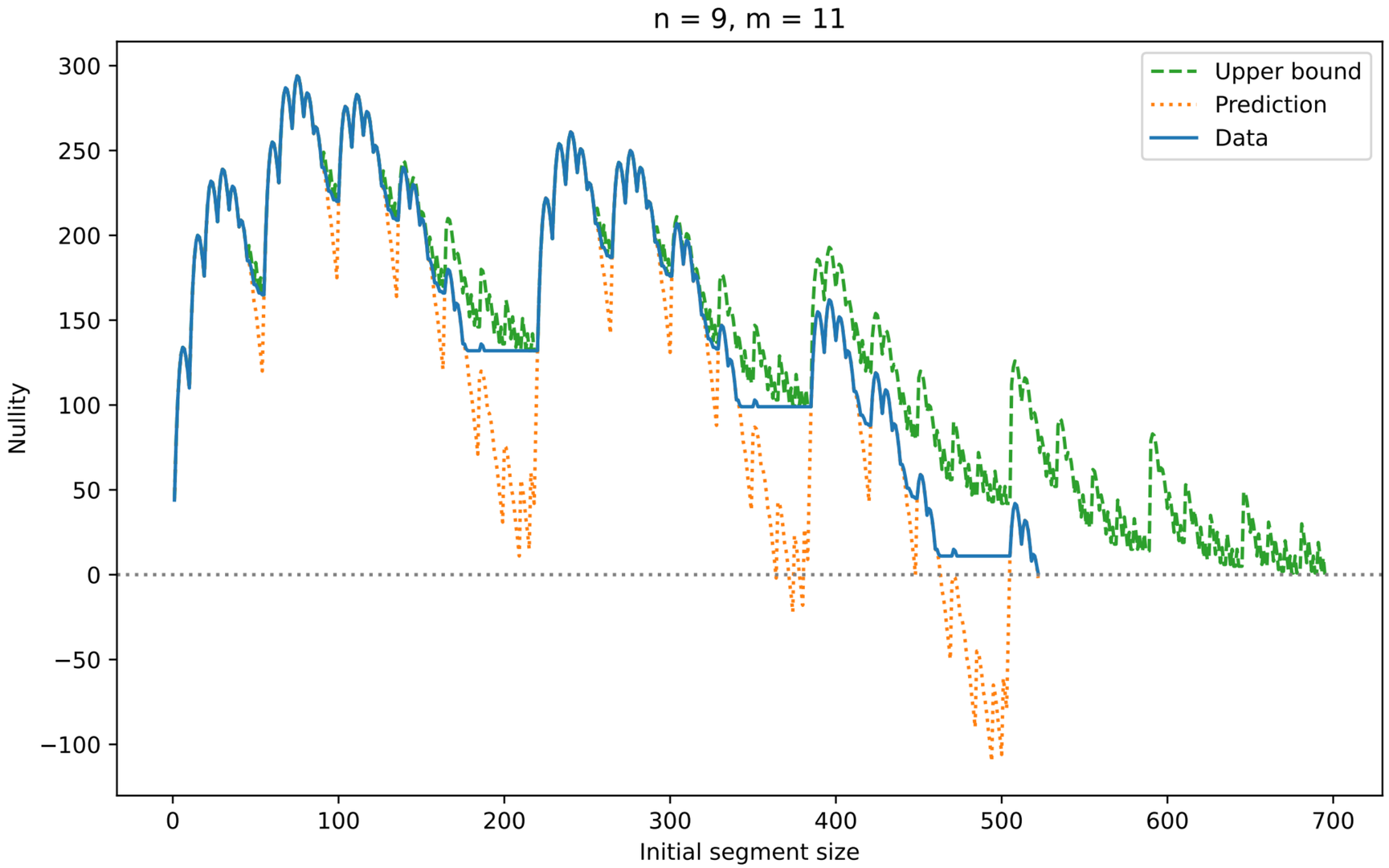
- Adding all up

$$\dim \mathrm{KSyz}_c^{\mu} \leq \dim \mathrm{KSyz}_c^{d} - \sum_{1 \leq k \leq d-2} \dim \mathrm{KSyz}_c^{k+2}(\pi_{a_k - 1}\mathcal{F}).$$

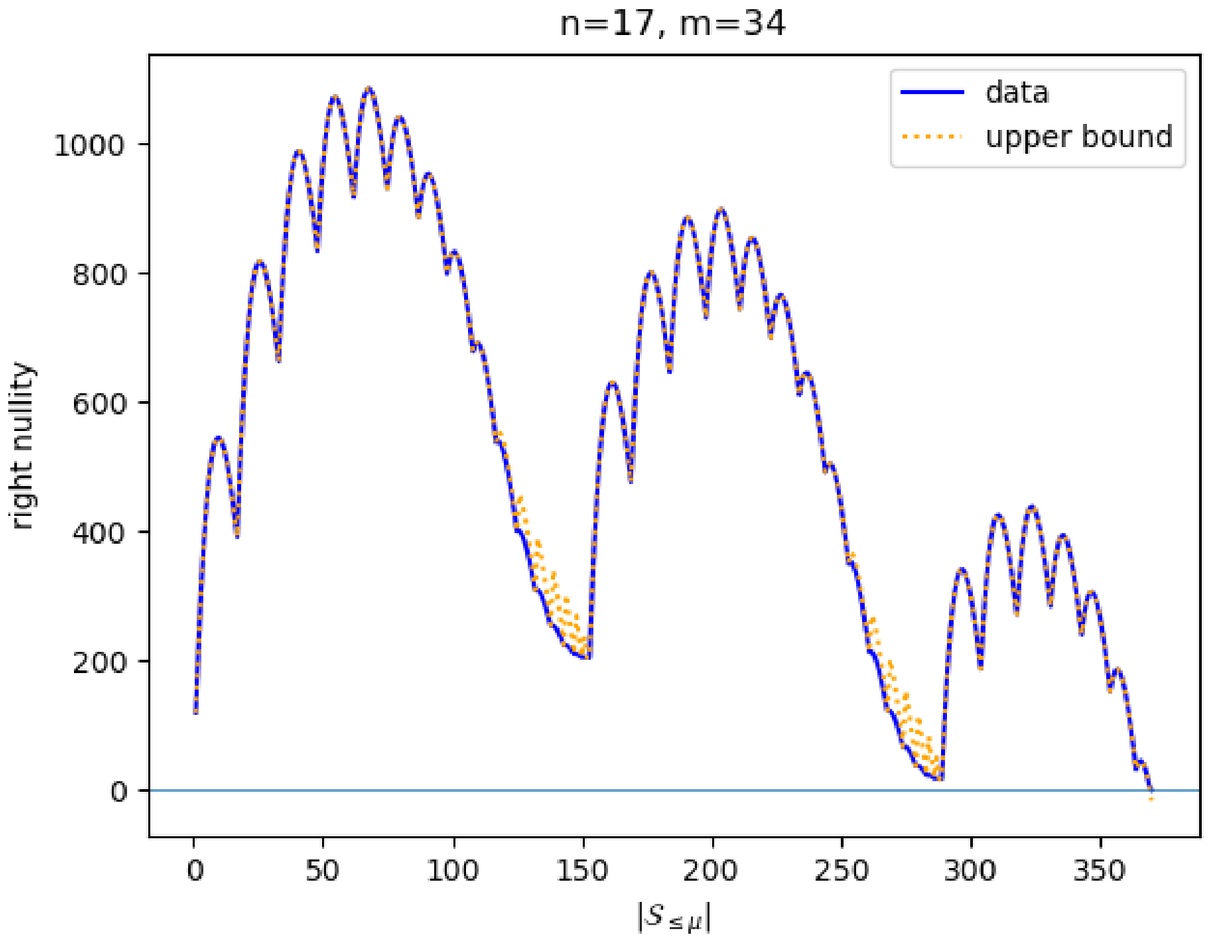
Theorem:

$$\operatorname{null} \mathrm{Mac}^{\mu} \leq |\partial^2 \mathcal{S}| - m|\mathcal{S}| + \dim \mathrm{KSyz}^{d} - \sum_{1 \leq k \leq d-2} \dim \mathrm{KSyz}^{k+2}(\pi_{a_k - 1}\mathcal{F}).$$

A more accurate nullity bound



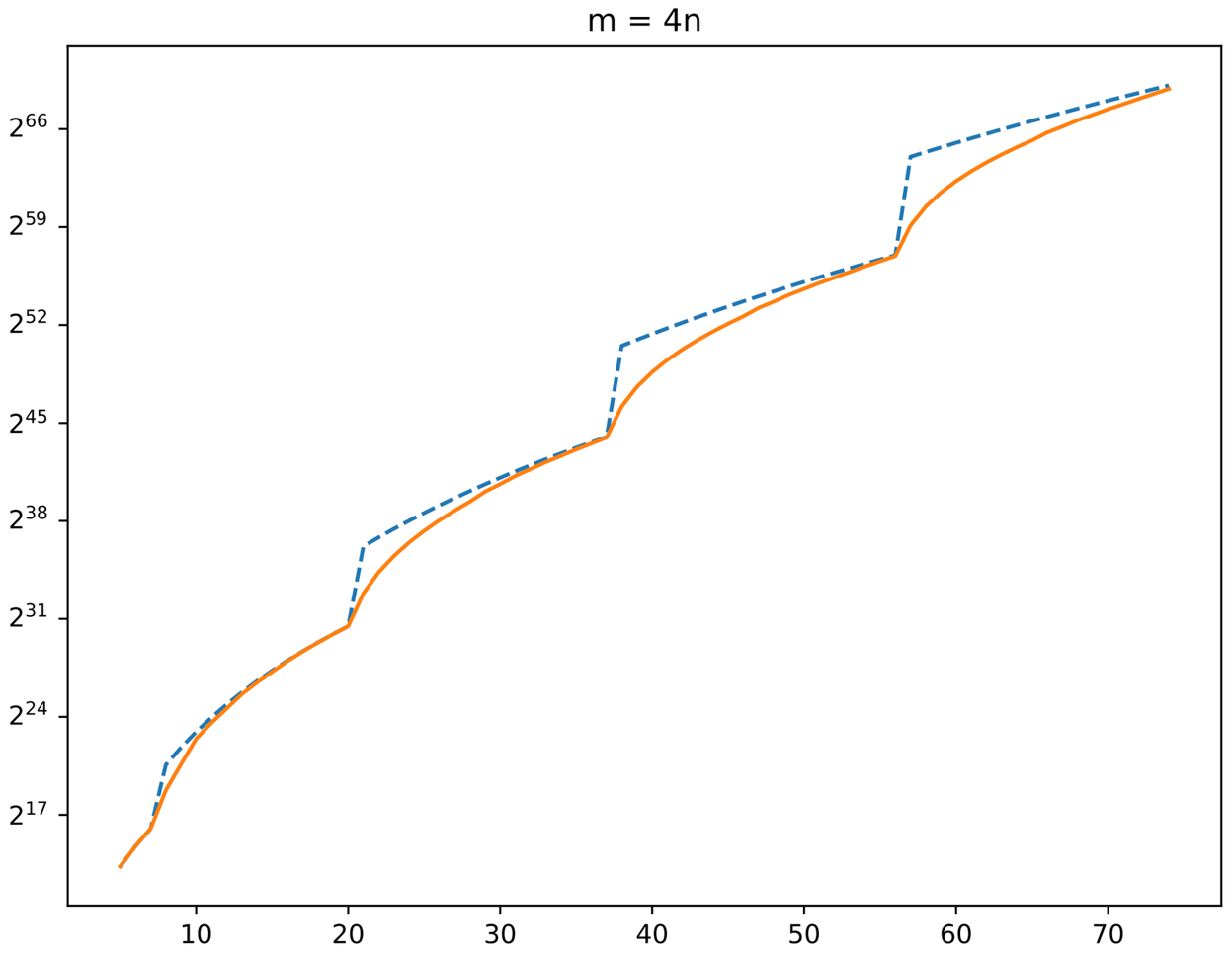
A more accurate nullity bound



Experiments

n	m	$\tilde{d}_{\text{reg}}$	experimental	prediction	XL
8	9	5	701	770	792
9	10	6	1938	2057	3003
10	11	6	4255	4914	5005
11	12	7	11798	12922	19448
9	11	5	1034	1126	1287
10	12	6	2967	3002	5005
11	13	6	5815	6025	8008
12	14	6	10373	12285	12376
11	16	5	2137	2137	3003
12	18	5	3042	3045	4368
13	19	5	5270	5326	6188
14	21	5	7565	7705	8568
9	18	4	284	284	495
10	20	4	501	501	715
16	32	5	6722	6722	15504
17	34	5	11441	11441	20349

Smoothing the complexity



Comparison to FXL

n	m	q	FXL			this paper		
			cost	k	d	cost	k	$\lvert\mathcal{S}_{\leq\mu}\rvert$
10	10	31	35.1	1	6	34.0	1	274
11	11	31	36.9	1	6	36.8	1	675
12	12	31	41.1	1	7	39.9	1	1676
13	13	31	42.7	1	7	42.7	2	609
14	14	31	45.0	2	6	44.9	2	1325
15	15	31	48.5	1	8	47.8	2	3145
16	16	31	50.7	2	7	50.4	2	7026
17	17	31	54.3	1	9	53.3	2	17823
18	18	31	56.4	2	8	55.8	2	39471
19	19	31	58.3	3	7	58.3	3	15358
20	20	31	62.1	2	9	61.1	2	219794
21	21	31	64.0	3	8	63.5	3	77922
22	22	31	67.7	2	10	66.4	3	201442

Thank you for listening!
?

Contact:
Simona Samardjiska
Department of Digital Security – Radboud University
simona.samardjiska@ru.nl