Algorithme de Changement d'Ordre de Complexité Sous-Cubique

Jean-Charles Faugère   Pierrick Gaudry   Louise Huot   Guénaël Renault

Motivation: zero-dim PoSSo and applications

PoSSo: Polynomial System Solving

PoSSo Problem: univariate polynomial representation

Input: $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$
Assumptions: $\mathcal{I}$ **radical** and **zero-dimensional**, $\mathbb{K}$ **infinite**
Output: $\mathcal{I} = \langle x_1 - h_1(x_n), \ldots, x_{n-1} - h_{n-1}(x_n), h_n(x_n) \rangle$.

Applications

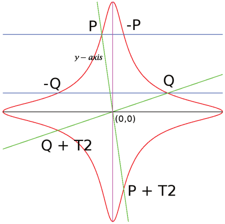
Coding theory, cryptanalysis, computational game theory, optimization, *etc*

Example: Point Decomposition Problem (DLP over Elliptic Curves)

$$R = P_1 \oplus \cdots \oplus P_n$$

$$P_i \in \mathcal{F}$$

Faugère, Gaudry, Huot, R. (J. Crypto 13)



State of the art

D = degree of $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$ = #solutions of $f_1 = \cdots = f_s = 0$.

Particular cases

$\mathbb{K}$ field of characteristic zero; $\delta \leq D$ number of real roots.

- (Mourrain, Pan 1998) Approximate all the real roots: $\widetilde{O}(12^n D^2)$ if $\delta = O(\log_2(D))$;
- (Bostan, Salvy, Schost 2003) RUR: $\widetilde{O}(n 2^n D^{\frac{5}{2}})$ if the multiplicative structure of the quotient ring is known.

General case

Computing **Univariate Polynomial Representation**: $O(nD^3)$.

Our aim

The **first algorithm** with sub-cubic complexity to solve this problem.

PoSSo and Gröbner basis

☞ Efficient Computation of 0-dim Gröbner Bases by Change of Ordering
(FGLM: Faugère, Gianni, Lazard, Mora 1993)

Univ. Pol. Representation $\simeq$ LEX Gröbner basis in *Shape position*.

Efficient Computation of a LEX Gröbner basis

Input: $S \subset \mathbb{K}[x_1, \ldots, x_n]$.
Output: The LEX Gröbner basis of $\langle S \rangle$.

1. Compute DRL Gröbner basis of $\langle S \rangle$;
2. Compute LEX Gröbner basis of $\langle S \rangle$ by change of ordering algorithm.

Gröbner basis and Complexity

$(f_1, \ldots, f_n)$ regular sequence with $\deg(f_i) \leq d$.
$2 \leq \omega < 2.3727$ is the linear algebra constant.

$\mathcal{I} = \langle f_1, \ldots, f_n \rangle$

↓ F_4, F_5 (Bardet, Faugère, Salvy 2005) $O\left(d^{\omega n}\right)$

GB DRL

↓ Change of Ordering

- generic $\mathcal{I}$: (Faugère, Mou 2013) $O\left(\sqrt{\frac{6}{n\pi}} D^{2+\frac{n-1}{n}}\right)$
- non-generic $\mathcal{I}$: (FGLM 1993) $O(nD^3)$.

GB LEX

Gröbner basis and Complexity

$(f_1, \ldots, f_n)$ regular sequence with $\deg(f_i) \leq d$.
$2 \leq \omega < 2.3727$ is the linear algebra constant.

$\mathcal{I} = \langle f_1, \ldots, f_n \rangle$

F_4, F_5 (Bardet, Faugère, Salvy 2005) $O\left(d^{\omega n}\right)$

$\rightarrow$ Bézout's bound reached: $O(D^\omega)$

GB DRL

Change of Ordering

Bottleneck

- generic $\mathcal{I}$: (Faugère, Mou 2013) $O\left(\sqrt{\frac{6}{n\pi}} D^{2+\frac{n-1}{n}}\right)$
- non-generic $\mathcal{I}$: (FGLM 1993) $O(nD^3)$.

GB LEX

☞ Change of ordering in $\tilde{O}(nD^\omega) \Rightarrow$ PoSSo in $\tilde{O}(d^{\omega n} + nD^\omega)$

Change of Ordering Complexity: Contributions

GB DRL

Change of Ordering

GB LEX

Bottleneck

- generic $\mathcal{I}$: (Faugère, Mou 2013) $O\left(\sqrt{\frac{6}{n\pi}}D^{2+\frac{n-1}{n}}\right)$
- non-generic $\mathcal{I}$: (FGLM 1993) $O(nD^3)$.

☞ Change of ordering in $\tilde{O}(nD^\omega) \Rightarrow$ PoSSo in $\tilde{O}(d^{\omega n} + nD^\omega)$

Contributions

- Consideration of Faugère & Mou in the non sparse case
- Use of the staircases structures for LEX and DRL Gröbner basis

Gröbner basis

Initial ideal

$\mathcal{I}$ an ideal and $>$ a monomial ordering $\text{in}_>(\mathcal{I}) = \{\text{LT}_>(f) \mid f \in \mathcal{I}\}$.

Gröbner basis (**not unique**)

Fix a monomial ordering $>$, $\{g_1, \ldots, g_s\}$ GB w.r.t. $>$ of $\mathcal{I}$ if

- $\{g_1, \ldots, g_s\} \subset \mathcal{I}$;
- $\langle \text{LT}_>(g_1), \ldots, \text{LT}_>(g_s) \rangle = \text{in}_>(\mathcal{I})$.

Reduced Gröbner basis (**unique**)

$G = \{g_1, \ldots, g_s\}$ GB of $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$ w.r.t. $>$ s.t.

$$\text{LT}_>(g_i) \text{ does not divide any terms in } g_j \text{ for all } 1 \leq i \neq j \leq s\,.$$

$\Rightarrow g_i = \text{LT}_>(g_i) + \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$ with $x^\alpha \notin \text{in}_>(\mathcal{I})$.

Quotient ring

Normal Form

Let $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. For any $f \in \mathbb{K}[x_1, \ldots, x_n]$ there exists a unique $h \in \mathbb{K}[x_1, \ldots, x_n]$ s.t.

- $f - h \in \mathcal{I}$;
- $h = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$ with $x^\alpha \notin \mathsf{in}_> (\mathcal{I})$.

$$h = \mathsf{NF}_> (f)$$

Quotient ring as $\mathbb{K}$-vector space of dimension D

$$\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I} = \{[f] \mid f \in \mathcal{I}\} \simeq \mathrm{Span}(x^\alpha \notin \mathsf{in}_> (\mathcal{I}))$$

with $[f] = \{h \in \mathbb{K}[x_1, \ldots, x_n] \mid f - h \in \mathcal{I}\}$.

$$\mathcal{I} \text{ dimension zero } \Rightarrow \{x^\alpha \notin \mathsf{in}_> (\mathcal{I})\} = \{\epsilon_D > \cdots > \epsilon_1 = 1\}$$

Change of ordering algorithm: key ideas

Coordinate vector ($\mathcal{G}_>$ GB of $\mathcal{I}$ w.r.t. $>$)

$v_\alpha = (c_1, \ldots, c_D)$ s.t. $\mathsf{NF}_>(x^\alpha) = \sum_{i=1}^{D} c_i \epsilon_i$.

$$f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha \in \mathcal{I} \Leftrightarrow \mathsf{NF}_>(f) = 0 \Leftrightarrow \sum_{\alpha \in \mathbb{N}^n} c_\alpha v_\alpha = 0$$

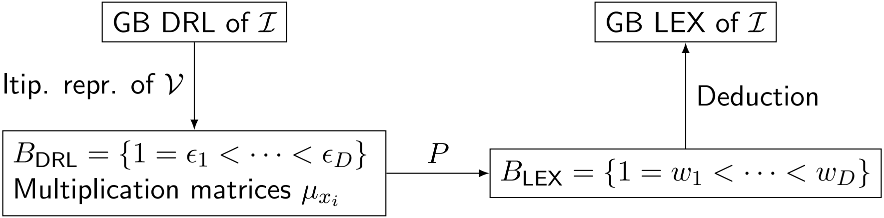
Multiplication matrices $\mu_{x_1}, \ldots, \mu_{x_n}$

$$\mu_{x_i} = \begin{array}{c} \begin{matrix} \mathsf{NF}_>(\epsilon_1 x_i) & \cdots & \mathsf{NF}_>(\epsilon_D x_i) \end{matrix} \\ \begin{pmatrix} \star & \cdots & \star \\ \vdots & \ddots & \vdots \\ \star & \cdots & \star \end{pmatrix} \begin{matrix} \epsilon_1 \\ \vdots \\ \epsilon_D \end{matrix} \end{array}$$

Let $\mathbf{1} = (1, 0, \ldots, 0) = v_{(0,\ldots,0)} \rightsquigarrow v_\alpha = \mu_{x_1}^{\alpha_1} \cdots \mu_{x_n}^{\alpha_n} \mathbf{1}$

FGLM in a nutshell

From DRL to LEX with $x_1 > x_2 > \cdots > x_n$
$\mathcal{V} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ is a D-dim $\mathbb{K}$-vector space

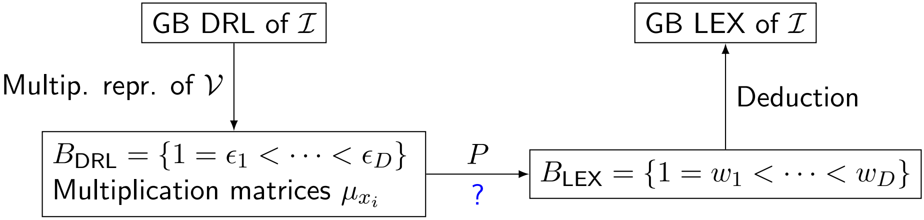


- $B_{\text{DRL}} = P \cdot B_{\text{LEX}}$
- $\mu_{x_i} : t \to \text{NF}_{\text{DRL}}(x_i t)$

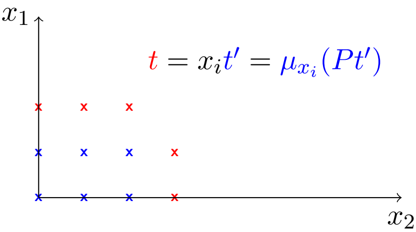
FGLM in a nutshell

From DRL to LEX with $x_1 > x_2 > \cdots > x_n$

$\mathcal{V} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ is a D-dim $\mathbb{K}$-vector space



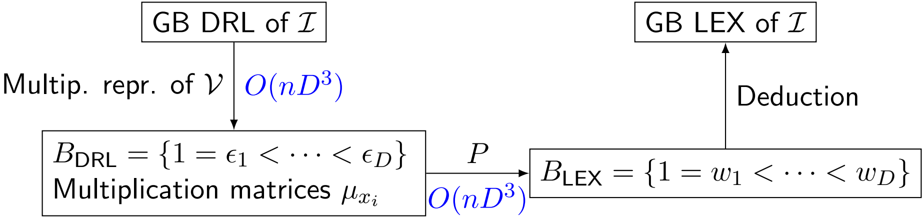
Assume the μ_{x_i} known



- $B_{\mathsf{DRL}} = P \cdot B_{\mathsf{LEX}}$
- $\mu_{x_i} : t \to \mathsf{NF}_{\mathsf{DRL}}(x_i t)$

FGLM in a nutshell

From DRL to LEX with $x_1 > x_2 > \cdots > x_n$
$\mathcal{V} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ is a D-dim $\mathbb{K}$-vector space



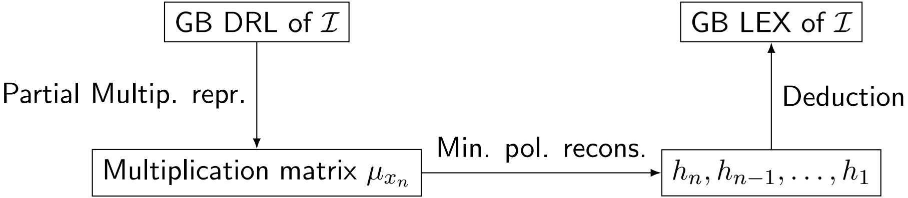
- $B_{\text{DRL}} = P \cdot B_{\text{LEX}}$
- $\mu_{x_i} : t \to \text{NF}_{\text{DRL}}(x_i t)$

☞ Use structures of GB LEX

Faugère & Mou Sparse FGLM framework

Assumption: GB LEX of $\mathcal{I}$ is in *shape position*

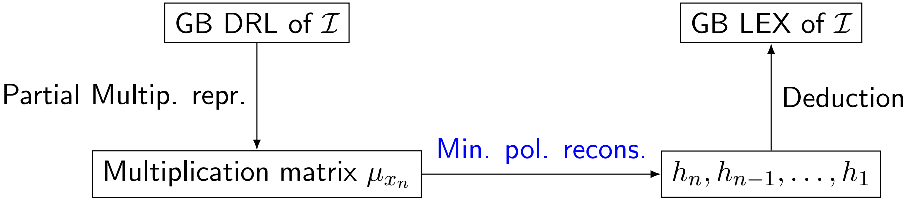
$$\mathcal{I} = \langle x_1 - h_1(x_n), \ldots, x_{n-1} - h_{n-1}(x_n), h_n(x_n) \rangle$$



Faugère & Mou Sparse FGLM framework

Assumption: GB LEX of $\mathcal{I}$ is in *shape position*

$$\mathcal{I} = \langle x_1 - h_1(x_n), \dots, x_{n-1} - h_{n-1}(x_n), h_n(x_n) \rangle$$



Faugère & Mou reconstruction of h_i: deterministic Wiedemann

- $\mu_{x_n}^j \cdot \mathbf{1}, \mu_{x_n}^j(\mu_{x_1} \cdot \mathbf{1}), \dots, \mu_{x_n}^j(\mu_{x_{n-1}} \cdot \mathbf{1}),\ j \in \{0, \dots, 2D-1\}$
- n Hankel linear systems to solve $\tilde{O}(nD^2)$

Faugère & Mou Sparse FGLM framework

$h_n : S = [(\mathbf{r}, \mu_{x_n}^j \mathbf{1}) \mid j = 0, \dots, 2D-1]$ with $(\mathbf{r}, \mu_{x_n}^j \mathbf{1}) = ({}^t\mu_{x_n}^j \mathbf{r}, \mathbf{1})$

Compute $h_1, \dots, h_{n-1}$

$h_i(x_n) = \sum_{k=0}^{D-1} c_{i,k} x_n^k$

$$x_i - h_i(x_n) \in \mathcal{I} \quad \Leftrightarrow \quad \mu_{x_i}\mathbf{1} - \sum_{k=0}^{D-1} c_{i,k}\mu_{x_n}^k \mathbf{1} = \mathbf{0}$$

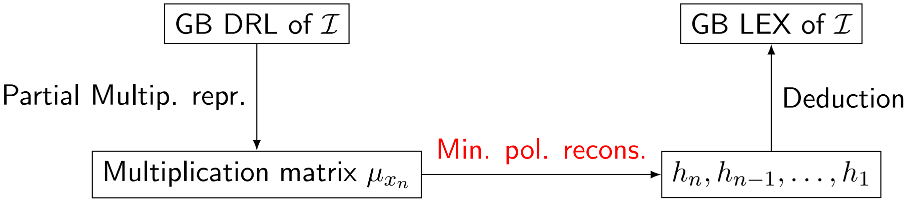
$\times \mu_{x_n}^j$ for $j = 0, \dots, D-1$ and $(r, \cdot) \rightsquigarrow$ Hankel linear systems

$$\underbrace{\begin{pmatrix} ({}^t\mu_{x_n}^0 \mathbf{r}, \mu_{x_i}\mathbf{1}) \\ ({}^t\mu_{x_n}^1 \mathbf{r}, \mu_{x_i}\mathbf{1}) \\ \vdots \\ ({}^t\mu_{x_n}^{D-1} \mathbf{r}, \mu_{x_i}\mathbf{1}) \end{pmatrix}}_{\mathbf{b_i}} = \underbrace{\begin{pmatrix} ({}^t\mu_{x_n}^0 \mathbf{r}, \mathbf{1}) & ({}^t\mu_{x_n}^1 \mathbf{r}, \mathbf{1}) & \dots & ({}^t\mu_{x_n}^{D-1} \mathbf{r}, \mathbf{1}) \\ ({}^t\mu_{x_n}^1 \mathbf{r}, \mathbf{1}) & ({}^t\mu_{x_n}^2 \mathbf{r}, \mathbf{1}) & \dots & ({}^t\mu_{x_n}^{D} \mathbf{r}, \mathbf{1}) \\ \vdots & \vdots & \ddots & \vdots \\ ({}^t\mu_{x_n}^{D-1} \mathbf{r}, \mathbf{1}) & ({}^t\mu_{x_n}^{D} \mathbf{r}, \mathbf{1}) & \dots & ({}^t\mu_{x_n}^{2D-2} \mathbf{r}, \mathbf{1}) \end{pmatrix}}_{\mathcal{H}} \underbrace{\begin{pmatrix} c_{i,0} \\ c_{i,1} \\ \vdots \\ c_{i,D-1} \end{pmatrix}}_{\mathbf{c_i}}$$

Faugère & Mou Sparse FGLM framework

Assumption: GB LEX of $\mathcal{I}$ is in *shape position*

$$\mathcal{I} = \langle x_1 - h_1(x_n), \ldots, x_{n-1} - h_{n-1}(x_n), h_n(x_n) \rangle$$



Faugère & Mou reconstruction of h_i: deterministic Wiedemann μ_{x_n} dense

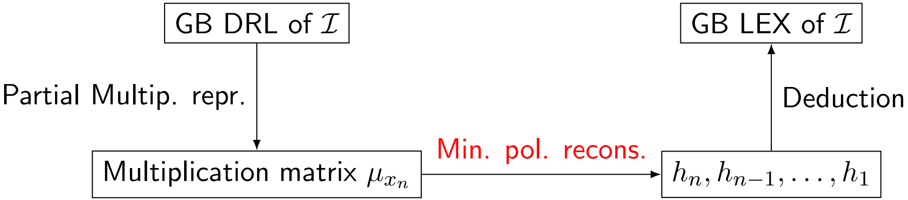
- $\mu_{x_n}^j \cdot \mathbf{1}, \mu_{x_n}^j(\mu_{x_1} \cdot \mathbf{1}), \ldots, \mu_{x_n}^j(\mu_{x_{n-1}} \cdot \mathbf{1}),\ j \in \{0, \ldots, 2D-1\}$ $O(nD^3)$
- n Hankel linear systems to solve $\tilde{O}(nD^2)$

☞ $\mu_{x_i} \cdot \mathbf{1} = x_1$ is known with no cost $\Rightarrow$ μ_{x_n} is sufficient!

Faugère & Mou Sparse FGLM framework

Assumption: GB LEX of $\mathcal{I}$ is in *shape position*

$$\mathcal{I} = \langle x_1 - h_1(x_n), \ldots, x_{n-1} - h_{n-1}(x_n), h_n(x_n) \rangle$$



Contribution: use of Keller-Gehrig $O(n \log(D) D^\omega)$

$$\mu_{x_n}^2 \left(\mu_{x_n}\mathbf{r} \mid \mathbf{r}\right) = \left(\mu_{x_n}^3\mathbf{r} \mid \mu_{x_n}^2\mathbf{r}\right)$$

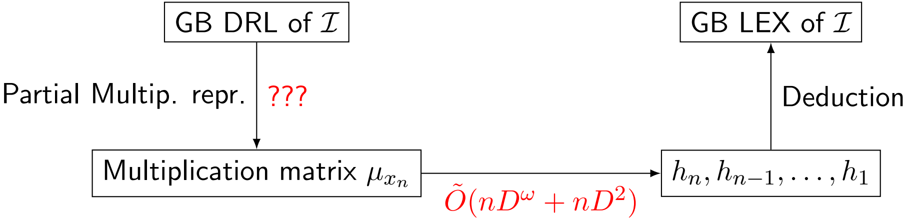
$$\vdots$$

$$\mu_{x_n}^{2^{\lceil \log_2(D) \rceil}} (\mu_{x_n}^{2^{\lceil \log_2(D) \rceil}-1}\mathbf{r}| \ldots |\mathbf{r}) = (\mu_{x_n}^{2D-1}\mathbf{r}|\mu_{x_n}^{2D-2}\mathbf{r}| \ldots |\mu_{x_n}^{2^{\lceil \log_2(D) \rceil}}\mathbf{r})$$

Faugère & Mou Sparse FGLM framework

Assumption: GB LEX of $\mathcal{I}$ is in *shape position*

$$\mathcal{I} = \langle x_1 - h_1(x_n), \ldots, x_{n-1} - h_{n-1}(x_n), h_n(x_n) \rangle$$



Contribution: use of Keller-Gehrig $O(n \log(D) D^\omega)$

$$\mu_{x_n}^2 \left(\mu_{x_n} \mathbf{r} \mid \mathbf{r} \right) = \left(\mu_{x_n}^3 \mathbf{r} \mid \mu_{x_n}^2 \mathbf{r} \right)$$

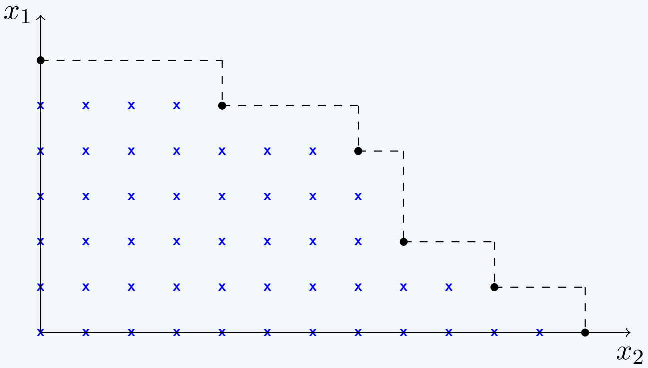
$$\vdots$$

$$\mu_{x_n}^{2^{\lceil \log_2(D) \rceil}} \left(\mu_{x_n}^{2^{\lceil \log_2(D) \rceil} - 1} \mathbf{r} | \ldots | \mathbf{r} \right) = \left(\mu_{x_n}^{2D-1} \mathbf{r} | \mu_{x_n}^{2D-2} \mathbf{r} | \ldots | \mu_{x_n}^{2^{\lceil \log_2(D) \rceil}} \mathbf{r} \right)$$

Computing μ_{x_n}: the FGLM Lemma

Computing μ_{x_n} $\Leftrightarrow$ computing $\mathsf{NF}_{drl}\left(\epsilon_i x_n\right)$ $i \in \{1, \ldots, D\}$.

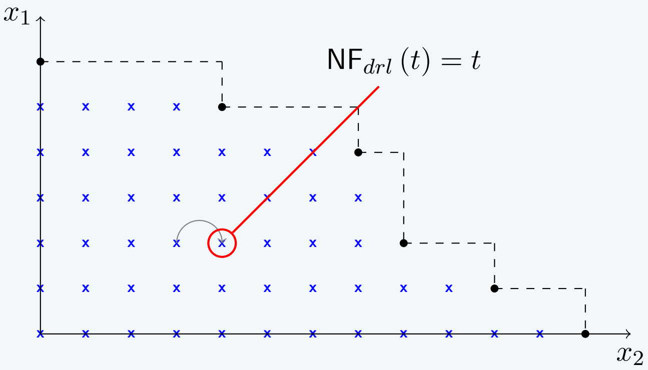
FGLM Lemma – Only three cases to consider



Computing μ_{x_n}: the FGLM Lemma

$$\text{Computing } \mu_{x_n} \Leftrightarrow \text{computing } \mathsf{NF}_{drl}(\epsilon_i x_n)\ i \in \{1, \ldots, D\}.$$

FGLM Lemma – Only three cases to consider

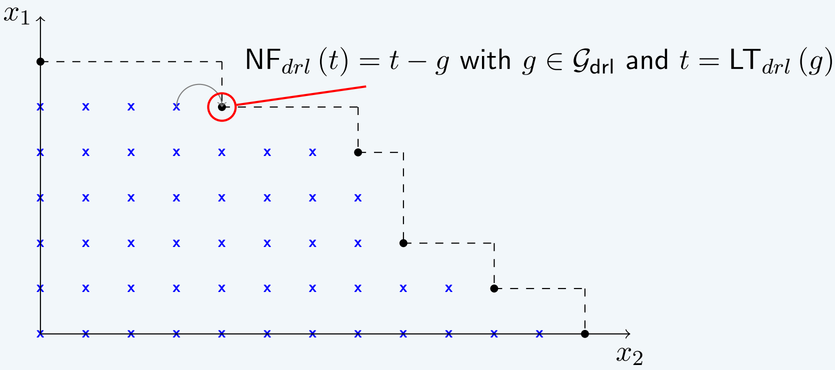


Case (1) $t = \epsilon_i x_j \in B$

Computing μ_{x_n}: the FGLM Lemma

Computing $\mu_{x_n} \Leftrightarrow$ computing $\mathsf{NF}_{drl}(\epsilon_i x_n)$ $i \in \{1, \ldots, D\}$.

FGLM Lemma – Only three cases to consider



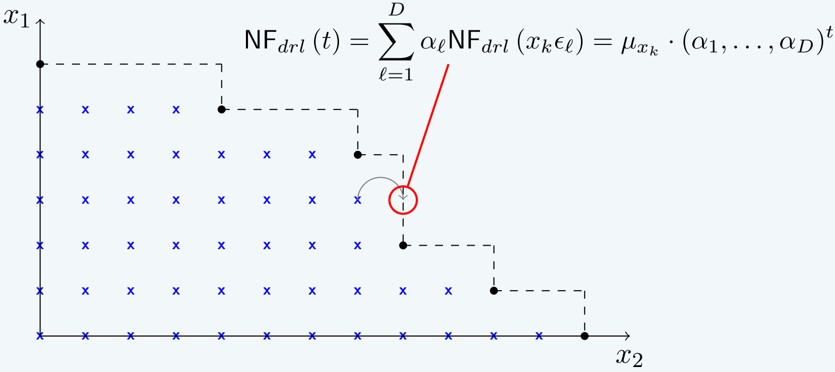
Case (2) $t = \epsilon_i x_j \in E(I) = \{\mathsf{LT}_{drl}(g) \mid g \in \mathcal{G}_{\mathsf{drl}}\}$

Computing μ_{x_n}: the FGLM Lemma

Computing μ_{x_n} $\Leftrightarrow$ computing $\mathsf{NF}_{drl}(\epsilon_i x_n)$ $i \in \{1, \ldots, D\}$.

$F = \{\epsilon_i x_j \mid i = 1, \ldots, D$ and $j = 1, \ldots, n\} \setminus B$: border

FGLM Lemma – Only three cases to consider



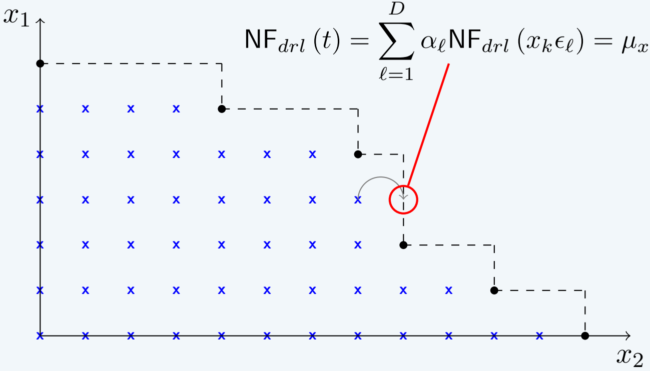
Case (3) $t = \epsilon_i x_i \in F \setminus E(I) \Rightarrow t = x_k t'$ with $t' \in F$ with $\mathsf{NF}_{drl}(t') = \sum_{i=\ell}^{D} \alpha_\ell \epsilon_\ell$

Computing μ_{x_n}: the FGLM Lemma

Computing μ_{x_n} $\Leftrightarrow$ computing $\mathsf{NF}_{drl}\left(\epsilon_i x_n\right)$ $i \in \{1,\ldots,D\}$.

FGLM Lemma – Only three cases to consider

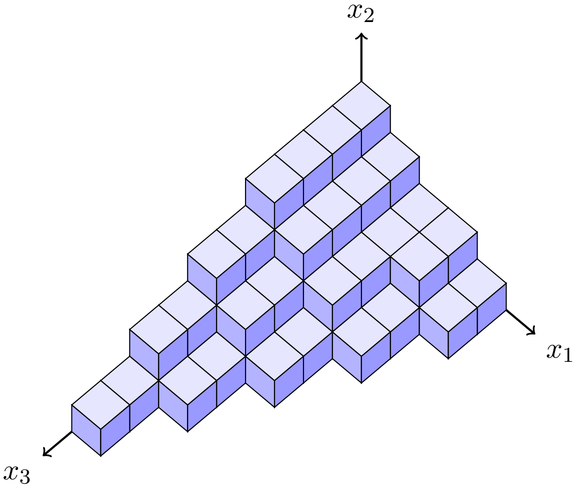
$$\mathsf{NF}_{drl}\left(t\right) = \sum_{\ell=1}^{D} \alpha_\ell \mathsf{NF}_{drl}\left(x_k \epsilon_\ell\right) = \mu_{x_k} \cdot (\alpha_1,\ldots,\alpha_D)^t$$



☞ Only the Case (3) is costly - can a structure avoid it?

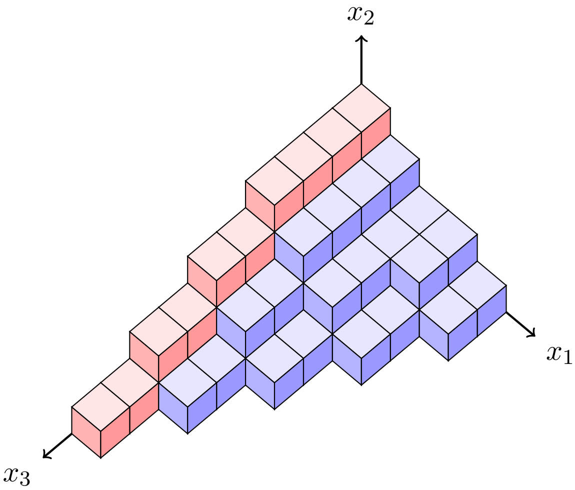
The $(1, 2)$-staircases position

DRL ordering with $x_1 > x_2 > x_3$



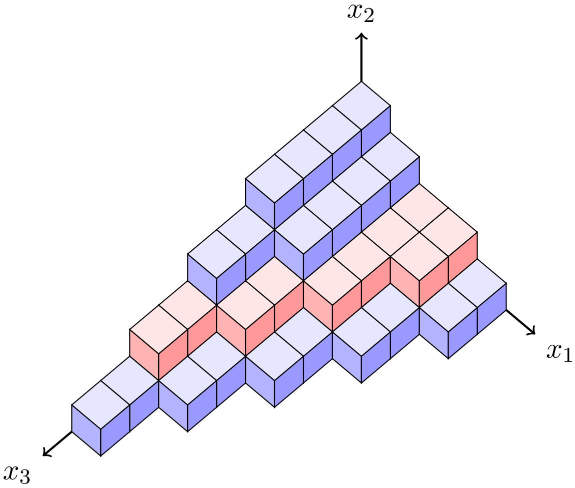
The $(1, 2)$-staircases position

DRL ordering with $x_1 > x_2 > x_3$



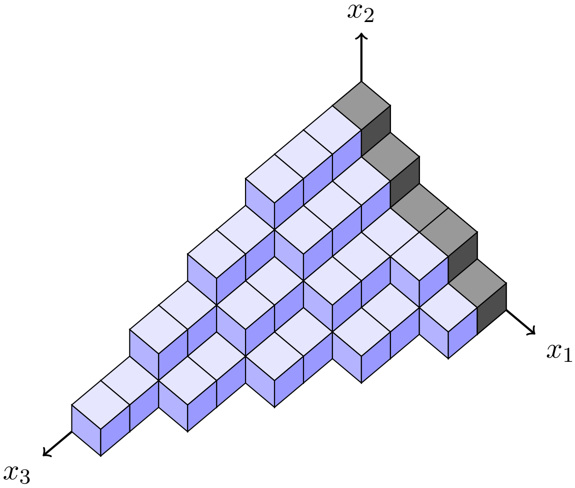
The $(1,2)$-staircases position

DRL ordering with $x_1 > x_2 > x_3$



The $(1, 2)$-staircases position

DRL ordering with $x_1 > x_2 > x_3$



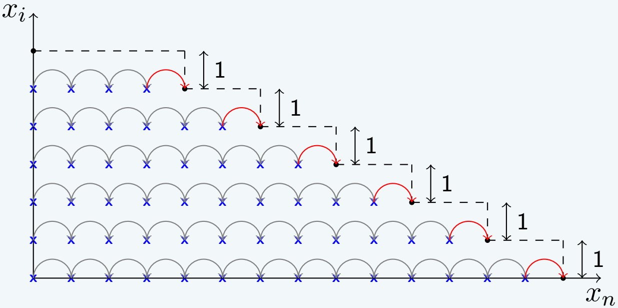
The $(1,2)$-staircases position: Generic Ideals

Moreno-Socias 1992

For a generic ideal $\mathcal{I}$, its DRL GB verifies $\epsilon x_n \in B \cup E(I)$ for $\epsilon \in B$.
A generic ideal is in $(1,2)$-*staircases position*.

FGLM Lemma: the no cost situation

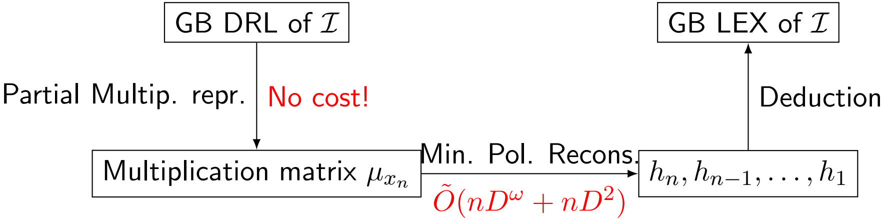
For any instantiation of $\deg_{x_j}$ for $j \in \{1, \ldots, n-1\} \setminus \{i\}$



☞ The computation of μ_{x_n} is free!

Faugère & Mou Sparse FGLM framework

Assumptions: LEX GB of $\mathcal{I}$ is in *shape position*
DRL GB of $\mathcal{I}$ is in $(1,2)$-*staircases position* (Generic Ideals)



☞ Non generic ideals?

$(1,2)$-staircases and shape position

Galligo, Bayer and Stillman, Pardue (1970's - 2000's)

$\mathcal{I}$ an *homogeneous ideal*. There exists a Zariski open subset $U \subset \mathsf{GL}(\mathbb{K}, n)$ s.t. $\forall g \in U$, $g \cdot I$ is in *(1,2)-staircases position*.

Shape Lemma, Gianni and Mora (1989)

$\mathcal{I}$ a *radical* ideal. There exists a Zariski open subset $U' \subset \mathsf{GL}(\mathbb{K}, n)$ s.t. $\forall g \in U'$, $g \cdot I$ is in *Shape position*.

Main theorem

☞ The $(1,2)$-staircases and shape position is generic!

$\mathcal{I}$ regular affine 0-dim and radical and $g \in U \cap U'(\neq \emptyset)$. The change of ordering from DRL to LEX of $g \cdot \mathcal{I}$ can be done in

$$\tilde{O}(nD^\omega + nD^2)$$

☞ "*Randomization*" on the choice of g

New algorithm for PoSSo

Let d such that $\deg(f_i) \leq d$.

Algorithm 1: Another algorithm for PoSSo.

Input : $S = \{f_1, \ldots, f_n\} \subset \mathbb{K}[x_1, \ldots, x_n]$ s.t. $\langle S \rangle$ is radical and regular.
Output: g in GL$(\mathbb{K}, n)$ and the LEX Gröbner basis of $\langle g \cdot S \rangle$ or *fail*.

"*Randomly*" choose g in GL$(\mathbb{K}, n)$;
Compute $\mathcal{G}_{\mathsf{drl}}$ the DRL GB $g \cdot S$; $O(d^{\omega n})$
if μ_{x_n} *can be read from* $\mathcal{G}_{drl}$ **then**
  Extract μ_{x_n} from $\mathcal{G}_{\mathsf{drl}}$; No cost
  if $\langle g \cdot S \rangle$ *is in Shape Position* **then**
    From μ_{x_n} and $\mathcal{G}_{\mathsf{drl}}$ compute $\mathcal{G}_{\mathsf{lex}}$; $O(\log_2(D)(nD^\omega + n\log_2(D)D^2))$
    return g and $\mathcal{G}_{\mathsf{lex}}$;
return *fail*;

Total complexity: $\tilde{O}(d^{\omega n} + nD^\omega)$ arithmetic operations.

Practical implications

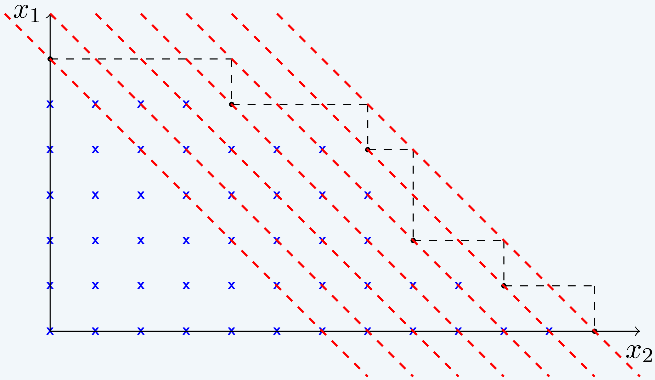
System	n	D	Algorithm	$\mathcal{G}_{\text{drl}}$	μ_{x_n}	#NF	$\mathcal{G}_{\text{lex}}$	Total
Random $d = 2$	15	32 768	usual	**1 580s**	41.5s	0	1 330s	2 950s
			This work	**1 580s**	41.5s	0	1 330s	2 950s
Random $d = 6$	6	46 656	usual	632s	20.3s	0	**1 700s**	2 350s
			This work	632s	20.3s	0	**1 700s**	2 350s
Random $d = 30$	3	27 000	usual	48.7s	0.9s	0	**95.6s**	145s
			This work	48.7s	0.9s	0	**95.6s**	145s
Eco	13	2 048	usual	28.2s	**36.5s**	1 153	0.43s	65.1s
			This work	**12.0s**	0.18s	0	0.23s	12.4s
	14	4 096	usual	176s	**1 100s**	2 353	1.47s	1 280s
			This work	**57.0s**	0.74s	0	1.23s	59.0s
	15	8 192	usual	1 030s	$>$ **2 days**	4 853		$>$ 2 days
			This work	**348s**	3.47s	0	30.6s	382s
Edwards	5	65 536	usual	12 300s	$>$ **2 days**			$>$ 2 days
			This work	**12 300s**	40.8s	0	7 820s	20 200s
Edwards weights	5	65 536	usual	566s	15.1s	0	**2 150s**	2 730s
			This work	566s	15.1s	0	**2 150s**	2 730s
Pathological	9	512	usual	0s	**12.8s**	255	0.01s	12.8s
			This work	$<$ 0.01s	$<$ 0.01s	0	$<$ 0.01s	$<$ 0.01s
	11	2 048	usual	0s	**7 520s**	1 023	23.0s	7 540s
			This work	**5.02s**	0.15s	0	0.13s	5.28s
	16	65 536	usual	0s	$>$ **2 days**	32 767		$>$ 2 days
			This work	**38 100s**	195s	0	14 300s	52 600s

First conclusion

New probabilistic algorithm for solving PoSSo

- Complexity $\tilde{O}(d^{\omega n} + nD^{\omega})$ arithmetic operations
- Real impacts in practice intractable → 20k seconds

Deterministic computation of μ_{x_i}?

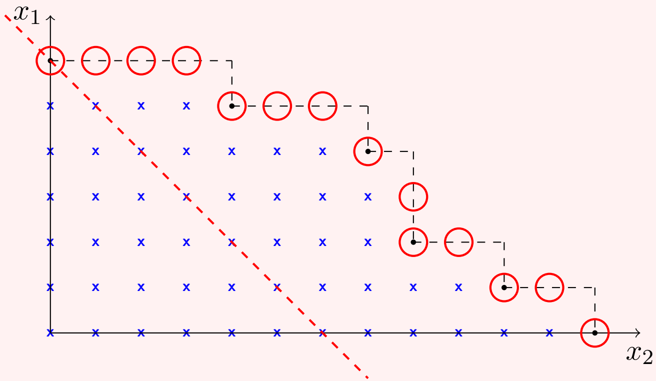


☞ All the NF of same degree terms are computed at the same time!

Computing $\mu_{x_1}, \ldots, \mu_{x_n}$

Computing $\mu_{x_1}, \ldots, \mu_{x_n}$ $\Leftrightarrow$ computing $\mathsf{NF}_{DRL}(\epsilon_i x_j)$ $i = 1, \ldots, D$ and $j =$

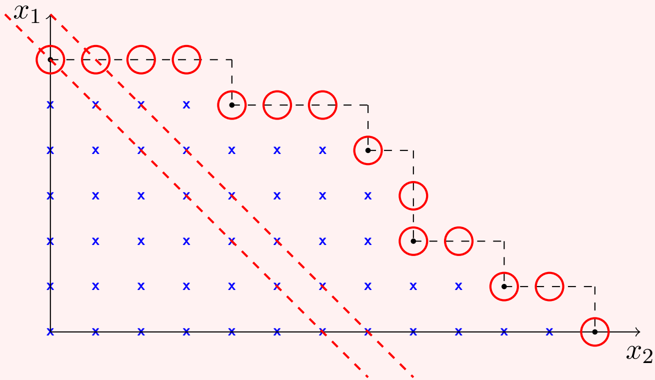
This work



Computing $\mu_{x_1}, \ldots, \mu_{x_n}$

Computing $\mu_{x_1}, \ldots, \mu_{x_n}$ $\Leftrightarrow$ computing $\mathsf{NF}_{DRL}(\epsilon_i x_j)$ $i = 1, \ldots, D$ and $j =$

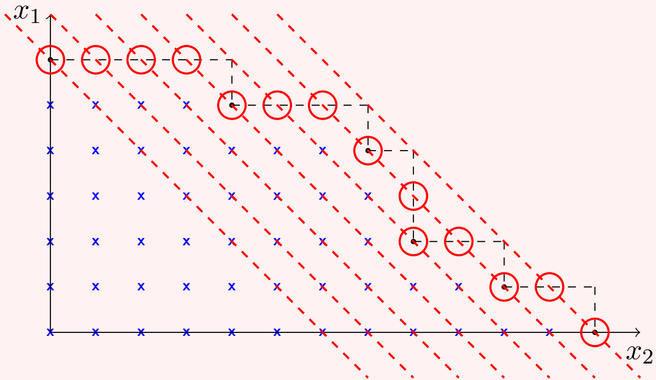
This work



Computing $\mu_{x_1}, \ldots, \mu_{x_n}$

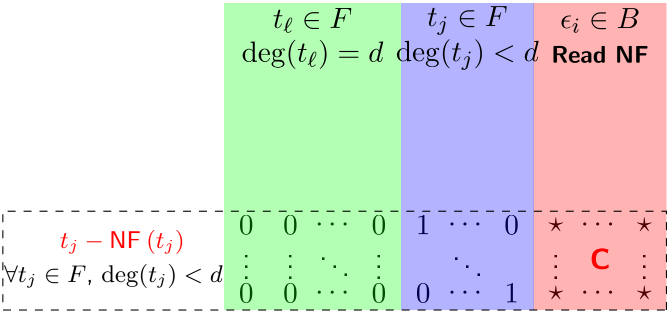
Computing $\mu_{x_1}, \ldots, \mu_{x_n}$ $\Leftrightarrow$ computing $\mathsf{NF}_{DRL}\left(\epsilon_i x_j\right)$ $i = 1, \ldots, D$ and $j =$

This work



Computing $\mu_{x_1}, \ldots, \mu_{x_n}$ using fast linear algebra

Iterative algorithm: loop on the **degree** d



Computing $\mu_{x_1}, \ldots, \mu_{x_n}$ using fast linear algebra

Iterative algorithm: loop on the **degree** d

	$t_\ell \in F$, $\deg(t_\ell) = d$				$t_j \in F$, $\deg(t_j) < d$			$\epsilon_i \in B$		
	1	$\star$	$\cdots$	$\star$	$\star$	$\cdots$	$\star$	$\star$	$\cdots$	$\star$
$f_\ell \in \mathcal{I}$, LT $(f_\ell) = t_\ell$	0	1		$\vdots$	$\star$	$\cdots$	$\star$	$\star$	$\cdots$	$\star$
$\forall t_\ell \in F$, $\deg(t_\ell) = d$	$\vdots$	**T**	$\ddots$	$\star$	$\vdots$	**A**	$\vdots$	$\vdots$	**B**	$\vdots$
	0	0	$\cdots$	1	$\star$	$\cdots$	$\star$	$\star$	$\cdots$	$\star$
	0	0	$\cdots$	0	1	$\cdots$	0	$\star$	$\cdots$	$\star$
$t_j -$ NF (t_j)	$\vdots$	$\vdots$	$\ddots$	$\vdots$		$\ddots$		$\vdots$	**C**	$\vdots$
$\forall t_j \in F$, $\deg(t_j) < d$	0	0	$\cdots$	0	0	$\cdots$	1	$\star$	$\cdots$	$\star$

- If $t_\ell \in E\,(>_1)\,\mathcal{I}$ then $f_\ell = g$ with $g \in \mathcal{G}_{>_1}$ st $\mathrm{LT}_{>_1}(g) = t_\ell$;
- Else $t_\ell \in F \setminus E\,(>_1)\,\mathcal{I} \Rightarrow t_\ell = x_k t_j$ and $f_\ell = x_k(t_j - \mathrm{NF}_{>_1}(t_j)) = t_\ell + \sum_{i=1}^{D} \alpha_i x_k \epsilon_i$.

Computing $\mu_{x_1}, \dots, \mu_{x_n}$ using fast linear algebra

Iterative algorithm: loop on the **degree** d

$t_\ell \in F$, $\deg(t_\ell) = d$	$t_j \in F$, $\deg(t_j) < d$	$\epsilon_i \in B$, **Read NF**

$$\left(\begin{array}{cccc|ccc|ccc}
1 & 0 & \cdots & 0 & 0 & \cdots & 0 & \star & \cdots & \star \\
0 & 1 & & \vdots & 0 & \cdots & 0 & \star & \cdots & \star \\
\vdots & & \ddots & 0 & \vdots & \ddots & \vdots & & \mathbf{T^{-1}(B - AC)} & \\
0 & 0 & \cdots & 1 & 0 & \cdots & 0 & \star & \cdots & \star \\
\hline
0 & 0 & \cdots & 0 & 1 & \cdots & 0 & \star & \cdots & \star \\
\vdots & \vdots & \ddots & \vdots & & \ddots & & \vdots & \mathbf{C} & \vdots \\
0 & 0 & \cdots & 0 & 0 & \cdots & 1 & \star & \cdots & \star
\end{array}\right)$$

Reduced Row Echelon Form $\rightsquigarrow$

$t_\ell -$ NF (t_ℓ)
$\forall t_\ell \in F$, $\deg(t_\ell) = d$

$t_j -$ NF (t_j)
$\forall t_j \in F$, $\deg(t_j) < d$

The normal forms of all the monomials of same degree can be computed simultaneously.

Computing $\mu_{x_1}, \ldots, \mu_{x_n}$ using fast linear algebra

Size of M at most $(nD \times (n+1)D)$.

Theorem

Given $\mathcal{G}_{DRL}$, the computation can be done in

$$O(d_{\max} n^{\omega} D^{\omega}) \text{ arithmetic operations}$$

where $d_{\max} = \max\{\deg(t) \mid t \in F\} = \max\{\deg(g) \mid g \in \mathcal{G}_{DRL}\}$.

Regular System

Let $S = \{f_1, \ldots, f_n\}$ with $\deg(f_i) \leq d$ and $(f_1, \ldots, f_n)$ is a regular sequence. For the DRL ordering

- Macaulay's bound $\Rightarrow d_{\max} \leq n(d-1)+1$;
- Bézout's bound $\Rightarrow D \leq d^n$.

d *fixed integer* $\Rightarrow O(d_{\max} n^{\omega} D^{\omega}) = O(n^{\omega+1} D^{\omega}) = O(\log_2(D)^{\omega+1} D^{\omega})$.

Final conclusion

- New probabilistic algo for solving PoSSo with omplexity $\tilde{O}(d^{\omega n} + nD^{\omega})$ arithmetic operations
- Sub-cubic deterministic algo for the computations of the μ_{x_i}'s $\rightsquigarrow$ triangular sets (see Louise's PhD, extended version)

Thank you!