Computing Generic Fibers of Polynomial Ideals Using FGLM and Hensel Lifting

Jérémy Berthomieu[2] and **Rafael Mohr[1,2]**

Journées Nationales de Calcul Formel 2024
06.03.2024

[1]RPTU Kaiserslautern-Landau [2]Sorbonne Université Paris

Introduction

What we are doing

$$\begin{cases} f_1(x_1, \ldots, x_n, \mathbf{z}) \\ \vdots \\ f_m(x_1, \ldots, x_n, \mathbf{z}) \end{cases}$$

polynomial system in $\mathbf{K}[x_1, \ldots, x_n, \mathbf{z}]$

$\mathbf{z} := \{z_1, \ldots, z_d\}, d = \dim$

projection to **z**-space dominant

What we are doing

Generic Fiber: Ideal $\langle f_1, \ldots, f_m \rangle$ in $\mathbf{K}(\mathbf{z})[\mathbf{x}]$

$$\begin{cases} f_1(x_1, \ldots, x_n, \mathbf{z}) \\ \vdots \\ f_m(x_1, \ldots, x_n, \mathbf{z}) \end{cases} \longrightarrow \begin{cases} h_1(x_1, x_2, \ldots, x_n, \mathbf{z}) \\ h_2(x_2, \ldots, x_n, \mathbf{z}) \\ \vdots \\ h_n(x_n, \mathbf{z}) \end{cases}$$

polynomial system in $\mathbf{K}[x_1, \ldots, x_n, \mathbf{z}]$

$\mathbf{z} := \{z_1, \ldots, z_d\}, d = \dim$

projection to $\mathbf{z}$-space dominant

reduced LEX Gröbner Basis

in $\mathbf{K}(\mathbf{z})[x_1, \ldots, x_n]$

What we are doing

Generic Fiber: Ideal $\langle f_1, \ldots, f_m \rangle$ in $\mathbf{K}(\mathbf{z})[\mathbf{x}]$

$$\begin{cases} f_1(x_1, \ldots, x_n, \mathbf{z}) \\ \vdots \\ f_m(x_1, \ldots, x_n, \mathbf{z}) \end{cases} \longrightarrow \begin{cases} h_1(x_1, x_2, \ldots, x_n, \mathbf{z}) \\ h_2(x_2, \ldots, x_n, \mathbf{z}) \\ \vdots \\ h_n(x_n, \mathbf{z}) \end{cases}$$

polynomial system in $\mathbf{K}[x_1, \ldots, x_n, \mathbf{z}]$

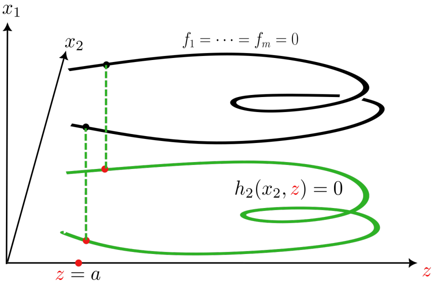
$\mathbf{z} := \{z_1, \ldots, z_d\}, d = \dim$

projection to $\mathbf{z}$-space dominant

reduced LEX Gröbner Basis

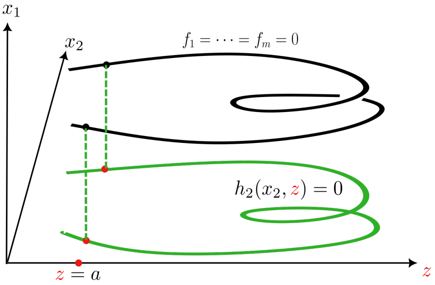
in $\mathbf{K}(\mathbf{z})[x_1, \ldots, x_n]$

classically: computed using elimination orderings



$$\begin{cases} h_1(x_1, x_2, z) = x_1 - g_1(x_2, z) \\ h_2(x_2, z) \end{cases}$$

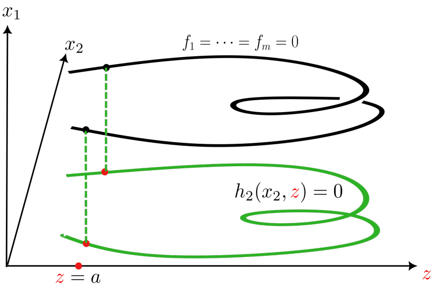
reduced LEX GB in $\mathbf{K}(z)[x_1, x_2]$



$$\begin{cases} h_1(x_1, x_2, z) = x_1 - g_1(x_2, z) \\ h_2(x_2, z) \end{cases}$$

reduced LEX GB in $\mathbf{K}(z)[x_1, x_2]$

Shape position: Solutions parametrized by a hypersurface.

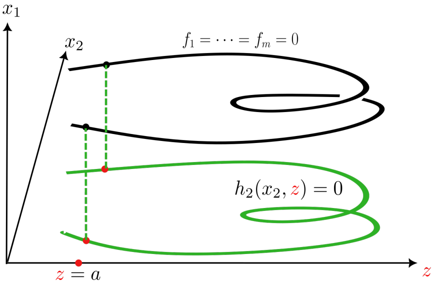


$$\begin{cases} h_1(x_1, x_2, z) = x_1 - g_1(x_2, z) \\ h_2(x_2, z) \end{cases}$$

reduced LEX GB in $\mathbf{K}(z)[x_1, x_2]$

Shape position: Solutions parametrized by a hypersurface.

Factors of $h_2 \Rightarrow$ Components of Curve!



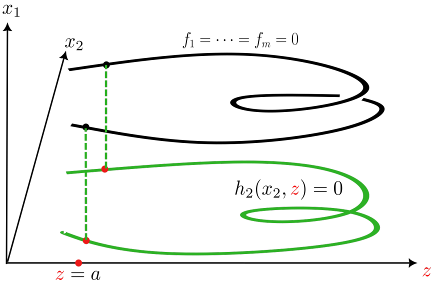
$$\begin{cases} h_1(x_1, x_2, z) = x_1 - g_1(x_2, z) \\ h_2(x_2, z) \end{cases}$$

reduced LEX GB in $\mathbf{K}(z)[x_1, x_2]$

Shape position: Solutions parametrized by a hypersurface.

Factors of $h_2 \Longrightarrow$ Components of Curve!

Rational Parametrization



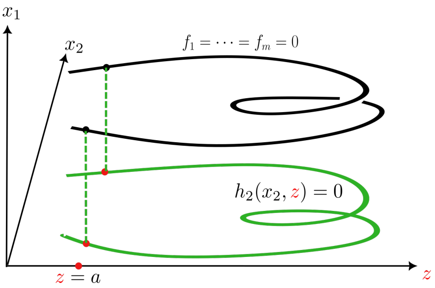
$$\begin{cases} h_1(x_1, x_2, z) = x_1 - g_1(x_2, z) \\ h_2(x_2, z) \end{cases}$$

reduced LEX GB in $\mathbf{K}(z)[x_1, x_2]$

Shape position: Solutions parametrized by a hypersurface.

Factors of $h_2 \implies$ Components of Curve!

Rational Parametrization — triangular sets e.g. (Hubert 03)



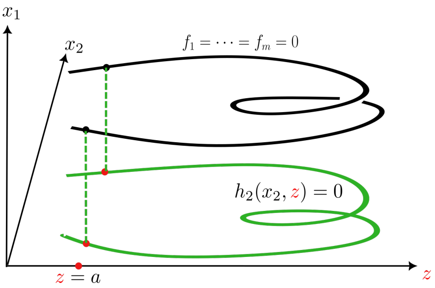
$$\begin{cases} h_1(x_1, x_2, z) = x_1 - g_1(x_2, z) \\ h_2(x_2, z) \end{cases}$$

reduced LEX GB in $\mathbf{K}(z)[x_1, x_2]$

Shape position: Solutions parametrized by a hypersurface.

Factors of $h_2 \Longrightarrow$ Components of Curve!

geometric resolutions e.g. (Giusti, Lecerf, Salvy 01) — **Rational Parametrization** — triangular sets e.g. (Hubert 03)



$$\begin{cases} h_1(x_1, x_2, z) = x_1 - g_1(x_2, z) \\ h_2(x_2, z) \end{cases}$$

reduced LEX GB in $\mathbf{K}(z)[x_1, x_2]$

Shape position: Solutions parametrized by a hypersurface.

Factors of h_2 $\Longrightarrow$ Components of Curve!

geometric resolutions e.g. (Giusti, Lecerf, Salvy 01)	Rational Parametrization	triangular sets e.g. (Hubert 03)

$$\begin{cases} h_n'(y,\mathbf{z})x_1 - g_1(y,\mathbf{z}) & = 0 \\ & \vdots \\ h_n'(y,\mathbf{z})x_n - g_n(y,\mathbf{z}) & = 0 \\ h_n(y,\mathbf{z}) & = 0 \end{cases}$$

geometric resolution

$y = \sum \alpha_i x_i$ **primitive element**

$h_n, g_i \in k(\mathbf{z})[T]$, h_n squarefree

$$\begin{cases} h_n'(y,\mathbf{z})x_1 - g_1(y,\mathbf{z}) & = 0 \\ & \vdots \\ h_n'(y,\mathbf{z})x_n - g_n(y,\mathbf{z}) & = 0 \\ h_n(y,\mathbf{z}) & = 0 \end{cases}$$

geometric resolution

$y = \sum \alpha_i x_i$ **primitive element**

$h_n, g_i \in k(\mathbf{z})[T]$, h_n squarefree

- e.g. (Lecerf 00), (Giusti, Lecerf, Salvy 01), (Lecerf 03), (Schost 03)

$$\begin{cases} h_n'(y,\mathbf{z})x_1 - g_1(y,\mathbf{z}) &= 0 \\ & \vdots \\ h_n'(y,\mathbf{z})x_n - g_n(y,\mathbf{z}) &= 0 \\ h_n(y,\mathbf{z}) &= 0 \end{cases}$$

geometric resolution

$y = \sum \alpha_i x_i$ **primitive element**

$h_n, g_i \in k(\mathbf{z})[T]$, h_n squarefree

- e.g. (Lecerf 00), (Giusti, Lecerf, Salvy 01), (Lecerf 03), (Schost 03)
- **complexity**: polynomial in some degree assoc. to system

$$
\begin{cases}
h_n'(y,\mathbf{z})x_1 - g_1(y,\mathbf{z}) & = 0 \\
 & \vdots \\
h_n'(y,\mathbf{z})x_n - g_n(y,\mathbf{z}) & = 0 \\
h_n(y,\mathbf{z}) & = 0
\end{cases}
$$

geometric resolution

$y = \sum \alpha_i x_i$ **primitive element**

$h_n, g_i \in k(\mathbf{z})[T]$, h_n squarefree

- e.g. (Lecerf 00), (Giusti, Lecerf, Salvy 01), (Lecerf 03), (Schost 03)
- **complexity**: polynomial in some degree assoc. to system
- encoded in **Noether position** except for (Schost 03)

$$\begin{cases} h_n'(y,\mathbf{z})x_1 - g_1(y,\mathbf{z}) & = 0 \\ & \vdots \\ h_n'(y,\mathbf{z})x_n - g_n(y,\mathbf{z}) & = 0 \\ h_n(y,\mathbf{z}) & = 0 \end{cases}$$

geometric resolution

$y = \sum \alpha_i x_i$ **primitive element**

$h_n, g_i \in k(\mathbf{z})[T]$, h_n squarefree

- e.g. (Lecerf 00), (Giusti, Lecerf, Salvy 01), (Lecerf 03), (Schost 03)
- **complexity**: polynomial in some degree assoc. to system
- encoded in **Noether position** except for (Schost 03)
- **Hensel lifting**: "imitates" Newton iteration

$$\begin{cases} h_n'(y,\mathbf{z})x_1 - g_1(y,\mathbf{z}) & = 0 \\ & \vdots \\ h_n'(y,\mathbf{z})x_n - g_n(y,\mathbf{z}) & = 0 \\ h_n(y,\mathbf{z}) & = 0 \end{cases}$$

geometric resolution

$y = \sum \alpha_i x_i$ **primitive element**

$h_n, g_i \in k(\mathbf{z})[T]$, h_n squarefree

- e.g. (Lecerf 00), (Giusti, Lecerf, Salvy 01), (Lecerf 03), (Schost 03)
- **complexity**: polynomial in some degree assoc. to system
- encoded in **Noether position** except for (Schost 03)
- **Hensel lifting**: "imitates" Newton iteration

Key Difference:

geometric vs. ideal-theoretic viewpoint

$$\begin{cases} h_n'(y,\mathbf{z})x_1 - g_1(y,\mathbf{z}) & = 0 \\ & \vdots \\ h_n'(y,\mathbf{z})x_n - g_n(y,\mathbf{z}) & = 0 \\ h_n(y,\mathbf{z}) & = 0 \end{cases}$$

geometric resolution

$y = \sum \alpha_i x_i$ **primitive element**

$h_n, g_i \in k(\mathbf{z})[T]$, h_n squarefree

- e.g. (Lecerf 00), (Giusti, Lecerf, Salvy 01), (Lecerf 03), (Schost 03)
- **complexity**: polynomial in some degree assoc. to system
- encoded in **Noether position** except for (Schost 03)
- **Hensel lifting**: "imitates" Newton iteration

Key Difference:

geometric vs. ideal-theoretic viewpoint

For example: Computing Generic Fibers

$\rightsquigarrow$ Primary Decomposition

$\rightsquigarrow$ Computation of Whitney stratifications as in (Helmer 23)

The Zero-dimensional Case

No parameters

no parameters, $dim = 0$, finitely many solutions

$$\begin{cases} f_1(x_1, \dots, x_n) \\ \vdots \\ f_m(x_1, \dots, x_n) \end{cases}$$

no parameters, *dim* $= 0$, finitely many solutions

(Buchberger 65)
(Faugère 99)
(Faugère 02)

$$\begin{cases} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_m(x_1, \ldots, x_n) \end{cases} \xrightarrow{\text{Buchberger, F4, F5}} \begin{cases} g_1(x_1, \ldots, x_n) \\ \vdots \\ g_r(x_1, \ldots, x_n) \end{cases}$$

DRL Gröbner Basis

in $\mathbf{K}[x_1, \ldots, x_n]$

no parameters, $dim = 0$, finitely many solutions

$$\begin{cases} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_m(x_1, \ldots, x_n) \end{cases} \xrightarrow{\text{Buchberger, F4, F5}} \begin{cases} g_1(x_1, \ldots, x_n) \\ \vdots \\ g_r(x_1, \ldots, x_n) \end{cases} \xrightarrow{\text{FGLM}} \begin{cases} h_1(x_1, x_2, \ldots, x_n) \\ h_2(x_2, \ldots, x_n) \\ \vdots \\ h_n(x_n) \end{cases}$$

Buchberger, F4, F5: (Buchberger 65) (Faugère 99) (Faugère 02)

FGLM: (Faugère, Gianni, Lazard, Mora 93) (Faugère, Mou 17) (Berthomieu, Neiger, Safey El Din 22) among others

DRL Gröbner Basis in $\mathbf{K}[x_1, \ldots, x_n]$

reduced LEX Gröbner Basis in $\mathbf{K}[x_1, \ldots, x_n]$

no parameters, *dim* = 0, finitely many solutions

(Faugère, Gianni, Lazard, Mora 93)
(Faugère, Mou 17)
(Berthomieu, Neiger, Safey El Din 22)
among others

(Buchberger 65)
(Faugère 99)
(Faugère 02)

$$\begin{cases} f_1(x_1,\dots,x_n) \\ \vdots \\ f_m(x_1,\dots,x_n) \end{cases} \xrightarrow{\text{Buchberger, F4, F5}} \begin{cases} g_1(x_1,\dots,x_n) \\ \vdots \\ g_r(x_1,\dots,x_n) \end{cases} \xrightarrow{\text{FGLM}} \begin{cases} h_1(x_1,x_2,\dots,x_n) \\ h_2(x_2,\dots,x_n) \\ \vdots \\ h_n(x_n) \end{cases}$$

DRL Gröbner Basis

in $\mathbf{K}[x_1,\dots,x_n]$

reduced LEX Gröbner Basis

in $\mathbf{K}[x_1,\dots,x_n]$

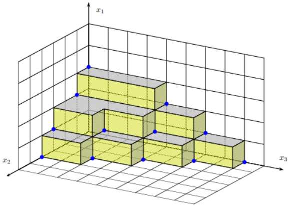
Triangular Structure ⟹ Solutions!

Define $I := \langle f_1, \ldots, f_m \rangle \subset \mathbf{K}[\mathbf{x}]$. Assume $\dim(I) = 0$, i.e. finitely many solutions. Recall:

$\dim(I) = 0 \Leftrightarrow \mathbf{K}[\mathbf{x}]/I$ finite dim. $\mathbf{K}$-vector space

Define $I := \langle f_1, \ldots, f_m \rangle \subset \mathbf{K}[\mathbf{x}]$. Assume $\dim(I) = 0$, i.e. finitely many solutions. Recall:

$\dim(I) = 0 \Leftrightarrow \mathbf{K}[\mathbf{x}]/I$ finite dim. $\mathbf{K}$-vector space

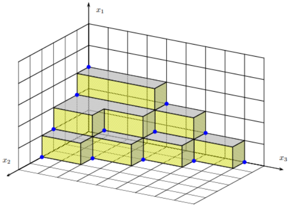


Staircase:
Monomial basis of $\mathbf{K}[\mathbf{x}]/I$.

Normal Form:
expression of any $f \in \mathbf{K}[\mathbf{x}]/I$ in staircase.

Define $I := \langle f_1, \dots, f_m \rangle \subset \mathbf{K}[\mathbf{x}]$. Assume $\dim(I) = 0$, i.e. finitely many solutions. Recall:

$\dim(I) = 0 \Leftrightarrow \mathbf{K}[\mathbf{x}]/I$ finite dim. $\mathbf{K}$-vector space



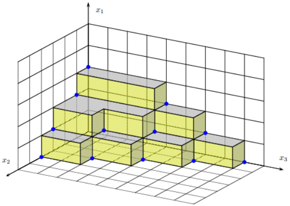
Staircase:
Monomial basis of $\mathbf{K}[\mathbf{x}]/I$.

Normal Form:
expression of any $f \in \mathbf{K}[\mathbf{x}]/I$ in staircase.

DRL GB

Define $I := \langle f_1, \ldots, f_m \rangle \subset \mathbf{K}[\mathbf{x}]$. Assume $\dim(I) = 0$, i.e. finitely many solutions. Recall:

$\dim(I) = 0 \Leftrightarrow \mathbf{K}[\mathbf{x}]/I$ finite dim. $\mathbf{K}$-vector space



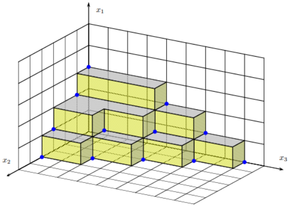
Staircase:
Monomial basis of $\mathbf{K}[\mathbf{x}]/I$.

Normal Form:
expression of any $f \in \mathbf{K}[\mathbf{x}]/I$ in staircase.

DRL GB → Staircase + NF's

Define $I := \langle f_1, \ldots, f_m \rangle \subset \mathbf{K}[\mathbf{x}]$. Assume $\dim(I) = 0$, i.e. finitely many solutions. Recall:

$$\dim(I) = 0 \Leftrightarrow \mathbf{K}[\mathbf{x}]/I \text{ finite dim. } \mathbf{K}\text{-vector space}$$



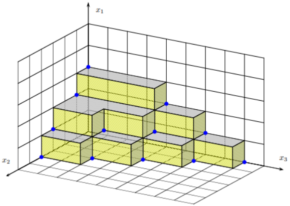
Staircase:
Monomial basis of $\mathbf{K}[\mathbf{x}]/I$.

Normal Form:
expression of any $f \in \mathbf{K}[\mathbf{x}]/I$ in staircase.

DRL GB → Staircase + NF's → linear relations between NF's

Define $I := \langle f_1, \dots, f_m \rangle \subset \mathbf{K}[\mathbf{x}]$. Assume $\dim(I) = 0$, i.e. finitely many solutions. Recall:

$\dim(I) = 0 \Leftrightarrow \mathbf{K}[\mathbf{x}]/I$ finite dim. $\mathbf{K}$-vector space



Staircase:
Monomial basis of $\mathbf{K}[\mathbf{x}]/I$.

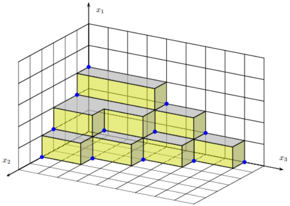
Normal Form:
expression of any $f \in \mathbf{K}[\mathbf{x}]/I$ in staircase.

DRL GB → Staircase + NF's → linear relations between NF's

FGLM: use this mechanism to get LEX GB!

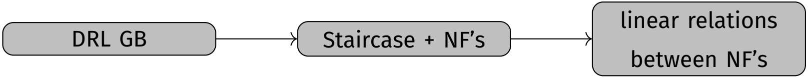
Define $I := \langle f_1, \ldots, f_m \rangle \subset \mathbf{K}[\mathbf{x}]$. Assume $\dim(I) = 0$, i.e. finitely many solutions. Recall:

$\dim(I) = 0 \Leftrightarrow \mathbf{K}[\mathbf{x}]/I$ finite dim. $\mathbf{K}$-vector space



Staircase:
Monomial basis of $\mathbf{K}[\mathbf{x}]/I$.

Normal Form:
expression of any $f \in \mathbf{K}[\mathbf{x}]/I$ in staircase.



FGLM: use this mechanism to get LEX GB!

for example: $h_n(x_n) \sim$ linear relation between NF's of x_n^k, $k = 0, 1, \ldots$

Our Algorithm

(Case $\mathbf{z} = \{z\}$)

with a parameter, $dim = 1$

$$\begin{cases} f_1(x_1, \dots, x_n, z) \\ \vdots \\ f_m(x_1, \dots, x_n, z) \end{cases}$$

with a parameter, $dim = 1$

$$\begin{cases} f_1(x_1, \ldots, x_n, z) \\ \vdots \\ f_m(x_1, \ldots, x_n, z) \end{cases} \xrightarrow{\text{Buchberger, F4, F5}} \begin{cases} g_1(x_1, \ldots, x_n, z) \\ \vdots \\ g_r(x_1, \ldots, x_n, z) \end{cases}$$

(Buchberger 65)
(Faugère 99)
(Faugère 02)

DRL Gröbner Basis

in $\mathbf{K}[x_1, \ldots, x_n, z]$

with a parameter, $dim = 1$

$$\begin{cases} f_1(x_1, \ldots, x_n, z) \\ \vdots \\ f_m(x_1, \ldots, x_n, z) \end{cases}$$

(Buchberger 65)
(Faugère 99)
(Faugère 02)

Buchberger, F4, F5 $\longrightarrow$

$$\begin{cases} g_1(x_1, \ldots, x_n, z) \\ \vdots \\ g_r(x_1, \ldots, x_n, z) \end{cases}$$

DRL Gröbner Basis

in $\mathbf{K}[x_1, \ldots, x_n, z]$

this work $\longrightarrow$

$$\begin{cases} h_1(x_1, x_2, \ldots, x_n, z) \\ h_2(x_2, \ldots, x_n, z) \\ \vdots \\ h_n(x_n, z) \end{cases}$$

reduced LEX Gröbner Basis

in $\mathbf{K}(z)[x_1, \ldots, x_n]$

with a parameter, $dim = 1$

$$\begin{cases} f_1(x_1,\ldots,x_n,z) \\ \vdots \\ f_m(x_1,\ldots,x_n,z) \end{cases} \xrightarrow{\text{Buchberger, F4, F5}} \begin{cases} g_1(x_1,\ldots,x_n,z) \\ \vdots \\ g_r(x_1,\ldots,x_n,z) \end{cases} \xrightarrow{\text{this work}} \begin{cases} h_1(x_1,x_2,\ldots,x_n,z) \\ h_2(x_2,\ldots,x_n,z) \\ \vdots \\ h_n(x_n,z) \end{cases}$$

(Buchberger 65)
(Faugère 99)
(Faugère 02)

DRL Gröbner Basis in $\mathbf{K}[x_1,\ldots,x_n,z]$

reduced LEX Gröbner Basis in $\mathbf{K}(z)[x_1,\ldots,x_n]$

Strategy: FGLM + Hensel Lifting

with a parameter, $dim = 1$

(Buchberger 65)
(Faugère 99)
(Faugère 02)

$$\begin{cases} f_1(x_1, \ldots, x_n, z) \\ \vdots \\ f_m(x_1, \ldots, x_n, z) \end{cases} \xrightarrow{\text{Buchberger, F4, F5}} \begin{cases} g_1(x_1, \ldots, x_n, z) \\ \vdots \\ g_r(x_1, \ldots, x_n, z) \end{cases} \xrightarrow{\text{this work}} \begin{cases} h_1(x_1, x_2, \ldots, x_n, z) \\ h_2(x_2, \ldots, x_n, z) \\ \vdots \\ h_n(x_n, z) \end{cases}$$

DRL Gröbner Basis

in $\mathbf{K}[x_1, \ldots, x_n, z]$

reduced LEX Gröbner Basis

in $\mathbf{K}(z)[x_1, \ldots, x_n]$

Strategy: FGLM + Hensel Lifting

(Pauer 92), (arnold 03), (Winkler 88), (Schost, St-Pierre 23)

1

Choose random $z = a$

$\Downarrow$

0-dim. system $f_1, \ldots, f_m = 0, z - a = 0$

1

Choose random $z = a$

$\Downarrow$

0-dim. system $f_1, \ldots, f_m = 0, z - a = 0$

$\longrightarrow$ using DRL GB

2

Run FGLM to obtain

$$\begin{cases} h_1(x_1, x_2, \ldots, x_{n-1}, a) \\ h_2(x_2, \ldots, x_{n-1}, a) \\ \vdots \\ h_c(x_{n-1}, a) \end{cases}$$

1

Choose random $z = a$

$\Downarrow$

0-dim. system $f_1, \ldots, f_m = 0, z - a = 0$

using DRL GB

2

Run FGLM to obtain

$$\begin{cases} h_1(x_1, x_2, \ldots, x_{n-1}, a) \\ h_2(x_2, \ldots, x_{n-1}, a) \\ \vdots \\ h_c(x_{n-1}, a) \end{cases}$$

using "FGLM mechanism" with DRL GB of

$\langle f_1, \ldots, f_m, (z - a)^2 \rangle$

3

Lifting step:

Lift modulo $f_1, \ldots, f_m, (z - a)^2$

by finding relations in staircase of

$\langle f_1, \ldots, f_m, (z - a)^2 \rangle$.

$\Downarrow$

$h_1, \ldots, h_c \mod (z - a)^2$

1

Choose random $z = a$

$\Downarrow$

0-dim. system $f_1, \ldots, f_m = 0, z - a = 0$

using DRL GB

2

Run FGLM to obtain

$$\begin{cases} h_1(x_1, x_2, \ldots, x_{n-1}, a) \\ h_2(x_2, \ldots, x_{n-1}, a) \\ \vdots \\ h_c(x_{n-1}, a) \end{cases}$$

using "FGLM mechanism" with DRL GB of

$\langle f_1, \ldots, f_m, (z - a)^2 \rangle$

3

Lifting step:

Lift modulo $f_1, \ldots, f_m, (z - a)^2$

by finding relations in staircase of

$\langle f_1, \ldots, f_m, (z - a)^2 \rangle$.

$\Downarrow$

$h_1, \ldots, h_c \mod (z - a)^2$

further lifts

4

Probabilistic termination using Padé approximation

$\Downarrow$

$h_1, \ldots, h_c$

Theorem

(Faugère, Gianni, Lazard, Mora 93):

dim 0, degree D system in $\mathbf{K}[x_1, \ldots, x_n]$

$$\text{DRL GB} \xrightarrow{O(nD^3) \text{ arit. ops.}} \text{LEX GB}$$

Theorem

(Faugère, Gianni, Lazard, Mora 93):

dim 0, degree D system in $\mathbf{K}[x_1, \dots, x_n]$

DRL GB $\xrightarrow{O(nD^3) \text{ arit. ops.}}$ LEX GB

Theorem

(Berthomieu, M. 24):

generic system $f_1, \dots, f_n$ of degree D in $\mathbf{K}[x_1, \dots, x_n, z]$

LEX GB of gen. fiber in $\mathbf{K}(z)[x_1, \dots, x_n]$

δ = degree of rational fraction coefficients

DRL GB $\xrightarrow[\text{using quadratic lifting}]{\tilde{O}(\delta(n-1)D^3) \text{ arit. ops.}}$ LEX GB of gen. fiber to precision δ

Given: DRL GB for $f_1, \ldots, f_m$.

Need (for lifting steps): DRL GB's for $f_1, \ldots, f_m, z - a$ and $f_1, \ldots, f_m, (z-a)^2$...

Given: DRL GB for $f_1, \ldots, f_m$.

Need (for lifting steps): DRL GB's for $f_1, \ldots, f_m, z - a$ and $f_1, \ldots, f_m, (z - a)^2$...

$n = m, f_1, \ldots, f_n$ generic $\Longrightarrow$ this step is free!

Given: DRL GB for $f_1, \ldots, f_m$.

Need (for lifting steps): DRL GB's for $f_1, \ldots, f_m, z - a$ and $f_1, \ldots, f_m, (z-a)^2$...

$n = m, f_1, \ldots, f_n$ generic $\Rightarrow$ this step is free!

$\Uparrow$

staircase for $f_1, \ldots, f_n, (z-a)^k$ = "truncated" staircase of $f_1, \ldots, f_n$

Given: DRL GB for $f_1, \ldots, f_m$.

Need (for lifting steps): DRL GB's for $f_1, \ldots, f_m, z - a$ and $f_1, \ldots, f_m, (z-a)^2$...

$n = m, f_1, \ldots, f_n$ generic $\Rightarrow$ this step is free!

$\Uparrow$

staircase for $f_1, \ldots, f_n, (z-a)^k$ = "truncated" staircase of $f_1, \ldots, f_n$

$\Downarrow$

lifting step: linear algebra with low displacement rank

(Bostan, Jeannerod, Mouilleron, Schost 17)

Given: DRL GB for $f_1, \ldots, f_m$.

Need (for lifting steps): DRL GB's for $f_1, \ldots, f_m, z - a$ and $f_1, \ldots, f_m, (z - a)^2$...

$n = m, f_1, \ldots, f_n$ generic $\Rightarrow$ this step is free!

$\Uparrow$

staircase for $f_1, \ldots, f_n, (z - a)^k$ = "truncated" staircase of $f_1, \ldots, f_n$

$\Downarrow$

lifting step: linear algebra with low displacement rank

(Bostan, Jeannerod, Mouilleron, Schost 17)

But: In more general case, needed DRL GB's are *highly non-free*, no nice staircase structure...

Incorporating Tracers

(Traverso 89)

Recall: We needed GB's for $f_1, \ldots, f_m, z - a$ and $f_1, \ldots, f_m, (z-a)^2$...

$f_1, \ldots, f_m$

↓ F4 (Faugère 99)

Tracer: Build and echolonize a series of matrices

"Learn" tracer T ← DRL GB over $\mathbf{K}[z]/(z-a) \cong \mathbf{K}$

$f_1, \ldots, f_m$

F4 (Faugère 99)

Tracer: Build and echolonize a series of matrices

DRL GB over $\mathbf{K}[z]/(z-a) \cong \mathbf{K}$ → "Learn" tracer T

apply T, lift LU-factorizations | arithmetic only in $\mathbf{K}$!

"DRL GB" over $\mathbf{K}[z]/(z-a)^2$

$f_1, \ldots, f_m$

F4 (FAUGÈRE 99)

Tracer: Build and echolonize a series of matrices

"Learn" tracer T ← DRL GB over $\mathbf{K}[z]/(z-a) \cong \mathbf{K}$

apply T, lift LU-factorizations | arithmetic only in $\mathbf{K}$!

"DRL GB" over $\mathbf{K}[z]/(z-a)^2$

apply T, lift LU-factorizations | arithmetic only in $\mathbf{K}$!

"DRL GB" over $\mathbf{K}[z]/(z-a)^3$

...

$f_1, \ldots, f_m$

F4 (Faugère 99)

Tracer: Build and echolonize a series of matrices

"Learn" tracer T ⟵ DRL GB over $\mathbf{K}[z]/(z-a) \cong \mathbf{K} \xrightarrow{\text{as before}} h_1, \ldots, h_c \mod (z-a)$

apply T, lift LU-factorizations | arithmetic only in $\mathbf{K}$!

"DRL GB" over $\mathbf{K}[z]/(z-a)^2 \longrightarrow h_1, \ldots, h_c \mod (z-a)^2$

apply T, lift LU-factorizations | arithmetic only in $\mathbf{K}$!

"DRL GB" over $\mathbf{K}[z]/(z-a)^3 \longrightarrow h_1, \ldots, h_c \mod (z-a)^3$

... ...

$f_1, \ldots, f_m$

F4 (FAUGÈRE 99)

Tracer: Build and echolonize a series of matrices

"Learn" tracer T ⟵ DRL GB over $\mathbf{K}[z]/(z-a) \cong \mathbf{K} \xrightarrow{\text{as before}} h_1, \ldots, h_c \mod (z-a)$

apply T, lift LU-factorizations | arithmetic only in $\mathbf{K}$!

"DRL GB" over $\mathbf{K}[z]/(z-a)^2 \longrightarrow h_1, \ldots, h_c \mod (z-a)^2$

apply T, lift LU-factorizations | arithmetic only in $\mathbf{K}$!

"DRL GB" over $\mathbf{K}[z]/(z-a)^3 \longrightarrow h_1, \ldots, h_c \mod (z-a)^3$

... ...

Same complexity for lifting $h_1, \ldots, h_c$!

Some Preliminary Experiments & Perspectives

Polynomial System	Our Algorithm Timing (in s)	`msolve`[1], using elim. orders Timing (in s)
ED(3,3)	121.34	–
M2	152.81	6.54
M3	3.11	–
PS(2,10)	5.56	1251.94
PS(2,12)	120.10	–
Sing(2,10)	3.04	4.25
SOS(6,4)	114.88	11366.36
SOS(6,5)	120.1	–
RD(3)	3.31	0.11
RD(4)	9.77	28.72
RD(5)	385.31	2277.56

[1](Berthomieu, Eder, Safey El Din 21)

Polynomial System	Our Algorithm Timing (in s)	msolve[1], using elim. orders Timing (in s)
ED(3,3)	121.34	–
M2	152.81	6.54
M3	3.11	–
PS(2,10)	5.56	1251.94
PS(2,12)	120.10	–
Sing(2,10)	3.04	4.25
SOS(6,4)	114.88	11366.36
SOS(6,5)	120.1	–
RD(3)	3.31	0.11
RD(4)	9.77	28.72
RD(5)	385.31	2277.56

computes just hypersurface equation

[1](Berthomieu, Eder, Safey El Din 21)

Polynomial System	Our Algorithm Timing (in s)	`msolve`[1], using elim. orders Timing (in s)
ED(3,3)	121.34	–
M2	152.81	6.54
M3	3.11	–
PS(2,10)	5.56	1251.94
PS(2,12)	120.10	–
Sing(2,10)	3.04	4.25
SOS(6,4)	114.88	11366.36
SOS(6,5)	120.1	–
RD(3)	3.31	0.11
RD(4)	9.77	28.72
RD(5)	385.31	2277.56

computes just hypersurface equation

naive implementation without tracers and structured linear algebra!

[1](Berthomieu, Eder, Safey El Din 21)

Polynomial System	Our Algorithm Timing (in s)	`msolve`[1], using elim. orders Timing (in s)
ED(3,3)	121.34	–
M2	152.81	6.54
M3	3.11	–
PS(2,10)	5.56	1251.94
PS(2,12)	120.10	–
Sing(2,10)	3.04	4.25
SOS(6,4)	114.88	11366.36
SOS(6,5)	120.1	–
RD(3)	3.31	0.11
RD(4)	9.77	28.72
RD(5)	385.31	2277.56

computes just hypersurface equation

naive implementation without tracers and structured linear algebra!

[1](Berthomieu, Eder, Safey El Din 21)

Polynomial System	Our Algorithm Timing (in s)	msolve[1], using elim. orders Timing (in s)
ED(3,3)	121.34	–
M2	152.81	6.54
M3	3.11	–
PS(2,10)	5.56	1251.94
PS(2,12)	120.10	–
Sing(2,10)	3.04	4.25
SOS(6,4)	114.88	11366.36
SOS(6,5)	120.1	–
RD(3)	3.31	0.11
RD(4)	9.77	28.72
RD(5)	385.31	2277.56

computes just hypersurface equation

naive implementation without tracers and structured linear algebra!

[1](Berthomieu, Eder, Safey El Din 21)

Perspectives:

Perspectives:

- Investigate probability of success, maximal number of lifting steps? (Schost 03)

Perspectives:

- Investigate probability of success, maximal number of lifting steps? (Schost 03)
- Specialized variants of FGLM (Faugère, Mou 17), (Neiger, Schost 20), (Berthomieu, Neiger, Safey El Din 22)...

Perspectives:

- Investigate probability of success, maximal number of lifting steps? (Schost 03)
- Specialized variants of FGLM (Faugère, Mou 17), (Neiger, Schost 20), (Berthomieu, Neiger, Safey El Din 22)...
- Computing generic fibers of colon ideals following (Berthomieu, Eder, Safey El Din 23)

Perspectives:

- Investigate probability of success, maximal number of lifting steps? (Schost 03)
- Specialized variants of FGLM (Faugère, Mou 17), (Neiger, Schost 20), (Berthomieu, Neiger, Safey El Din 22)...
- Computing generic fibers of colon ideals following (Berthomieu, Eder, Safey El Din 23)
- Implementation in `msolve` (with tracers and structured linear algebra)!

Perspectives:

- Investigate probability of success, maximal number of lifting steps? (Schost 03)
- Specialized variants of FGLM (Faugère, Mou 17), (Neiger, Schost 20), (Berthomieu, Neiger, Safey El Din 22)...
- Computing generic fibers of colon ideals following (Berthomieu, Eder, Safey El Din 23)
- Implementation in `msolve` (with tracers and structured linear algebra)!

Thank you!