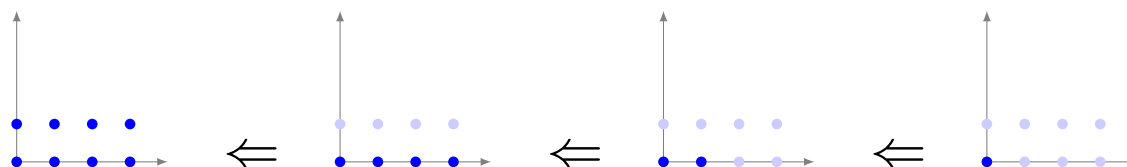


Computation of syzygies via multivariate matrix multiplication



Simone Naldi (joint with Vincent Neiger)

Applications of Computer Algebra – July 2021



General context

$R = K[X_1, \dots, X_r]$ the ring of *multivariate* polynomials over K

Given an R -submodule $\mathcal{M} \subset R^n$

Given elements $\mathbf{f}_1, \dots, \mathbf{f}_m \in R^n / \mathcal{M}$

Find *syzygies* for $\mathbf{F} = (\mathbf{f}_1, \dots, \mathbf{f}_m)$, i.e. $(p_1, \dots, p_m) \in R^m$ s.t.

$$\mathbf{pF} = p_1 \mathbf{f}_1 + \dots + p_m \mathbf{f}_m = 0 \quad (\text{in } R^n / \mathcal{M})$$

$$\text{Syz}_{\mathcal{M}}(\mathbf{F}) = \{\mathbf{p} \in R^m : \mathbf{pF} \in \mathcal{M}\}$$

$\dim_K(R^m / \mathcal{M}) = D \Rightarrow \dim_K(R^m / \text{Syz}_{\mathcal{M}}(\mathbf{F})) \leq D$: the *codimension* of the output module is controlled by the *codimension* of the input one

Hermite-Padé approximation \Rightarrow syzygies

$R = K[X]$ the ring of *univariate* polynomials over a field K

Given $f \in R/\langle X^d \rangle$, find $p_1, p_2 \in R$ such that

$$f = \frac{p_2}{p_1} \pmod{X^d} \quad (\iff p_1 f + p_2(-1) = 0)$$

More generally, given $f_1, \dots, f_m \in R/\langle X^d \rangle$, find $p_1, \dots, p_m \in R$

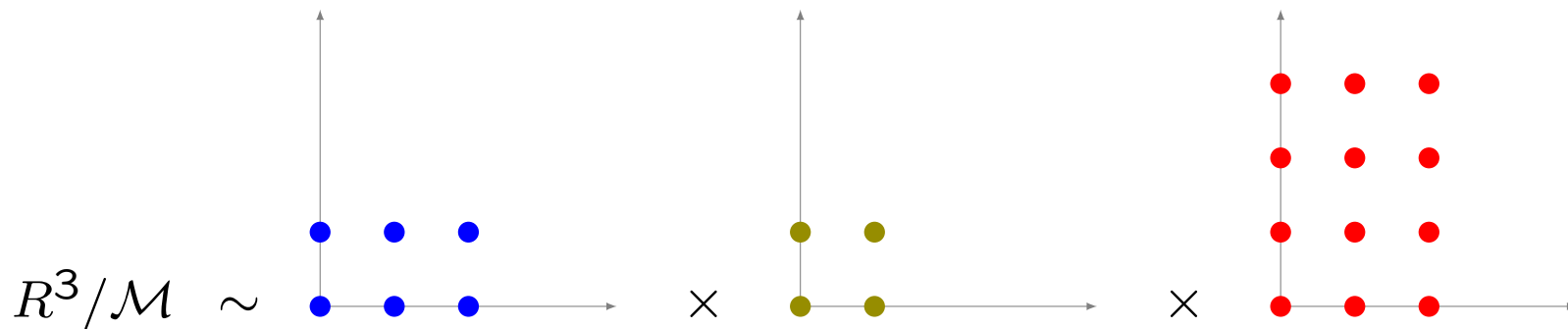
such that $(p_1, \dots, p_m) \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} = 0 \pmod{X^d}$

$(p_1, \dots, p_m) \in R^m$ is also called an *approximant* for (f_1, \dots, f_m)

Example: bivariate Hermite-Padé

$\mathcal{M} = I_1 \times \cdots \times I_n$ where each ideal I_i is a “box”

$$\mathcal{M} = \langle X^3, Y^2 \rangle \times \langle X^2, Y^2 \rangle \times \langle X^3, Y^4 \rangle$$



$$D = 6 + 4 + 12$$

$$p_1 \begin{bmatrix} f_{11} \\ f_{12} \\ f_{13} \end{bmatrix} + p_2 \begin{bmatrix} f_{21} \\ f_{22} \\ f_{23} \end{bmatrix} + \cdots + p_m \begin{bmatrix} f_{m1} \\ f_{m2} \\ f_{m3} \end{bmatrix} = 0 \pmod{\begin{matrix} \langle X^3, Y^2 \rangle \\ \langle X^2, Y^2 \rangle \\ \langle X^3, Y^4 \rangle \end{matrix}}$$

Problem and contribution

Input:

- an R -module $\mathcal{M} \subset R^n$
- elements $F = (f_1, \dots, f_m) \in R^n / \mathcal{M}$
- a monomial order \preceq on R^m

Output: the \preceq -Gröbner basis of $\text{Syz}_{\mathcal{M}}(F)$

Assumption: $D := \dim_K(R^n / \mathcal{M}) < +\infty$

- general divide and conquer approach

Marinari-Möller-Mora '93 + Beckermann-Labahn '94

- relying on multiplication of Gröbner bases

via multiplication of multivariate polynomial matrices

- Multivariate Hermite-Padé: improved complexity

$O^{\sim}(m^{\omega}d^{\omega+2})$ where $\mathcal{M} = \langle X^d, Y^d \rangle$ (previous: $O^{\sim}(md^{2\omega-2} + d^{2\omega})$)

Input representation

Following a viewpoint pioneered by Marinari-Möller-Mora (MMM) we assume that the input has a dual representation:

there are K -linear functionals $\varphi_j : R^n \rightarrow K$, $j = 1, \dots, D$ s.t.

$\mathcal{M}_i = \ker(\varphi_1) \cap \dots \cap \ker(\varphi_i)$ is an R -module for all i

and $\mathcal{M} = \mathcal{M}_D$

Based on this representation, an iterative algorithm is described in MMM 1993 (generalizing Möller-Buchberger and FGLM)

We interpret this algorithm with **polynomial matrix operations** (products of Gröbner bases)

~> allows us to design a **divide-and-conquer** strategy.

Elementary Gröbner bases (EGB)

Ideal case ($n = 1$). If $\dim_K(R/I) = 1$ then

$$I = \langle X_1 - \alpha_1, \dots, X_r - \alpha_r \rangle \text{ for some } \alpha$$

$$\{X_1 - \alpha_1, \dots, X_r - \alpha_r\} \text{ is a GB of } I.$$

Module case ($n \geq 1$). For $\pi \leq m$ and vectors $\lambda_1, \lambda_2, \alpha$, define:

$$\mathbf{E} = \begin{bmatrix} \mathbf{I}_{\pi-1} & \lambda_1 & & \\ & \mathbf{X} - \alpha & & \\ & \lambda_2 & & \\ & & \mathbf{I}_{m-\pi} & \end{bmatrix} \in R^{(m+r-1) \times m} \quad (1)$$

Theorem. (GB of codimension 1 submodules)

- If $\dim_K(R^m/\mathcal{M}) = 1$, for every \preccurlyeq the \preccurlyeq -reduced GB of \mathcal{M} has the form (1), with $\lambda_i = 0$ if $e_i \prec e_\pi$ for all $i \neq \pi$.
- ◀ For \mathbf{E} as in (1), $\mathcal{M} = \langle \mathbf{E} \rangle$ is such that $\dim_K(R^m/\mathcal{M}) = 1$, and \mathbf{E} is a reduced \preccurlyeq -GB for any \preccurlyeq such that $\lambda_i = 0$ if $e_i \prec e_\pi$ for all $i \neq \pi$.

Example of EGB

The matrix

$$\mathbf{E} = \begin{bmatrix} X & 0 \\ Y & 0 \\ 1 & 1 \end{bmatrix} \in K[X, Y]^{3 \times 2}$$

is an $\preceq_{\text{lex}}^{\text{top}}$ -elementary Gröbner basis of

$$\text{Syz}_{\langle X, Y \rangle} \left(\begin{bmatrix} 1 \\ -1 \end{bmatrix} \right) = \{ (p_1, p_2) \in K[X, Y]^2 \mid p_1 - p_2 \in \langle X, Y \rangle \}$$

In this case: $\pi = 1$, $\alpha = (0, 0) \in K^2$, $\lambda_2 = 1$ and $m = 2$.

Multiplication by EGB

Let $\mathbf{P} \in R^{k \times m}$ be a \preccurlyeq -Gröbner basis (of $\langle \mathbf{P} \rangle$) and let \mathbf{E} be an elementary Gröbner basis of the good size.

Question: *Under which assumption (and with respect to what order) is \mathbf{EP} again a Gröbner basis?*

Theorem. If:

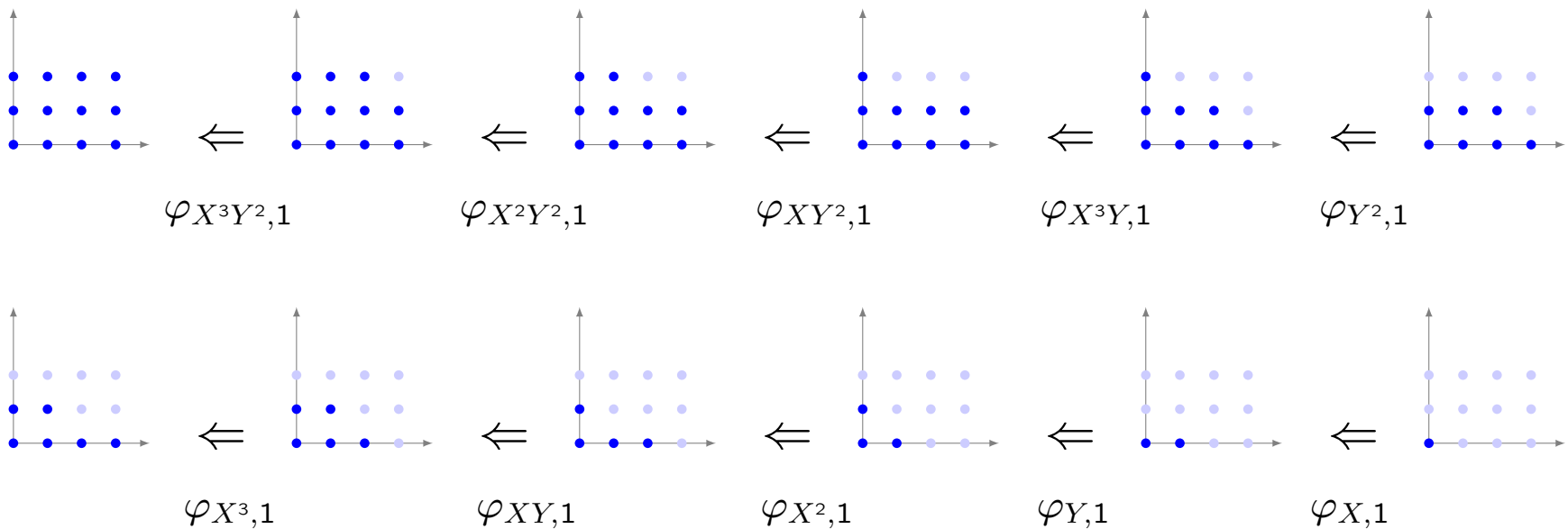
- \preccurlyeq_L well-chosen order dep. on \preccurlyeq , $L = (\mu_1, \dots, \mu_k) = \text{Im}_{\preccurlyeq}(\mathbf{P})$
- \mathbf{E} is reduced \preccurlyeq_L -Gröbner basis
- $\mu_i \neq \mu_\pi$ for all $i \neq \pi$ // π is fixed by \mathbf{E}
- $\langle \mathbf{EP} \rangle \neq \langle \mathbf{P} \rangle$

then \mathbf{EP} is a \preccurlyeq -Gröbner basis.

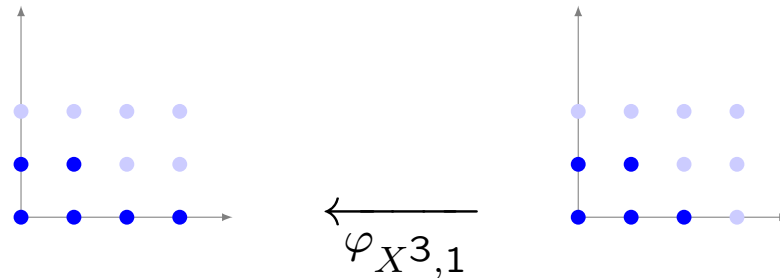
Multivariate Padé approximation

- $\mathcal{M} = \langle X_1^{d_{11}}, \dots, X_r^{d_{1r}} \rangle \times \dots \times \langle X_1^{d_{n1}}, \dots, X_r^{d_{nr}} \rangle \subseteq \mathbb{R}^n$
- The functionals are $\varphi_{\mu,i}(\cdot) = \text{coeff}(\cdot, \mu e_i)$

Here's the picture for $n = 1$ and $\mathcal{M} = \langle X^4, Y^3 \rangle$



A one-step algorithm



We first describe the typical situation where

$\mathcal{M} \subset R^n$ is a given R – module

$F \in R^{m \times n}$ is given with rows in R^n / \mathcal{M}

$\varphi : R^n \rightarrow K$ linear, such that $\ker(\varphi) \cap \mathcal{M}$ is module

we know a Gröbner basis \mathbf{P} of $\langle \mathbf{P} \rangle = \text{Syz}_{\mathcal{M}}(F)$

Goal : compute a GB of $\text{Syz}_{\ker(\varphi) \cap \mathcal{M}}(F)$

“Correctness” of one-step algorithm

Recap of assumptions

\mathcal{M} and $\ker(\varphi) \cap \mathcal{M}$ are modules

$\mathbf{P} \in R^{k \times m}$ minimal \preccurlyeq -Gröbner basis of $\text{Syz}_{\mathcal{M}}(\mathbf{F})$

Theorem. Assume that the input of the algorithm is such that

$\mathbf{G} = \mathbf{P}\mathbf{F}$, and

$(\mu_1, \dots, \mu_k) = \text{Im}_{\preccurlyeq}(\mathbf{P})$.

Then the output (\mathbf{Q}, L) is such that $\mathbf{Q}\mathbf{P}$ is a minimal \preccurlyeq -Gröbner basis of $\text{Syz}_{\ker(\varphi) \cap \mathcal{M}}(\mathbf{F})$ and $L = \text{Im}_{\preccurlyeq}(\mathbf{Q}\mathbf{P})$.

The output matrix \mathbf{Q}

It is a submatrix of an elementary Gröbner basis, precisely:

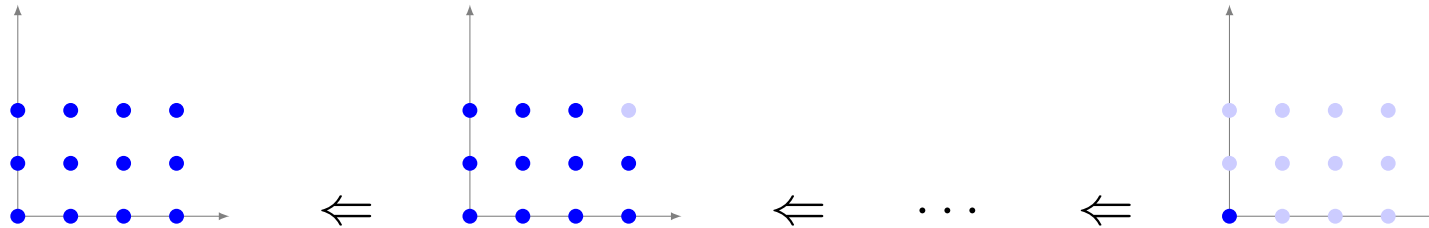
$$R^{(k+\ell-1) \times k} \ni \mathbf{Q} = \left[\begin{array}{ccc} \mathbf{I}_{\pi-1} & \lambda_1 & \\ & X_{j_1} - \alpha_{j_1} & \\ & \vdots & \\ & X_{j_\ell} - \alpha_{j_\ell} & \\ & \lambda_2 & \mathbf{I}_{m-\pi} \end{array} \right] \left. \vphantom{\begin{array}{ccc} \mathbf{I}_{\pi-1} & \lambda_1 & \\ & X_{j_1} - \alpha_{j_1} & \\ & \vdots & \\ & X_{j_\ell} - \alpha_{j_\ell} & \\ & \lambda_2 & \mathbf{I}_{m-\pi} \end{array}} \right\} \begin{array}{l} \text{some rows of EGB} \\ \text{have been deleted} \end{array}$$

Theorem. Assume that $\langle \mathbf{EP} \rangle \neq \langle \mathbf{P} \rangle$ and that \mathbf{P} is a minimal \preceq -Gröbner basis. Let $j_1 < \dots < j_\ell$ be the indices $j \in \{1, \dots, r\}$ such that

$$X_j \mu_\pi \notin \langle \mu_i, i \neq \pi \rangle.$$

Then the above matrix \mathbf{Q} (submatrix of \mathbf{E}) is such that \mathbf{QP} is a minimal \preceq -Gröbner basis of $\langle \mathbf{EP} \rangle$.

Sequential algorithm



The base case described above can be iterated as follows:

Input: functionals $\varphi_1, \dots, \varphi_D$, matrix $F \in R^{m \times n}$, order \preccurlyeq

Output: a minimal \preccurlyeq -GB of $\text{Syz}_{\mathcal{M}}(F)$ where $\mathcal{M} = \bigcap_i \ker(\varphi_i)$

```

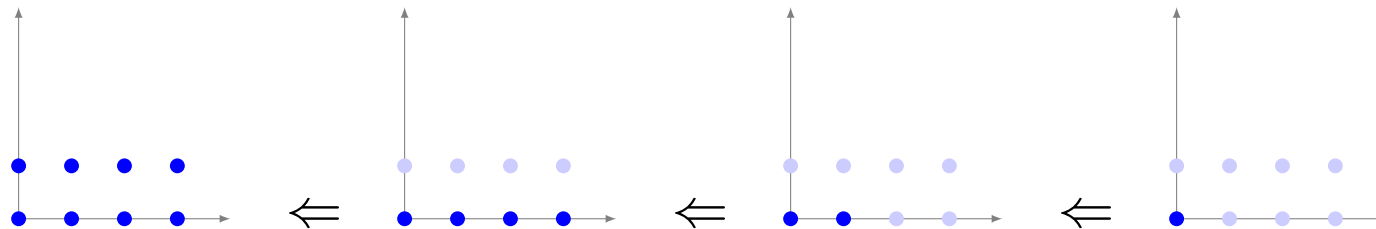
 $P \leftarrow I_m \in \mathcal{R}^{m \times m}; G \leftarrow F; L \leftarrow (\mathbf{e}_1, \dots, \mathbf{e}_m) = \text{lm}_{\preccurlyeq}(P)$ 
for  $i = 1, \dots, D$  do
     $(Q, L) \leftarrow \text{SYZYGY\_BASECASE}(\varphi_i, G, \preccurlyeq, L)$ 
     $P \leftarrow QP; G \leftarrow QG$ 
return  $P$ 
    
```

Divide and conquer

The algorithm is turned into a d-a-conq one:

```
if  $D = 1$  then return SYZGY_BASECASE( $\varphi_i, G, \leq, K$ )  
 $(Q_1, L_1) \leftarrow$  SYZGY_DAC( $\varphi_1, \dots, \varphi_{\lfloor D/2 \rfloor}, G, \leq, K$ )  
 $(Q_2, L_2) \leftarrow$  SYZGY_DAC( $\varphi_{\lfloor D/2 \rfloor + 1}, \dots, \varphi_D, Q_1 G, \leq, L_1$ )  
return  $(Q_2 Q_1, L_2)$ 
```

The set of functionals is divided in two parts, and the matrix multiplication is organized by consequence.



Complexity of bivariate Padé

For $R = K[X, Y]$, let

$$\mathcal{M} = \langle X^d, Y^e \rangle \times \cdots \times \langle X^d, Y^e \rangle \subset R^n,$$

let $\mathbf{F} \in R^{m \times n}$ with $\deg_X(\mathbf{F}) < d$ and $\deg_Y(\mathbf{F}) < e$, and let \preceq be a monomial order on R^m .

Complexity bound for bivariate Padé. The algorithm computes a minimal \preceq -GB of $\text{Syz}_{\mathcal{M}}(\mathbf{F})$ using

$$O\tilde{~}((M^{\omega-1} + Mn)(M + n)de)$$

operations in K , where $M = m \min(d, e)$.

Finally, one example

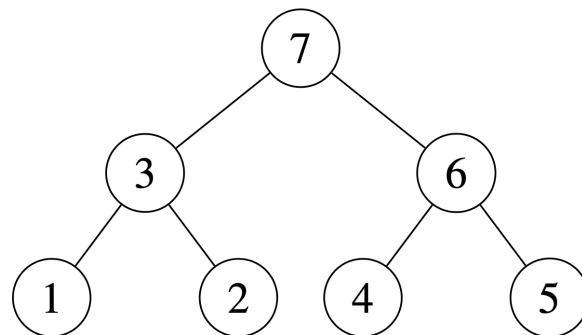
We want to compute syzygies of

$$F = \begin{bmatrix} 1 \\ -1 \end{bmatrix} \in K[X, Y]^{2 \times 1}$$

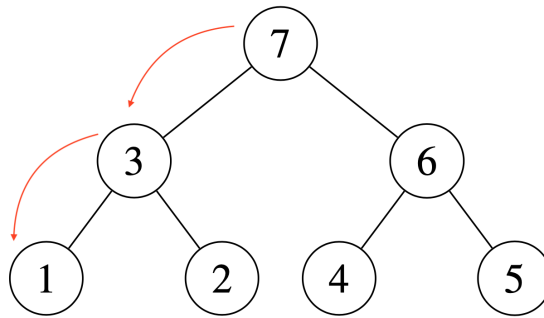
modulo the ideal $I = \langle X^2, Y^2 \rangle$.

I assume $K[X, Y]$ with the lexicographic order $\preccurlyeq_{\text{lex}}$ with $Y \preccurlyeq_{\text{lex}} X$ and let \preccurlyeq be the term over position order $\preccurlyeq_{\text{lex}}^{\text{top}}$.

The algorithm organises the steps in a tree of the form



- On the top (*step 7*), we call $\text{Padé}(2, 2, \mathbf{F}, \preceq, L)$. The recursive call will reduce the computation to $\text{Padé}(2, 1, \mathbf{F}, \preceq, L)$ (*step 3*), then $\text{Padé}(1, 1, \mathbf{F}, \preceq, L)$ (*step 1*).



- $\text{Padé}(1, 1, \mathbf{F}, \preceq, L)$ on *step 1*: The output is computed with the “base case algorithm” with functional $\varphi(f) = \text{coeff}(f, 1)$:

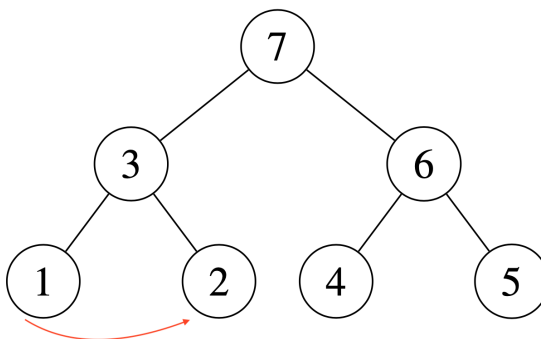
$$\mathbf{Q}_1 = \begin{bmatrix} X & 0 \\ Y & 0 \\ 1 & 1 \end{bmatrix}$$

and its leading terms $L_1 = ((X, 0), (Y, 0), (0, 1))$.

- Back to *Node 3*, we compute the “residual”

$$G_2 = X^{-1}(\mathbf{Q}_1 F \bmod X^2, Y) = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Next we call $\text{Padé}(1, 1, G_2, \preceq, L_1)$, base case (*Node 2*).



This step computes the matrix

$$\mathbf{Q}_2 = \begin{bmatrix} X & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

and the new leading monomials $L_2 = ((X^2, 0), (Y, 0), (0, 1))$.

Note that \mathbf{Q}_2 is a subset of the elementary Gröbner basis

$$E_2 = \begin{bmatrix} X & 0 & 0 \\ Y & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where one row has been deleted, since it is redundant.

- Now the first recursive call of the top call is completed. We

compute the residual

$$\widehat{\mathbf{G}}_2 = Y^{-1}(\mathbf{Q}\mathbf{F} \bmod X^2, Y^2) = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}.$$

and go to (*Node 6*).

- *Node 6* has in input $(2, 1, \widehat{\mathbf{G}}_2, \preceq, L_2)$, and we do the same on the right part of the tree, whose output is the matrix

$$\widehat{\mathbf{Q}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & Y & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

- Finally we get the output of the main call (*Node 7*), that is

$$\widehat{\mathbf{Q}}\mathbf{Q}_2\mathbf{Q}_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & Y & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X^2 & 0 \\ Y & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} X^2 & 0 \\ Y^2 & 0 \\ 1 & 1 \end{bmatrix}$$

whose leading monomials are \widehat{L}_2 and which is the sought \preceq -Gröbner basis of syzygies for \mathbf{F} modulo $\langle X^2, Y^2 \rangle$.

Related work

Univariate case

Beckermann-Labahn '94 – $O^{\sim}(m^{\omega} D)$

Giorgi-Jeannerod-Villard '03 – $O^{\sim}(m^{\omega-1} D)$

Neiger-Vu '17 – $O^{\sim}(m^{\omega-1} D)$

[Hermite-Padé X^D]
[[$\langle X^d \rangle \times \dots \times \langle X^d \rangle$, $n \approx m$]
[more general]

Multivariate interpolation

Möller-Buchberger '82

Faugère-Gianni-Lazard-Mora '93

Marinari-Möller-Mora '93

O'Keefe-Fitzpatrick '02 – $O(r D^3)$

FGHR '14, Neiger-Schost '20 – $O^{\sim}(m D^{\omega-1} + r D^{\omega})$

Combinatorial algorithms

Cerlienco-Mureddu '93

Mora-Ceria '18 – $O(r D^2 \log D)$

Multidimensional linear recurrent sequences

Sakata '88

Mourrain '17

Berthomieu-Faugère '18