

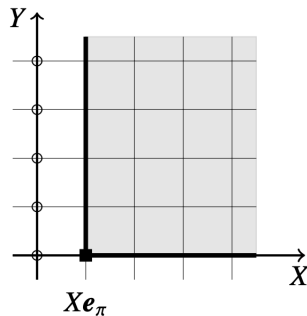
Gröbner bases of syzygies and polynomial matrix multiplication

Algebraic rewriting seminar

Simone Naldi (jw V. Neiger)

XLIM – Université de Limoges

December 6th, 2021



K	<i>field</i>
$R = K[X_1, X_2, \dots, X_r]$	<i>ring of r-variate polynomials over K</i>
$\mathcal{M} \subset R^n$	<i>R-submodule of R^n</i>
$D = \dim_K(R^n/\mathcal{M})$	<i>co-dimension</i>
$\mathbf{f}_1, \dots, \mathbf{f}_m \in R^n/\mathcal{M}$	<i>input elements (row vectors)</i>
$\mathbf{F} = (\mathbf{f}_1, \dots, \mathbf{f}_m) \in R^{m \times n}$	<i>matrix with rows $\mathbf{f}_1, \dots, \mathbf{f}_m$</i>

The goal is to compute syzygies, that is vectors $\mathbf{p} = (p_1, \dots, p_m) \in R^{1 \times m}$

$$p_1 \mathbf{f}_1 + \dots + p_m \mathbf{f}_m = \mathbf{0} \pmod{\mathcal{M}}$$

In particular, we aim at computing a Gröbner basis (for some order) of the first syzygy module

$$\text{Syz}_{\mathcal{M}}(\mathbf{F}) = \{\mathbf{p} \in R^{1 \times m} \mid \mathbf{p}\mathbf{F} \in \mathcal{M}\}$$

Hermite-Padé approximation

$R = K[X]$ 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

$$f = \frac{p_2}{p_1} \pmod{X^d} \quad (\iff [p_1 \ p_2] \begin{bmatrix} f \\ -1 \end{bmatrix} = 0)$$

More generally, given $f_1, \dots, f_m \in R/\langle X^d \rangle$, find $\mathbf{p} \in R^m$ s.t.

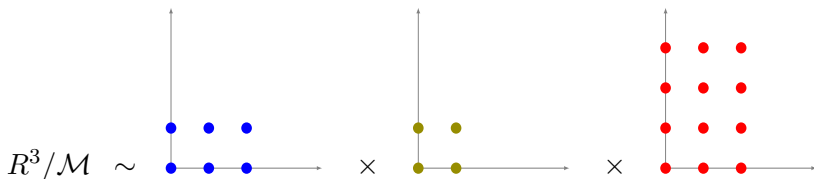
$$\mathbf{p} \mathbf{F} = [p_1 \ \dots \ p_m] \begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix} = 0 \pmod{X^d}$$

According to our notation: $r = 1, n = 1, \mathcal{M} = \langle X^d \rangle, D = d$.

Hermite-Padé approximation (module)

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

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



$$D = 6 + 4 + 12$$

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

D points $\alpha_1, \dots, \alpha_D \in \mathbb{R}^r$

$f_1, \dots, f_m \in R = K[X_1, \dots, X_r]$

The goal is to find all linear combinations $\mathbf{p} = (p_1, \dots, p_m)$ such that

$$p_1(\alpha_i)f_1(\alpha_i) + \dots + p_m(\alpha_i)f_m(\alpha_i) = 0 \quad \forall i = 1, \dots, D$$

that is, that belong to the ideal $I = I(\{\alpha_1, \dots, \alpha_D\})$.

Special choice: if $m = 1$, $f_1 = 1$, the object to be computed is

$$\text{Syz}_I(1) = \{p \in R \mid p(\alpha_i) = 0, \forall i\} = I$$

-
- For every ideal I , one has $\text{Syz}_I(1) = I$ (not only ideals of points)
 - An algorithm that computes a GB of $\text{Syz}_I(1)$ computes a GB of I
 - One can apply this algorithm to compute a change of ordering

Input representation

We assume that the input module \mathcal{M} has a “dual iterative representation”:

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

$$\mathcal{M} = \ker(\varphi), \text{ où } \varphi = (\varphi_1, \dots, \varphi_D) : R^n \rightarrow K^D$$

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

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

Our contribution: We interpret this algorithm with [polynomial matrix operations](#) (“products of Gröbner bases”): this allows us to design a [divide-and-conquer](#) strategy.

Interpolation : the functionals are the evaluations at α_j , and the condition is satisfied, $I(\{\alpha_1, \dots, \alpha_D\})$ can be constructed by adding the points iteratively

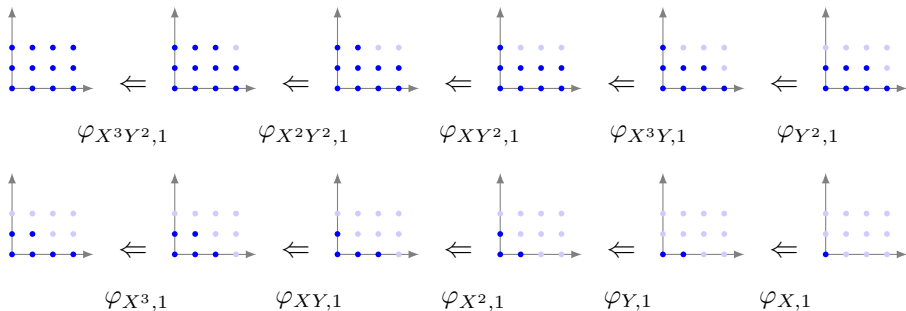
$$\mathcal{M}_i = I(\{\alpha_1, \dots, \alpha_i\}) \text{ is a module, for every order of points}$$

Padé Approximation : the functional φ_j is the coefficient of the j -th monomial in the monomial basis of R^n/\mathcal{M} (but the order now matters!) :

$$\mathcal{M} = \langle X_1^{d_{11}}, \dots, X_r^{d_{1r}} \rangle \times \dots \times \langle X_1^{d_{n1}}, \dots, X_r^{d_{nr}} \rangle \subseteq R^n$$

The functionals are $\varphi_{\mu,i}(\cdot) = \text{coeff}(\cdot, \mu e_i)$, for μe_i in the *escalier* of \mathcal{M}

Example. For $n = 1$ and $\mathcal{M} = \langle X^4, Y^3 \rangle$



Monomials of R^n are of the form μe_i where μ is a ring monomial and e_i is the i -th element of the canonical basis.

Let $\mathcal{N} \subset R^n$, and let \preccurlyeq be a term order in R^n . A *Gröbner basis* of \mathcal{N} is a subset $G \subset \mathcal{N}$ such that $\langle \text{lm}_{\preccurlyeq}(G) \rangle = \langle \text{lm}_{\preccurlyeq}(\mathcal{N}) \rangle$

There is a “natural” class of orders on syzygies (R^m), that can be defined from the order on R^n :

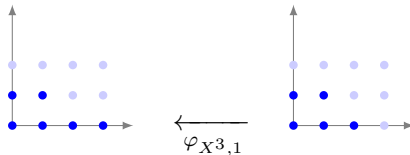
Let \preccurlyeq and $L = (\mu_1, \dots, \mu_m)$ be a term order and a list of monomials of R^n . We say that \preccurlyeq_L is a *Schreyer order* for \preccurlyeq and L if

$$\nu_1 \mu_i \prec \nu_2 \mu_j \implies \nu_1 e_i \prec_L \nu_2 e_j$$

for all ν_1, ν_2 ring monomials, and $i, j = 1, \dots, m$.

\preccurlyeq_L is the order that appears in Schreyer's theorem.

One step of the iteration



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

$\mathbf{F} \in R^{m \times n}$ with rows in R^n / \mathcal{N}

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

we know a Gröbner basis \mathbf{P} of $\text{Syz}_{\mathcal{N}}(\mathbf{F})$

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

$\mathcal{N} = \langle X^3, X^2Y, Y^2 \rangle$

$\varphi = \varphi_{X^3,1}$

$\text{Syz}_{\langle X^3, X^2Y, Y^2 \rangle}(\mathbf{F})$

$\text{Syz}_{\langle X^4, X^2Y, Y^2 \rangle}(\mathbf{F})$

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 modules)

► If $\dim_K(R^m/\mathcal{M}) = 1$, for every \preceq the \preceq -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 \preceq -GB for any \preceq such that $\lambda_i = 0$ if $e_i \prec e_\pi$ for all $i \neq \pi$.

One-step algorithm (sketch)

Soit $G = PF = (g_1, \dots, g_k)$, and we know that this is zero modulo \mathcal{N} .

We evaluate $(\varphi(g_1), \dots, \varphi(g_k)) =: (v_1, \dots, v_k)$. If this is zero, one deduces $\text{Syz}_{\mathcal{N}}(\mathbf{F}) = \text{Syz}_{\ker(\varphi) \cap \mathcal{N}}(\mathbf{F})$.

Otherwise, we define some well-chosen vectors

$$\begin{aligned} \leq_K &\leftarrow \text{SCHREYERORDER}(\leq, \mathbf{K}) \\ \pi &\leftarrow \arg \min_{\leq_K} \{e_i \mid 1 \leq i \leq k, v_i \neq 0\} \quad \triangleright \text{the index } i \text{ such that} \\ &v_i \neq 0 \text{ which minimizes } e_i \text{ with respect to } \leq_K \\ \{j_1 < \dots < j_\ell\} &\leftarrow \{j \in \{1, \dots, r\} \mid X_j \mu_\pi \notin \langle \mu_i, i \neq \pi \rangle\} \\ \alpha_{j_s} &\leftarrow \varphi(X_{j_s} g_\pi) / v_\pi \text{ for } 1 \leq s \leq \ell \\ \lambda_i &\leftarrow -v_i / v_\pi \text{ for } 1 \leq i < \pi \text{ and } \pi < i \leq k \end{aligned}$$

in order to construct an elementary matrix \mathbf{E} satisfying

$$\langle \mathbf{E} \rangle = \text{Syz}_{\ker(\varphi) \cap \mathcal{N}}(\mathbf{PF})$$

One-step algorithm (sketch, cont'd)

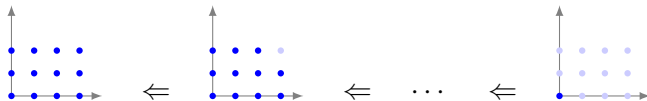
Finally we output the following matrix \mathbf{Q} (a submatrix of \mathbf{E})

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

so that we have this result:

Theorem. If the input matrix \mathbf{P} is a minimal \preceq -Gröbner basis, then the submatrix \mathbf{Q} is such that \mathbf{QP} is a minimal \preceq -Gröbner basis of $\text{Syz}_{\ker(\varphi) \cap \mathcal{M}}(\mathbf{F})$.

Sequential algorithm



The base case described above can be iterated as follows:

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

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

```
P ← I_m ∈ R^{m × m}; G ← F; L ← (e_1, …, e_m) = lm_{\preccurlyeq}(P)
for i = 1, …, D do
  (Q, L) ← SYZGY_BASECASE(φ_i, G, \preccurlyeq, L)
  P ← QP; G ← QG
return P
```

The sequential algorithm produces D matrices $\mathbf{Q}_1, \mathbf{Q}_2, \dots, \mathbf{Q}_D$ such that $\mathbf{Q}_D \mathbf{Q}_{D-1} \cdots \mathbf{Q}_1$ is a Gröbner basis of

$$\langle \mathbf{Q}_D \mathbf{Q}_{D-1} \cdots \mathbf{Q}_1 \rangle = \text{Syz}_{\mathcal{M}}(\mathbf{F})$$

which suggests a divide-and-conquer strategy, based on the re-organization of products :

```
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  $(Q_2 Q_1, L_2)$ 
```

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 .

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

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

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

For $m = 2, n = 1, d = e$ (classical Padé) this complexity is of the order $O^{\sim}(d^{\omega+2}) = O^{\sim}(D^{\frac{\omega+2}{2}})$, and the approach by linear algebra (Vincent's talk) gives $O^{\sim}(D^{\omega})$.

One example I

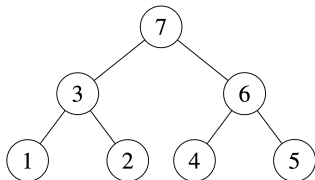
We want to compute syzygies of

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

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

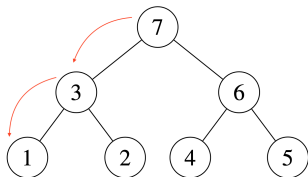
I assume $K[X, Y]$ with the lexicographic order \preceq_{lex} with $Y \preceq_{\text{lex}} X$ and let \preceq be the term over position order $\preceq_{\text{lex}}^{\text{top}}$.

The algorithm organises the steps in a tree of the form



One example II

- 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 $\varphi(f) = \text{coeff}(f, 1)$:

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

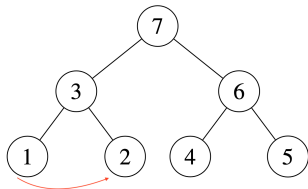
and its leading terms $L_1 = ((X, 0), (Y, 0), (0, 1))$.

One example III

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

$$\mathbf{G}_2 = X^{-1}(\mathbf{Q}_1 \mathbf{F} \bmod X^2, Y) = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Next we call $\text{Padé}(1, 1, \mathbf{G}_2, \preceq, L_1)$, base case (*Node 2*).



One example IV

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 $\langle X^2, Y^2 \rangle$.

This talk is based on



“A divide-and-conquer algorithm for computing Gröbner bases of syzygies in finite dimension” (S. Naldi, V. Neiger) ACM ISSAC 2020, pp. 380-387

Related papers:



“A Uniform Approach for the Fast Computation of Matrix-Type Padé Approximants”
(B. Beckermann, G. Labahn) SIAM J. Matrix Anal. Appl. 15, 3 (1994), 804–823



“Gröbner bases of ideals defined by functionals with an application to ideals of projective points”
(M. G. Marinari, H. M. Moller, T. Mora) Appl. Algebra Engrg. Comm. Comput. 4, 2 (1993), 103–145