

Gröbner bases of syzygy modules and multivariate Padé approximation



Simone Naldi (jw Vincent Neiger)

Séminaire POLSYS – June 2020



Hermite-Padé approximation

Given $f \in R = K[X]$ of degree $d - 1$, we look for $p_1, p_2 \in R$ s.t.

$$f = \frac{p_2}{p_1} \pmod{\langle X^d \rangle}$$

In other words (p_1, p_2) is a relation of $(f, -1)$ modulo X^d :

$$p_1 f - p_2 = 0 \pmod{\langle X^d \rangle}$$

In general given $f_1, \dots, f_m \in R/\langle X^d \rangle$, one looks for $p_i \in R$ s.t.

$$p_1 f_1 + \dots + p_m f_m = 0 \pmod{\langle X^d \rangle}$$

In this case $(p_1, \dots, p_m) \in R^m$ is a *syzygy* of f_1, \dots, f_m modulo X^d (comm. algebra), or an *approximant* (Padé literature).

Example

Consider the Padé approximation problem ($K = \mathbb{Z}/5\mathbb{Z}$)

$$\begin{bmatrix} p_1 & p_2 & p_3 & p_4 \end{bmatrix} \begin{bmatrix} 2X^4 - 4X - 1 \\ 3X^5 + X^4 + X^3 - X - 1 \\ X - 1 \\ 2X^2 + X + 1 \end{bmatrix} = 0 \pmod{\langle X^6 \rangle}$$

A trivial solution always exists : $\begin{bmatrix} X^6 & 0 & 0 & 0 \end{bmatrix}$

The main question is how to represent the set of *all* relations.

Remark that (p_1, p_2, p_3, p_4) is an element of the global module R^4 , whereas the input $(f_1, f_2, f_3, f_4)^T$ is reduced modulo X^6 .

General context

From now on $\mathbf{X} = (X_1, \dots, X_r)$ and $R = K[\mathbf{X}]$

Given a R -module $\mathcal{N} \subset R^n$, and elements $\mathbf{f}_1, \dots, \mathbf{f}_m \in R^n / \mathcal{N}$

We assume $\dim_K(R^n / \mathcal{N}) = D < +\infty$

Compute elements $p_1, \dots, p_m \in R$ such that

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

Compact notation: $\mathbf{pF} = 0$ with

$\mathbf{p} = 1 \times m$ vector of p_1, \dots, p_m

$\mathbf{F} = m \times 1$ column vector of (row vectors) $\mathbf{f}_1, \dots, \mathbf{f}_m$
 $= m \times n$ polynomial matrix, that is $\mathbf{F} \in R^{m \times n}$

Syzygy modules

The set of all syzygies of \mathbf{F} (its rows are mod \mathcal{N})

$$\begin{aligned}\text{Syz}_{\mathcal{N}}(\mathbf{F}) &= \{(p_1, \dots, p_m) \in R^m \mid p_1 \mathbf{f}_1 + \dots + p_m \mathbf{f}_m = 0\} \\ &= \{\mathbf{p} \in R^m \mid \mathbf{p}\mathbf{F} = 0\}\end{aligned}$$

is a R -submodule of R^m .

In our work we assume that R^n/\mathcal{N} has finite dimension D as a K -vector space, and since we have a natural morphism

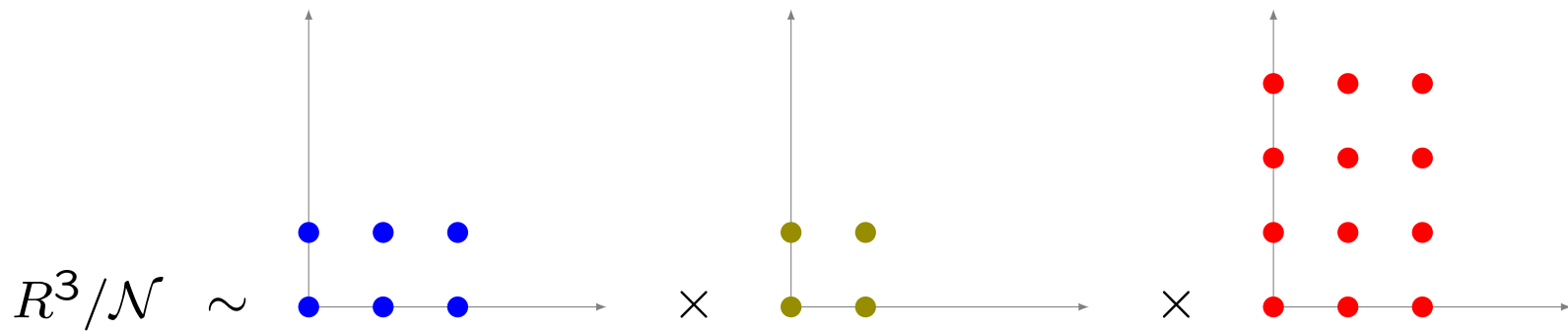
$$R^m \ni \mathbf{p} \mapsto \mathbf{p}\mathbf{F} \in R^n/\mathcal{N}$$

with kernel $\text{Syz}_{\mathcal{N}}(\mathbf{F})$, one deduces $\dim_K(R^m/\text{Syz}_{\mathcal{N}}(\mathbf{F})) \leq D$

Roughly speaking: the vs-dimension of the output module we want to represent is “controlled by” the vs-dimension of the input module.

Concrete situation: Bivariate Padé

For instance $\mathcal{N} = I_1 \times \cdots \times I_n$ with $I_i \subset R$ 0-dim ideals



$$\mathcal{N} \sim \langle X^3, Y^2 \rangle \times \langle X^2, Y^2 \rangle \times \langle X^3, Y^4 \rangle$$

$$D = 6 + 4 + 12$$

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

Monomial orders for modules

A *monomial* in R^m is an element of the form μe_i where $\mu \in R$ is a monomial and e_i is the i -th vector of canonical basis ($\text{Mon}(R^m)$).

A *monomial order* on R^m is a total order \preceq on $\text{Mon}(R^m)$ such that for $\nu \in \text{Mon}(R)$ and $\mu_1, \mu_2 \in \text{Mon}(R^m)$

$$\mu_1 \preceq \mu_2 \Rightarrow \mu_1 \preceq \nu\mu_1 \preceq \nu\mu_2$$

From \preceq in R one can define “canonical” module orders, f.ex.:

position-over-term: $\mu e_i \preceq^{pot} \nu e_j$ if $i < j$ or ($i = j$ and $\mu \preceq \nu$)

term-over-position: $\mu e_i \preceq^{top} \nu e_j$ if $\mu \prec \nu$ or ($\mu = \nu$ and $i < j$)

Gröbner bases

$\mathcal{P} \subset R^m$: $\langle \mathcal{P} \rangle$ the R -submodule generated by \mathcal{P} .

$\mathbf{P} \in R^{k \times m}$: $\langle \mathbf{P} \rangle$ the R -submodule of R^m gen. by the rows of \mathbf{P} .

Let $\mathcal{M} \subset R^m$. A matrix \mathbf{P} in $R^{k \times m}$ whose rows are in \mathcal{M} is said to be a \preccurlyeq -Gröbner basis of \mathcal{M} if

$$\langle \text{Im}_{\preccurlyeq}(\mathcal{M}) \rangle = \langle \text{Im}_{\preccurlyeq}(\mathbf{P}) \rangle.$$

Example ($r = m = 2, n = 1$). The syzygy module

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

is generated by $(Xe_1, Ye_1, e_1 + e_2)$, that is, by the rows of

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

Furthermore, \mathbf{E} is the reduced $\preccurlyeq_{\text{lex}}^{\text{top}}$ -Gröbner basis of $\text{Syz}_{\langle X, Y \rangle} \left(\begin{bmatrix} 1 \\ -1 \end{bmatrix} \right)$.

Example (continued)

$$K = \mathbb{Z}/5\mathbb{Z}, R = K[X]$$

$$\mathbf{F} = \begin{bmatrix} 2X^4 - 4X - 1 \\ 3X^5 + X^4 + X^3 - X - 1 \\ X - 1 \\ 2X^2 + X + 1 \end{bmatrix} \quad (\text{approx. mod } \langle X^6 \rangle)$$

A GB (TOP order in R^4) of $\text{Syz}_{\langle X^6 \rangle}(\mathbf{F})$ is :

$$\mathbf{P} = \begin{bmatrix} -X - 1 & 2X & X + 2 & 1 \\ 2X & 2X - 2 & -1 & X + 2 \\ X^2 - X - 2 & -1 & -1 & 1 \\ 2X + 1 & X^2 + 2X + 1 & 1 & -2 \end{bmatrix}$$

Schreyer orders

It is convenient to define special orders when dealing with sygygies which we call Schreyer orders.

Given:

\preceq a monomial order on R^m and

$L = (\mu_1, \dots, \mu_k)$ a list of monomials of R^m (often Im of GB)

A *Schreyer order* for \preceq and L is any monomial order \preceq_L on R^k , such that it compares $\nu_1 e_i, \nu_2 e_j \in \text{Mon}(R^k)$ as follows:

if $\nu_1 \mu_i \prec \nu_2 \mu_j$ then $\nu_1 e_i \preceq_L \nu_2 e_j$

This extends to $r > 1$ similar orders used in the univariate case (*shifts*).

Moreover a Schreyer order always exists: just take

$\nu_1 e_i \preceq_L \nu_2 e_j$ iff $\nu_1 \mu_i \prec \nu_2 \mu_j$ or $(\nu_1 \mu_i = \nu_2 \mu_j$ and $i < j)$.

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 elementary Gröbner basis of $\langle \mathbf{E} \rangle = \text{Syz}_{\langle X, Y \rangle}([\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}])$.

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 Schreyer with respect to \preccurlyeq and $L = (\mu_1, \dots, \mu_k) = \text{Im}_{\preccurlyeq}(\mathbf{P})$
- \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.

A “counterexample”

An open question is to have necessary and sufficient condition on \mathbf{E} and \mathbf{P} so that their product is still Gröbner.

What we know is that it is not sufficient that \mathbf{P} is a reduced GB:

Example. ($r = 2, m = 1, n = 1$)

Let $R = K[X, Y]$ and $\mathbf{P} = (X, Y + 1)^T \in R^{2 \times 1}$. Then:

- \mathbf{P} is a reduced \preccurlyeq_1 -Gröbner basis (any \preccurlyeq_1)
- $\mathbf{E} = (Xe_1, Ye_1, e_2)^T \in R^{3 \times 2}$ is a reduced \preccurlyeq_2 -Gröbner
- $\mathbf{EP} = (X^2, XY, Y + 1)^T \in R^{3 \times 1}$
- Since $X = X(Y + 1) - XY$ then $\langle \mathbf{EP} \rangle = \langle \mathbf{P} \rangle$ and $\langle \text{Im}_{\preccurlyeq_3}(\mathbf{EP}) \rangle \neq \langle \text{Im}_{\preccurlyeq_3}(\langle \mathbf{EP} \rangle) \rangle$

which means that \mathbf{EP} is **not** a \preccurlyeq_3 -Gröbner basis (for all \preccurlyeq_3).

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.

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

An iterative algorithm is described in MMM 1993 (generalizing Buchberger-Möller multivariate interpolation algorithm), based on this dual representation.

We interpret such algorithms in a module framework and incorporate fast **polynomial matrix multiplication** which allows to design a **divide-and-conquer** strategy.

Example: Interpolation

Take $n = 1$, and fix D distinct points $\alpha_1, \dots, \alpha_D \in K^r$.

In this case the functionals are evaluations at these points, and $\mathcal{N} \subset R$ is the vanishing ideal :

$$\mathcal{N} = \{f \in R : \varphi_i(f) := f(\alpha_i) = 0, i = 1, \dots, D\}.$$

In our framework the question would be: given $\mathbf{F} \in (R/\mathcal{N})^m$ and the points α_i , describe the set of $\mathbf{p} \in R^m$ such that

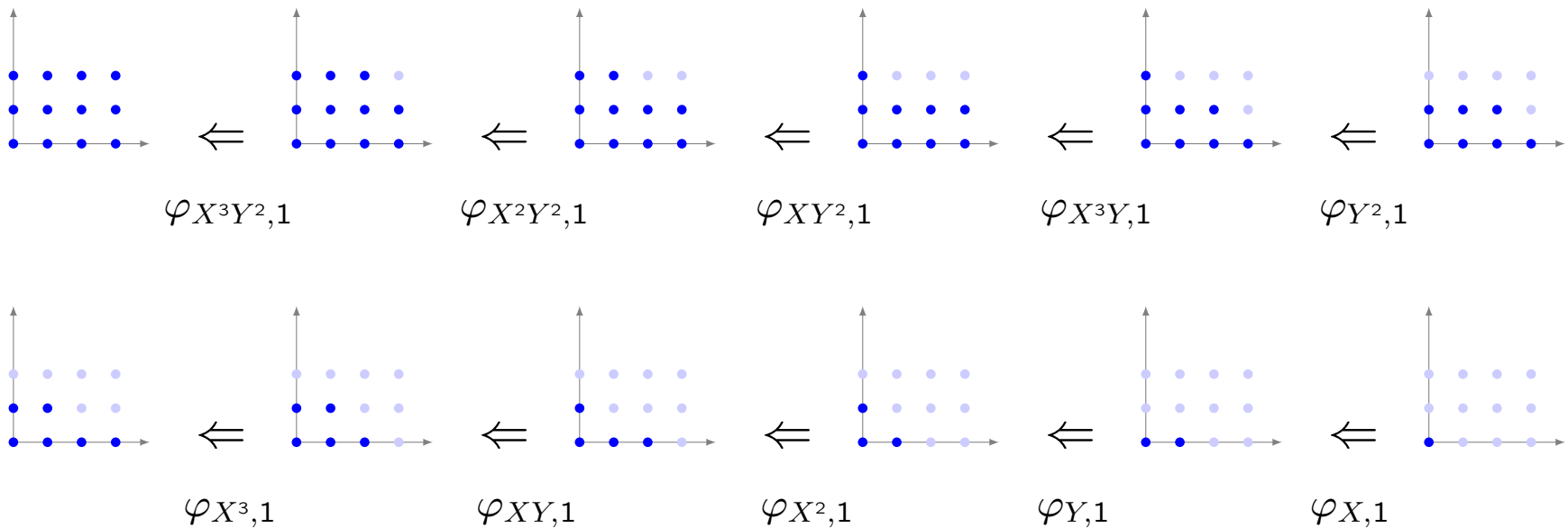
$$\mathbf{p}\mathbf{F} = \sum_j p_j f_j = 0 \text{ in } R/\mathcal{N} \iff \sum_j p_j(\alpha_i) f_j(\alpha_i) = 0 \text{ for all } i.$$

Special case. If $m = 1$ and $\mathbf{F} = [1]$, we look for a GB of the vanishing ideal.

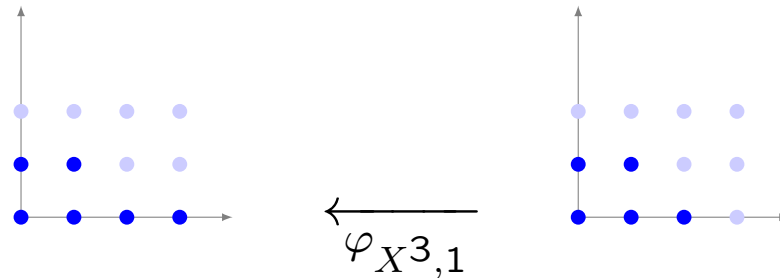
Multivariate Padé approximation

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

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



A one-step algorithm



We first describe the typical situation where

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

$F \in R^{m \times n}$ is given 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 $\langle \mathbf{P} \rangle = \text{Syz}_{\mathcal{N}}(F)$

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

Algorithm 1 SYZGY_BASECASE(φ, G, \preceq, L)

Input:

- a linear functional $\varphi : \mathcal{R}^n \rightarrow \mathbb{K}$,
- a matrix G in $\mathcal{R}^{k \times n}$ with rows $\mathbf{g}_1, \dots, \mathbf{g}_k \in \mathcal{R}^n$,
- a monomial order \preceq on \mathcal{R}^m ,
- a list $\mathbf{K} = (\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_k)$ of elements of $\text{Mon}(\mathcal{R}^m)$.

Output:

- a matrix Q in $\mathcal{R}^{(k+\ell-1) \times k}$ for some $\ell \in \{0, \dots, r\}$,
 - a list L of $k + \ell - 1$ elements of $\text{Mon}(\mathcal{R}^k)$.
- 1: $(v_1, \dots, v_k) \leftarrow (\varphi(\mathbf{g}_1), \dots, \varphi(\mathbf{g}_k)) \in \mathbb{K}^k$
 - 2: **if** $(v_1, \dots, v_k) = (0, \dots, 0)$ **then return** (I_k, \mathbf{K})
 - 3: $\preceq_{\mathbf{K}} \leftarrow \text{SCHREYERORDER}(\preceq, \mathbf{K})$
 - 4: $\pi \leftarrow \arg \min_{\preceq_{\mathbf{K}}} \{\mathbf{e}_i \mid 1 \leq i \leq k, v_i \neq 0\}$ \triangleright the index i such that $v_i \neq 0$ which minimizes \mathbf{e}_i with respect to $\preceq_{\mathbf{K}}$
 - 5: $\{j_1 < \dots < j_\ell\} \leftarrow \{j \in \{1, \dots, r\} \mid X_j \boldsymbol{\mu}_\pi \notin \langle \boldsymbol{\mu}_i, i \neq \pi \rangle\}$
 - 6: $\alpha_{j_s} \leftarrow \varphi(X_{j_s} \mathbf{g}_\pi) / v_\pi$ for $1 \leq s \leq \ell$
 - 7: $\lambda_i \leftarrow -v_i / v_\pi$ for $1 \leq i < \pi$ and $\pi < i \leq k$
 - 8: $Q \leftarrow$ matrix in $\mathcal{R}^{(k+\ell-1) \times k}$ as in Eq. (3)
 - 9: $L \leftarrow (\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_{\pi-1}, X_{j_1} \boldsymbol{\mu}_\pi, \dots, X_{j_\ell} \boldsymbol{\mu}_\pi, \boldsymbol{\mu}_{\pi+1}, \dots, \boldsymbol{\mu}_k)$
 - 10: **return** (Q, L)
-

Algorithm 1 SYZGY_BASECASE(φ, G, \preceq, L)

Input:

- • a linear functional $\varphi : \mathcal{R}^n \rightarrow \mathbb{K}$,
- • a matrix G in $\mathcal{R}^{k \times n}$ with rows $\mathbf{g}_1, \dots, \mathbf{g}_k \in \mathcal{R}^n$,
- • a monomial order \preceq on \mathcal{R}^m ,
- • a list $\mathbf{K} = (\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_k)$ of elements of $\text{Mon}(\mathcal{R}^m)$.

Output:

- a matrix Q in $\mathcal{R}^{(k+\ell-1) \times k}$ for some $\ell \in \{0, \dots, r\}$,
 - a list L of $k + \ell - 1$ elements of $\text{Mon}(\mathcal{R}^k)$.
- 1: $(v_1, \dots, v_k) \leftarrow (\varphi(\mathbf{g}_1), \dots, \varphi(\mathbf{g}_k)) \in \mathbb{K}^k$
 - 2: **if** $(v_1, \dots, v_k) = (0, \dots, 0)$ **then return** (I_k, \mathbf{K})
 - 3: $\preceq_{\mathbf{K}} \leftarrow \text{SCHREYERORDER}(\preceq, \mathbf{K})$
 - 4: $\pi \leftarrow \arg \min_{\preceq_{\mathbf{K}}} \{\mathbf{e}_i \mid 1 \leq i \leq k, v_i \neq 0\}$ \triangleright the index i such that $v_i \neq 0$ which minimizes \mathbf{e}_i with respect to $\preceq_{\mathbf{K}}$
 - 5: $\{j_1 < \dots < j_\ell\} \leftarrow \{j \in \{1, \dots, r\} \mid X_j \boldsymbol{\mu}_\pi \notin \langle \boldsymbol{\mu}_i, i \neq \pi \rangle\}$
 - 6: $\alpha_{j_s} \leftarrow \varphi(X_{j_s} \mathbf{g}_\pi) / v_\pi$ for $1 \leq s \leq \ell$
 - 7: $\lambda_i \leftarrow -v_i / v_\pi$ for $1 \leq i < \pi$ and $\pi < i \leq k$
 - 8: $Q \leftarrow$ matrix in $\mathcal{R}^{(k+\ell-1) \times k}$ as in Eq. (3)
 - 9: $L \leftarrow (\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_{\pi-1}, X_{j_1} \boldsymbol{\mu}_\pi, \dots, X_{j_\ell} \boldsymbol{\mu}_\pi, \boldsymbol{\mu}_{\pi+1}, \dots, \boldsymbol{\mu}_k)$
 - 10: **return** (Q, L)
-

Algorithm 1 SYZGY_BASECASE(φ, G, \preceq, L)

Input:

- a linear functional $\varphi : \mathcal{R}^n \rightarrow \mathbb{K}$,
- a matrix G in $\mathcal{R}^{k \times n}$ with rows $\mathbf{g}_1, \dots, \mathbf{g}_k \in \mathcal{R}^n$,
- a monomial order \preceq on \mathcal{R}^m ,
- a list $\mathbf{K} = (\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_k)$ of elements of $\text{Mon}(\mathcal{R}^m)$.

Output:

→ • a matrix Q in $\mathcal{R}^{(k+\ell-1) \times k}$ for some $\ell \in \{0, \dots, r\}$,

→ • a list L of $k + \ell - 1$ elements of $\text{Mon}(\mathcal{R}^k)$.

1: $(v_1, \dots, v_k) \leftarrow (\varphi(\mathbf{g}_1), \dots, \varphi(\mathbf{g}_k)) \in \mathbb{K}^k$

2: **if** $(v_1, \dots, v_k) = (0, \dots, 0)$ **then return** (I_k, \mathbf{K})

3: $\preceq_{\mathbf{K}} \leftarrow \text{SCHREYERORDER}(\preceq, \mathbf{K})$

4: $\pi \leftarrow \arg \min_{\preceq_{\mathbf{K}}} \{\mathbf{e}_i \mid 1 \leq i \leq k, v_i \neq 0\}$ \triangleright the index i such that $v_i \neq 0$ which minimizes \mathbf{e}_i with respect to $\preceq_{\mathbf{K}}$

5: $\{j_1 < \dots < j_\ell\} \leftarrow \{j \in \{1, \dots, r\} \mid X_j \boldsymbol{\mu}_\pi \notin \langle \boldsymbol{\mu}_i, i \neq \pi \rangle\}$

6: $\alpha_{j_s} \leftarrow \varphi(X_{j_s} \mathbf{g}_\pi) / v_\pi$ for $1 \leq s \leq \ell$

7: $\lambda_i \leftarrow -v_i / v_\pi$ for $1 \leq i < \pi$ and $\pi < i \leq k$

8: $Q \leftarrow$ matrix in $\mathcal{R}^{(k+\ell-1) \times k}$ as in Eq. (3)

9: $L \leftarrow (\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_{\pi-1}, X_{j_1} \boldsymbol{\mu}_\pi, \dots, X_{j_\ell} \boldsymbol{\mu}_\pi, \boldsymbol{\mu}_{\pi+1}, \dots, \boldsymbol{\mu}_k)$

10: **return** (Q, L)

“Correctness” of one-step algorithm

Recap of assumptions

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

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

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

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

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



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

Algorithm 1 SYZGY_BASECASE(φ, G, \preceq, L)

Input:

- a linear functional $\varphi : \mathcal{R}^n \rightarrow \mathbb{K}$,
- a matrix G in $\mathcal{R}^{k \times n}$ with rows $\mathbf{g}_1, \dots, \mathbf{g}_k \in \mathcal{R}^n$,
- a monomial order \preceq on \mathcal{R}^m ,
- a list $\mathbf{K} = (\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_k)$ of elements of $\text{Mon}(\mathcal{R}^m)$.

Output:







- a matrix Q in $\mathcal{R}^{(k+\ell-1) \times k}$ for some $\ell \in \{0, \dots, r\}$,
 - a list L of $k + \ell - 1$ elements of $\text{Mon}(\mathcal{R}^k)$.
- 1: $(v_1, \dots, v_k) \leftarrow (\varphi(\mathbf{g}_1), \dots, \varphi(\mathbf{g}_k)) \in \mathbb{K}^k$  if $\phi(\text{PF}) = 0$
 - 2: **if** $(v_1, \dots, v_k) = (0, \dots, 0)$ **then return** (I_k, \mathbf{K})  **indeed in this case**
ker(ϕ) $\cap \mathbf{N} = \mathbf{N}$
 - 3: $\preceq_{\mathbf{K}} \leftarrow \text{SCHREYERORDER}(\preceq, \mathbf{K})$
 - 4: $\pi \leftarrow \arg \min_{\preceq_{\mathbf{K}}} \{\mathbf{e}_i \mid 1 \leq i \leq k, v_i \neq 0\}$ \triangleright the index i such that
 $v_i \neq 0$ which minimizes \mathbf{e}_i with respect to $\preceq_{\mathbf{K}}$
 - 5: $\{j_1 < \dots < j_\ell\} \leftarrow \{j \in \{1, \dots, r\} \mid X_j \boldsymbol{\mu}_\pi \notin \langle \boldsymbol{\mu}_i, i \neq \pi \rangle\}$
 - 6: $\alpha_{j_s} \leftarrow \varphi(X_{j_s} \mathbf{g}_\pi) / v_\pi$ for $1 \leq s \leq \ell$
 - 7: $\lambda_i \leftarrow -v_i / v_\pi$ for $1 \leq i < \pi$ and $\pi < i \leq k$
 - 8: $Q \leftarrow$ matrix in $\mathcal{R}^{(k+\ell-1) \times k}$ as in Eq. (3)
 - 9: $L \leftarrow (\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_{\pi-1}, X_{j_1} \boldsymbol{\mu}_\pi, \dots, X_{j_\ell} \boldsymbol{\mu}_\pi, \boldsymbol{\mu}_{\pi+1}, \dots, \boldsymbol{\mu}_k)$
 - 10: **return** (Q, L)
-

Algorithm 1 SYZGY_BASECASE(φ, G, \preceq, L)

Input:

- a linear functional $\varphi : \mathcal{R}^n \rightarrow \mathbb{K}$,
- a matrix G in $\mathcal{R}^{k \times n}$ with rows $\mathbf{g}_1, \dots, \mathbf{g}_k \in \mathcal{R}^n$,
- a monomial order \preceq on \mathcal{R}^m ,
- a list $\mathbf{K} = (\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_k)$ of elements of $\text{Mon}(\mathcal{R}^m)$.

Output:

- a matrix Q in $\mathcal{R}^{(k+\ell-1) \times k}$ for some $\ell \in \{0, \dots, r\}$,
 - a list L of $k + \ell - 1$ elements of $\text{Mon}(\mathcal{R}^k)$.
- 1: $(v_1, \dots, v_k) \leftarrow (\varphi(\mathbf{g}_1), \dots, \varphi(\mathbf{g}_k)) \in \mathbb{K}^k$
 - 2: **if** $(v_1, \dots, v_k) = (0, \dots, 0)$ **then return** (I_k, \mathbf{K})
 - 3: $\preceq_{\mathbf{K}} \leftarrow \text{SCHREYERORDER}(\preceq, \mathbf{K})$  Schreyer order
 - 4: $\pi \leftarrow \arg \min_{\preceq_{\mathbf{K}}} \{\mathbf{e}_i \mid 1 \leq i \leq k, v_i \neq 0\}$  \triangleright the index i such that $v_i \neq 0$ which minimizes \mathbf{e}_i with respect to $\preceq_{\mathbf{K}}$  pivot
 - 5: $\{j_1 < \dots < j_\ell\} \leftarrow \{j \in \{1, \dots, r\} \mid X_j \boldsymbol{\mu}_\pi \notin \langle \boldsymbol{\mu}_i, i \neq \pi \rangle\}$ 
 - 6: $\alpha_{j_s} \leftarrow \varphi(X_{j_s} \mathbf{g}_\pi) / v_\pi$ for $1 \leq s \leq \ell$ 
 - 7: $\lambda_i \leftarrow -v_i / v_\pi$ for $1 \leq i < \pi$ and $\pi < i \leq k$  here we define the good EGB
 - 8: $Q \leftarrow$ matrix in $\mathcal{R}^{(k+\ell-1) \times k}$ as in Eq. (3)
 - 9: $L \leftarrow (\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_{\pi-1}, X_{j_1} \boldsymbol{\mu}_\pi, \dots, X_{j_\ell} \boldsymbol{\mu}_\pi, \boldsymbol{\mu}_{\pi+1}, \dots, \boldsymbol{\mu}_k)$
 - 10: **return** (Q, L)
-

The output matrix \mathbf{Q}

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

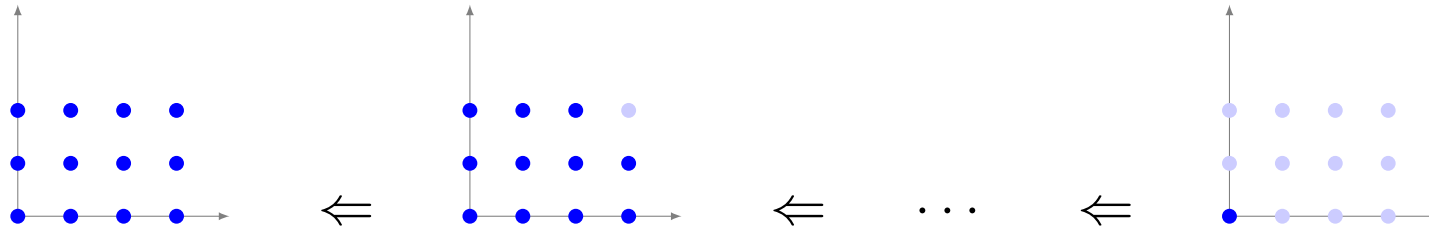
$$R^{(k+\ell-1) \times k} \ni \mathbf{Q} = \left[\begin{array}{ccc} \mathbf{I}_{\pi-1} & \lambda_1 & \\ & X_{j_1} - \alpha_{j_1} & \\ & \vdots & \\ & X_{j_\ell} - \alpha_{j_\ell} & \\ & \lambda_2 & \mathbf{I}_{m-\pi} \end{array} \right] \left. \vphantom{\begin{array}{ccc} \mathbf{I}_{\pi-1} & \lambda_1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

Theorem. Assume that $\langle \mathbf{EP} \rangle \neq \langle \mathbf{P} \rangle$ and that \mathbf{P} is a minimal \preceq -Gröbner basis. Let $j_1 < \cdots < j_\ell$ 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 $\mathbf{F} \in R^{m \times n}$, order \preccurlyeq

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

```

$$P \leftarrow I_m \in R^{m \times m}; G \leftarrow F; L \leftarrow (\mathbf{e}_1, \dots, \mathbf{e}_m) = \text{lm}_{\preccurlyeq}(P)$$
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 SYZGYG_Y_BASECASE( $\varphi_i, G, \preceq, K$ )  
 $(Q_1, L_1) \leftarrow$  SYZGYG_Y_DAC( $\varphi_1, \dots, \varphi_{\lfloor D/2 \rfloor}, G, \preceq, K$ )  
 $(Q_2, L_2) \leftarrow$  SYZGYG_Y_DAC( $\varphi_{\lfloor D/2 \rfloor + 1}, \dots, \varphi_D, Q_1 G, \preceq, L_1$ )  
return  $(Q_2 Q_1, L_2)$ 
```

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

Theorem. Assume \mathbf{P} is minimal \preceq -Gröbner basis of $\text{Syz}_{\mathcal{M}}(\mathbf{F})$ $G = \mathbf{P}\mathbf{F}$, $\text{Im}_{\preceq}(\mathbf{P}) = (\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_k)$, and $\mathcal{N}_i \cap \mathcal{M}$ is R -module for $1 \leq i \leq D$, ($\mathcal{N}_i = \bigcap_{1 \leq j \leq i} \ker(\varphi_j)$).

Then the output (Q, L) is such that $Q\mathbf{P}$ is a minimal \preceq -Gröbner basis of $\text{Syz}_{\mathcal{N}_D \cap \mathcal{M}}(\mathbf{F})$ and $L = \text{Im}_{\preceq}(Q\mathbf{P})$. [$\mathcal{M} = R^n$ and $\mathbf{P} = \mathbf{I}_m$ for orig. prob.]

Bivariate Padé

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

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

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 $\text{Syz}_{\mathcal{N}}(\mathbf{F})$ using

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

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

Related work

$D = \dim_K(R^n/\mathcal{N})$, r variables

Univariate case

Beckermann '92

Beckermann-Labahn '94

Neiger-Vu '17

$$O^{\sim}(m^{\omega} D)$$
$$O^{\sim}(m^{\omega-1} D)$$

(M-Padé)
(Hermite-Padé X^D)
(in-out size $O(m D)$)

Change of monomial ordering

FGLM '93

FGHR '14, Neiger '16

$$O(r D^3)$$

$$O^{\sim}(r D^{\omega})$$

(assuming mult. mat.)

Dual description via functionals

BM '82, MMM '92

O'Keefe-Fitzpatrick '97,'02

$$O(r D^3 + f r D^2)$$

$$O(r D^3)$$

(D functionals)
(appl. coding theory)

Combinatorial algorithms (LEX)

Cerlienco-Mureddu '93, Mora-Ceria '18

Linear recurrent sequences

Berlekamp-Massey '68, Sakata '88

Berthomieu-Faugère '15-

Mourrain '17

Conclusion

Computation of GB of syzygies in R^n/\mathcal{N}

Incorporating polynomial matrix multiplication

Complexity bounds for bivariate Padé

To appear in the Proc. of ISSAC 2020

Arxiv link : <https://arxiv.org/abs/2002.06404>