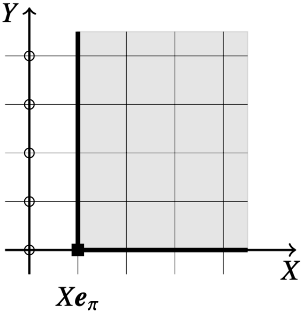
Gröbner bases of syzygies and polynomial matrix multiplication

Algebraic rewriting seminar

Simone Naldi (jw V. Neiger)
XLIM – Université de Limoges

December 6th, 2021



xlim INSTITUT DE RECHERCHE Université de Limoges Université de Poitiers cnrs

General context and notation

K *field*

General context and notation

K *field*

$R = K[X_1, X_2, \ldots, X_r]$ *ring of r-variate polynomials over K*

General context and notation

K	*field*
$R = K[X_1, X_2, \ldots, X_r]$	*ring of r-variate polynomials over K*
$\mathcal{M} \subset R^n$	*R-submodule of R^n*

General context and notation

K *field*

$R = K[X_1, X_2, \ldots, X_r]$ *ring of r-variate polynomials over K*

$\mathcal{M} \subset R^n$ *R-submodule of R^n*

$D = \dim_K(R^n/\mathcal{M})$ *co-dimension*

General context and notation

K	*field*
$R = K[X_1, X_2, \ldots, X_r]$	*ring of r-variate polynomials over K*
$\mathcal{M} \subset R^n$	*R-submodule of R^n*
$D = \dim_K(R^n/\mathcal{M})$	*co-dimension*
$\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m \in R^n/\mathcal{M}$	*input elements (row vectors)*

General context and notation

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

General context and notation

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

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

$$p_1 \boldsymbol{f}_1 + \cdots + p_m \boldsymbol{f}_m = \boldsymbol{0}$$

General context and notation

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

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

$$p_1 \boldsymbol{f}_1 + \cdots + p_m \boldsymbol{f}_m = \boldsymbol{0} \pmod{\mathcal{M}}$$

General context and notation

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

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

$$p_1 \boldsymbol{f}_1 + \cdots + p_m \boldsymbol{f}_m = \boldsymbol{0} \pmod{\mathcal{M}}$$

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

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

Hermite-Padé approximation

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

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

$$f = \frac{p_2}{p_1} \mod X^d$$

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

$$f = \frac{p_2}{p_1} \mod X^d \qquad (\Longleftrightarrow \begin{bmatrix} p_1 & p_2 \end{bmatrix} \begin{bmatrix} f \\ -1 \end{bmatrix} = 0)$$

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

$$f = \frac{p_2}{p_1} \mod X^d \qquad \left(\iff \begin{bmatrix} p_1 & p_2 \end{bmatrix} \begin{bmatrix} f \\ -1 \end{bmatrix} = 0\right)$$

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

$$\boldsymbol{p}\,\boldsymbol{F} = \begin{bmatrix} p_1 & \ldots & p_m \end{bmatrix} \begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix} = 0 \mod X^d$$

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

$$f = \frac{p_2}{p_1} \mod X^d \qquad \left(\iff \begin{bmatrix} p_1 & p_2 \end{bmatrix} \begin{bmatrix} f \\ -1 \end{bmatrix} = 0\right)$$

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

$$\boldsymbol{p}\,\boldsymbol{F} = \begin{bmatrix} p_1 & \ldots & p_m \end{bmatrix} \begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix} = 0 \mod X^d$$

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

Hermite-Padé approximation (module)

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

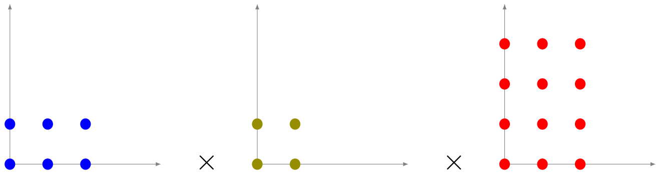
$$\mathcal{M} = \langle X^3, Y^2 \rangle \times \langle X^2, Y^2 \rangle \times \langle X^3, Y^4 \rangle$$

Hermite-Padé approximation (module)

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

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

$R^3/\mathcal{M} \sim$



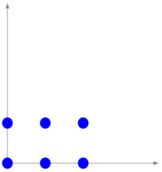
$$D = \mathbf{6} + \mathbf{4} + \mathbf{12}$$

Hermite-Padé approximation (module)

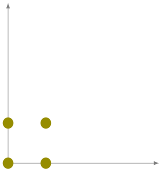
$\mathcal{M} = I_1 \times \cdots \times I_n$ where each ideal I_i is a "box"

$$\mathcal{M} \;=\; {\color{blue}\langle X^3, Y^2\rangle} \;\times\; {\color{olive}\langle X^2, Y^2\rangle} \;\times\; {\color{red}\langle X^3, Y^4\rangle}$$

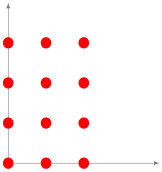
$R^3/\mathcal{M} \;\sim$



$\times$



$\times$



$$D \;=\; {\color{blue}\mathbf{6}} + {\color{olive}\mathbf{4}} + {\color{red}\mathbf{12}}$$

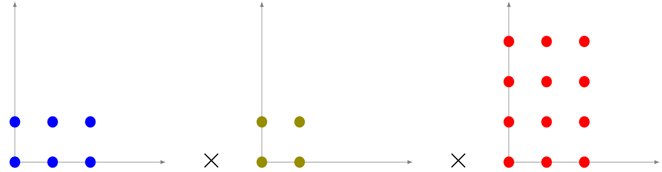
$$p_1[{\color{blue}f_{11}}, {\color{olive}f_{12}}, {\color{red}f_{13}}] + \cdots + p_m[{\color{blue}f_{m1}}, {\color{olive}f_{m2}}, {\color{red}f_{m3}}] = 0$$

Hermite-Padé approximation (module)

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

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

$R^3/\mathcal{M} \;\sim$



$$D \;=\; \mathbf{6} + \mathbf{4} + \mathbf{12}$$

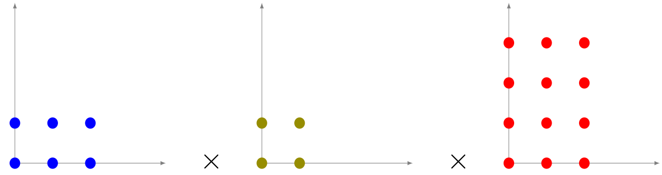
$$p_1[f_{11}, f_{12}, f_{13}] + \;\cdots\; + \;p_m[f_{m1}, f_{m2}, f_{m3}] = 0 \mod \langle X^3, Y^2 \rangle$$

Hermite-Padé approximation (module)

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

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

$$R^3/\mathcal{M} \;\sim$$



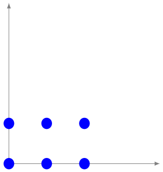
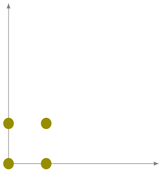
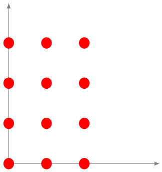
$$D \;=\; \mathbf{6} + \mathbf{4} + \mathbf{12}$$

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

Hermite-Padé approximation (module)

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

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

$R^3/\mathcal{M} \;\sim$  $\times$  $\times$ 

$$D \;=\; \mathbf{6} + \mathbf{4} + \mathbf{12}$$

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

Interpolation

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

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

Interpolation

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

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

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

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

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

Interpolation

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 $\boldsymbol{p} = (p_1, \dots, p_m)$ such that

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

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

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

Interpolation

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

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

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

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

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

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

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

- For every ideal I, one has $\mathrm{Syz}_I(1) = I$ (not only ideals of points)

Interpolation

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 $\boldsymbol{p} = (p_1, \dots, p_m)$ such that

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

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

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

- For every ideal I, one has $\mathrm{Syz}_I(1) = I$ (not only ideals of points)
- An algorithm that computes a GB of $\mathrm{Syz}_I(1)$ computes a GB of I

Interpolation

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

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

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

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

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

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

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

- For every ideal I, one has $\mathrm{Syz}_I(1) = I$ (not only ideals of points)
- An algorithm that computes a GB of $\mathrm{Syz}_I(1)$ 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 $\varphi_j : R^n \to K$, $j = 1, \ldots, D$ s.t.

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

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

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.

Input representation

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

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

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

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

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, $I(\{\alpha_1, \ldots, \alpha_D\})$ can be constructed by adding the points iteratively

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

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!) :

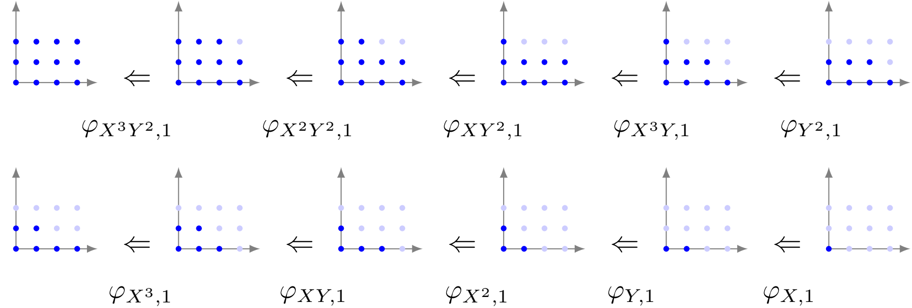
$\mathcal{M} = \langle X_1^{d_{11}}, \ldots, X_r^{d_{1r}} \rangle \times \cdots \times \langle X_1^{d_{n1}}, \ldots, X_r^{d_{nr}} \rangle \subseteq R^n$
The functionals are $\varphi_{\mu,i}(\cdot) = \text{coeff}(\cdot, \mu \boldsymbol{e}_i)$, for $\mu \boldsymbol{e}_i$ in the *escalier* of $\mathcal{M}$

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!) :

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

The functionals are $\varphi_{\mu,i}(\cdot) = \mathrm{coeff}(\cdot, \mu \boldsymbol{e}_i)$, for $\mu \boldsymbol{e}_i$ in the *escalier* of $\mathcal{M}$

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



Gröbner bases and syzygies

Monomials of R^n are of the form $\mu \boldsymbol{e}_i$ where μ is a ring monomial and $\boldsymbol{e}_i$ is the i-th element of the canonical basis.

Gröbner bases and syzygies

Monomials of R^n are of the form $\mu \boldsymbol{e}_i$ where μ is a ring monomial and $\boldsymbol{e}_i$ 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 $\langle \mathrm{lm}_{\preccurlyeq}(G) \rangle = \langle \mathrm{lm}_{\preccurlyeq}(\mathcal{N}) \rangle$

Gröbner bases and syzygies

Monomials of R^n are of the form $\mu \boldsymbol{e}_i$ where μ is a ring monomial and $\boldsymbol{e}_i$ 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 $\langle \mathrm{lm}_{\preccurlyeq}(G) \rangle = \langle \mathrm{lm}_{\preccurlyeq}(\mathcal{N}) \rangle$

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

Gröbner bases and syzygies

Monomials of R^n are of the form $\mu \boldsymbol{e}_i$ where μ is a ring monomial and $\boldsymbol{e}_i$ 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 $\langle \mathrm{lm}_{\preccurlyeq}(G) \rangle = \langle \mathrm{lm}_{\preccurlyeq}(\mathcal{N}) \rangle$

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

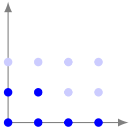
Let $\preccurlyeq$ and $L = (\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_m)$ be a term order and a list of monomials of R^n. We say that $\preccurlyeq_L$ is a *Schreyer order for* $\preccurlyeq$ *and* L if

$$\nu_1 \boldsymbol{\mu}_i \prec \nu_2 \boldsymbol{\mu}_j \implies \nu_1 \boldsymbol{e}_i \prec_L \nu_2 \boldsymbol{e}_j$$

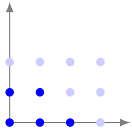
for all ν_1, ν_2 ring monomials, and $i, j = 1, \ldots, m$.

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

One step of the iteration



$$\xleftarrow[\varphi_{X^3,1}]{}$$



$\mathcal{N} \subset R^n$ is a given $R-$ module $\qquad \mathcal{N} = \langle X^3, X^2Y, Y^2 \rangle$

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

$\varphi : R^n \to K$ linear, such that $\ker(\varphi) \cap \mathcal{N}$ is module $\qquad \varphi = \varphi_{X^3,1}$

we know a Gröbner basis $\mathbf{P}$ of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ $\qquad \mathrm{Syz}_{\langle X^3,X^2Y,Y^2 \rangle}(\boldsymbol{F})$

Goal : compute a GB of $\mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{F})$ $\qquad \mathrm{Syz}_{\langle X^4,X^2Y,Y^2 \rangle}(\boldsymbol{F})$

Elementary Gröbner bases

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

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

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

Elementary Gröbner bases

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

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

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

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

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

Elementary Gröbner bases

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

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

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

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

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

Theorem. (GB of codimension 1 modules)

▶ If $\dim_K(R^m/\mathcal{M}) = 1$, for every $\preccurlyeq$ the $\preccurlyeq$ −reduced GB of $\mathcal{M}$ has the form (1), with with $\lambda_i = 0$ if $\boldsymbol{e}_i \prec \boldsymbol{e}_\pi$ 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 $\boldsymbol{e}_i \prec \boldsymbol{e}_\pi$ for all $i \neq \pi$.

One-step algorithm (sketch)

Soit $\boldsymbol{G} = \boldsymbol{P}\boldsymbol{F} = (\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k)$, and we know that this is zero modulo $\mathcal{N}$.

One-step algorithm (sketch)

Soit $\boldsymbol{G} = \boldsymbol{P}\boldsymbol{F} = (\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k)$, and we know that this is zero modulo $\mathcal{N}$.

We evaluate $(\varphi(\boldsymbol{g}_1), \ldots, \varphi(\boldsymbol{g}_k)) =: (v_1, \ldots, v_k)$. If this is zero, one deduces $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F}) = \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{F})$.

One-step algorithm (sketch)

Soit $\boldsymbol{G} = \boldsymbol{P}\boldsymbol{F} = (\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k)$, and we know that this is zero modulo $\mathcal{N}$.

We evaluate $(\varphi(\boldsymbol{g}_1), \ldots, \varphi(\boldsymbol{g}_k)) =: (v_1, \ldots, v_k)$. If this is zero, one deduces $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F}) = \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{F})$.

Otherwise, we define some well-chosen vectors

$\preccurlyeq_{\boldsymbol{K}} \leftarrow \textsc{SchreyerOrder}(\preccurlyeq, \boldsymbol{K})$
$\pi \leftarrow \arg\min_{\preccurlyeq_{\boldsymbol{K}}} \{\boldsymbol{e}_i \mid 1 \le i \le k, v_i \neq 0\}$ ▷ *the index i such that $v_i \neq 0$ which minimizes $\boldsymbol{e}_i$ with respect to $\preccurlyeq_{\boldsymbol{K}}$*
$\{j_1 < \cdots < j_\ell\} \leftarrow \{j \in \{1, \ldots, r\} \mid X_j \boldsymbol{\mu}_\pi \notin \langle \boldsymbol{\mu}_i, i \neq \pi \rangle\}$
$\alpha_{j_s} \leftarrow \varphi(X_{j_s} \boldsymbol{g}_\pi)/v_\pi$ for $1 \le s \le \ell$
$\lambda_i \leftarrow -v_i/v_\pi$ for $1 \le i < \pi$ and $\pi < i \le k$

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

$$\langle \mathbf{E} \rangle = \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{P}\boldsymbol{F})$$

One-step algorithm (sketch, cont'd)

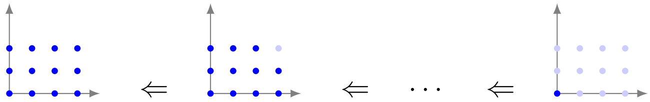
Finally we output the following matrix $\mathbf{Q}$ (a submatrix of $\mathbf{E}$)

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

so that we have this result:

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

Sequential algorithm



The base case described above can be iterated as follows:

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

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

$\boldsymbol{P} \leftarrow \boldsymbol{I}_m \in \mathcal{R}^{m \times m}$; $\boldsymbol{G} \leftarrow \boldsymbol{F}$; $\boldsymbol{L} \leftarrow (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m) = \mathrm{lm}_{\preccurlyeq}(\boldsymbol{P})$
for $i = 1, \ldots, D$ **do**
    $(\boldsymbol{Q}, \boldsymbol{L}) \leftarrow \textsc{Syzygy\_BaseCase}(\varphi_i, \boldsymbol{G}, \preccurlyeq, \boldsymbol{L})$
    $\boldsymbol{P} \leftarrow \boldsymbol{Q}\boldsymbol{P}$; $\boldsymbol{G} \leftarrow \boldsymbol{Q}\boldsymbol{G}$
return $\boldsymbol{P}$

Divide-and-conquer algorithm

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

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

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

if $D = 1$ **then return** $\textsc{Syzygy\_BaseCase}(\varphi_i, \boldsymbol{G}, \preccurlyeq, \boldsymbol{K})$
$(\boldsymbol{Q}_1, \boldsymbol{L}_1) \leftarrow \textsc{Syzygy\_DaC}(\varphi_1, \ldots, \varphi_{\lfloor D/2 \rfloor}, \boldsymbol{G}, \preccurlyeq, \boldsymbol{K})$
$(\boldsymbol{Q}_2, \boldsymbol{L}_2) \leftarrow \textsc{Syzygy\_DaC}(\varphi_{\lfloor D/2 \rfloor + 1}, \ldots, \varphi_D, \boldsymbol{Q}_1\boldsymbol{G}, \preccurlyeq, \boldsymbol{L}_1)$
return $(\boldsymbol{Q}_2\boldsymbol{Q}_1, \boldsymbol{L}_2)$

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

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

Theorem. The algorithm computes a minimal $\preccurlyeq$-GB of $\operatorname{Syz}_{\mathcal{M}}(\boldsymbol{F})$ using

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

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

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

Theorem. The algorithm computes a minimal $\preccurlyeq$-GB of $\mathrm{Syz}_{\mathcal{M}}(\boldsymbol{F})$ using

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

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

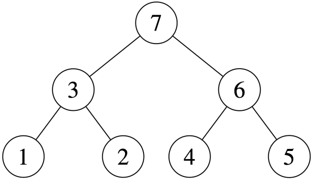
For $m = 2, n = 1, d = e$ (classical Padé) this complexity is of the order $O\tilde{}(d^{\omega+2}) = O\tilde{}(D^{\frac{\omega+2}{2}})$, and the approach by linear algebra (Vincent's talk) gives $O\tilde{}(D^{\omega})$.

One example I

We want to compute syzygies of

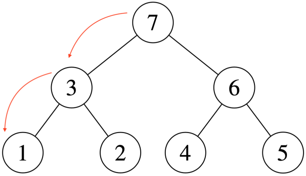
$$\boldsymbol{F} = \begin{bmatrix} 1 \\ -1 \end{bmatrix} \in K[X,Y]^{2\times 1}$$

modulo the ideal $I = \langle X^2, Y^2 \rangle$.
I assume $K[X,Y]$ with the lexicographic order $\preccurlyeq_{\mathrm{lex}}$ with $Y \preccurlyeq_{\mathrm{lex}} X$ and let $\preccurlyeq$ be the term over position order $\preccurlyeq_{\mathrm{lex}}^{\mathrm{top}}$.
The algorithm organises the steps in a tree of the form



One example II

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



- Padé$(1, 1, \boldsymbol{F}, \preccurlyeq, L)$ on *step 1*: The output is computed with the "base case algorithm" with functional $\varphi(f) = coeff(f, 1)$:

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

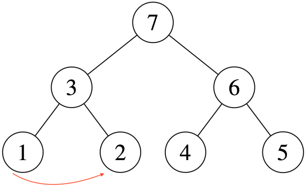
and its leading terms $L_1 = ((X, 0), (Y, 0), (0, 1))$.

One example III

- Back to *Node 3*, we compute the "residual"

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

Next we call Padé$(1, 1, \boldsymbol{G}_2, \preccurlyeq, L_1)$, 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

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

and go to (*Node 6*).

One example V

- *Node 6* has in input $(2, 1, \widehat{\boldsymbol{G}}_2, \preccurlyeq, L_2)$, 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 $\preccurlyeq$-Gröbner basis of syzygies for $\boldsymbol{F}$ modulo $\langle X^2, Y^2 \rangle$.

References

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