On the computation of algebraic relations of bivariate polynomials
(and application to the moment problem)

work in progress by

Simone Naldi, Vincent Neiger and Grace Younes

Applications of Computer Algebra
June 2018 – Santiago de Compostela

General context

Given a $K[\mathbf{X}]$–module $\mathcal{M} \subset K[\mathbf{X}]^n$, $\mathbf{X} = (X_1, \ldots, X_r)$
and elements $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m \in K[\mathbf{X}]^n/\mathcal{M}$

Compute elements $p_1, \ldots, p_m \in K[\mathbf{X}]$ such that

$$p_1\boldsymbol{f}_1 + \cdots + p_m\boldsymbol{f}_m = 0 \text{ in } K[\mathbf{X}]^n/\mathcal{M}$$

Often we use the compact notation $P\boldsymbol{F} \in \mathcal{M}$ with

$P = 1 \times m$ vector of $p_1, \ldots, p_m$

$\boldsymbol{F} = m \times 1$ column vector of (row vectors) $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m$
$= m \times n$ polynomial matrix, that is $\boldsymbol{F} \in K[\mathbf{X}]^{m\times n}$

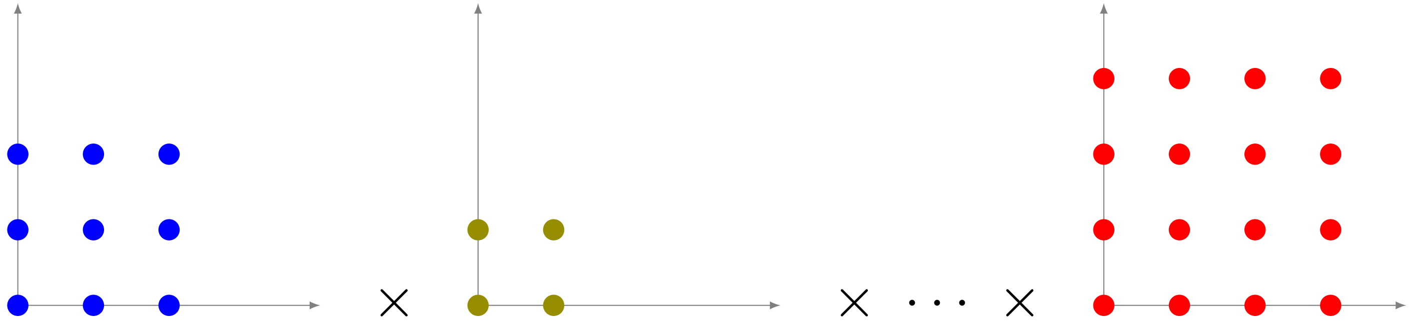
Concrete situation

$K[\mathbf{X}]^n/\mathcal{M}$ is a finite-dimensional $K-$vector space:

$$D = \dim_K(K[\mathbf{X}]^n/\mathcal{M}) < +\infty$$

For instance $\mathcal{M} = I_1 \times \cdots \times I_n$ with $I_i \subset K[\mathbf{X}]$ $0-$dim ideal

Interesting basic case: products of boxes



$$K[\mathbf{X}]^n/\mathcal{M} \sim \quad \times \quad \times \cdots \times$$

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

Special cases

Rational reconstruction $[r=1, n=1]$

given $f, g \in K[X]_D$, find $p_1, p_2 \in K[X]_{D/2}$:

$$f = p_1/p_2 \bmod \langle g \rangle$$

(*Padé approximation* $g = X^D$)

Hermite-Padé approximation $[r=2, n=1]$

given $f_i \in K[X,Y]/\langle X^d, Y^d \rangle$, find $p_i \in K[X,Y]_{(d/\sqrt{m}, d/\sqrt{m})}$:

$$p_1 f_1 + \cdots + p_m f_m \in \langle X^d, Y^d \rangle$$

Modular inversion $[n=1]$

$$pf = 1 \text{ in } K[\mathbf{X}]/I$$

Structured linear algebra over K

Computing one relation $P \in K[\mathbf{X}]^m$ is a linear algebra problem : For instance, say we look for a, b satisfying

$$au + bv \in \left\langle X^D \right\rangle$$

given polynomials u, v. This corresponds to solving a truncated block-Hankel linear system over K

$$\begin{bmatrix} & & & u_0 & & & & v_0 \\ & & u_0 & u_1 & & & v_0 & v_1 \\ & \iddots & & \vdots & & \iddots & & \vdots \\ u_0 & & & & v_0 & & & \\ \vdots & & & \vdots & \vdots & & & \vdots \\ u_{D/2-1} & \cdots & u_{D-2} & u_{D-1} & v_{D/2-1} & \cdots & v_{D-2} & v_{D-1} \end{bmatrix} \begin{bmatrix} a_{D/2} \\ \vdots \\ a_0 \\ b_{D/2} \\ \vdots \\ b_0 \end{bmatrix} = 0$$

Structured linear algebra over K

$$au + \cdots \in \left\langle X^d, Y^d \right\rangle$$

$$\begin{bmatrix} & & & & & & & & u_{00} \\ & & & & & & & u_{00} & u_{10} \\ & & & & & & u_{00} & u_{10} & u_{20} \\ & & & & & u_{00} & & & u_{01} \\ & & & & u_{00} & u_{10} & & u_{01} & u_{11} \\ & & & u_{00} & u_{10} & u_{20} & u_{01} & u_{11} & u_{21} \\ & & u_{00} & & & u_{01} & & & u_{02} \\ & u_{00} & u_{10} & & u_{01} & u_{11} & & u_{02} & u_{12} \\ u_{00} & u_{10} & u_{20} & u_{01} & u_{11} & u_{21} & u_{02} & u_{12} & u_{22} \end{bmatrix} \begin{bmatrix} a_{22} \\ a_{12} \\ a_{02} \\ a_{21} \\ a_{11} \\ a_{01} \\ a_{20} \\ a_{10} \\ a_{00} \end{bmatrix} = 0$$

Recently : Bostan-Jeannerod-Mouilleron-Schost '17

↪ $O^{\sim}(\alpha^{\omega-1} D)$ matrices with displacement rank α

Algorithmic problem

The kernel of the morphism of modules

$$\begin{array}{rrcl} \varphi : & K[\mathbf{X}]^m & \longrightarrow & K[\mathbf{X}]^n/\mathcal{M} \\ & (p_1, \ldots, p_m) & \longmapsto & p_1 \boldsymbol{f}_1 + \cdots + p_m \boldsymbol{f}_m \end{array}$$

is the module of relations mod $\mathcal{M}$:

$$\mathrm{Rel}_{\mathcal{M}}(\boldsymbol{F}) = \left\{ P = (p_1, \ldots, p_m) \in K[\mathbf{X}]^m : P\boldsymbol{F} \in \mathcal{M} \right\}$$

It holds that $\dim(K[\mathbf{X}]^m/\mathrm{Rel}_{\mathcal{M}}(\boldsymbol{F})) \leq D < +\infty$.

General goal :

compute a Groebner basis of $\mathrm{Rel}_{\mathcal{M}}(\boldsymbol{F}) = \ker \varphi$

for a given term order $\prec$ (that may be chosen according to degree constraints on $p_1, \ldots, p_m$)

Related work

$D = \dim_K(K[\mathbf{X}]^n/\mathcal{M})$
r = numb. of var. $X_1, \ldots, X_r$

Change of monomial ordering

FGLM '93	$O(r\,D^3)$	
FGHR '14, Neiger '16	$O^{\sim}(r\,D^{\omega})$	(assuming mult. mat.)

Dual description via functionals

BM '82, MMM '92	$O(r\,D^3 + f r D^2)$	(D functionals)
O'Keeffe-Fitzpatrick '97,'02	$O(r\,D^3)$	(appl. coding theory)

Univariate case

Beckermann-Labahn '94	$O^{\sim}(m^{\omega}\,D)$	(Hermite-Padé X^D)
Neiger-Vu '17	$O^{\sim}(m^{\omega-1}\,D)$	(in-out size $O(m\,D)$)

Example

Consider the Padé approximation over $K = \mathbb{Z}/5\mathbb{Z}$:

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

A trivial relation : $P = \begin{bmatrix} X^6 & 0 & 0 & 0 \end{bmatrix}$

A GB (TOP order) of $\mathrm{Rel}_{\langle X^6 \rangle}(F)$ is at most quadratic :

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

A structured example

We want to compute all relations between the rows of

$$F = \begin{bmatrix} 2 & a+b & a^2+b^2 & a^3+b^3 \\ a+b & a^2+b^2 & a^3+b^3 & a^4+b^4 \\ a^2+b^2 & a^3+b^3 & a^4+b^4 & a^5+b^5 \\ a^3+b^3 & a^4+b^4 & a^5+b^5 & a^6+b^6 \end{bmatrix}$$

For $\mathcal{M} = K[a,b]^4$ a GB is given by

$$P = \begin{bmatrix} ab & -a-b & 1 & \\ & ab & -a-b & 1 \end{bmatrix} = \begin{bmatrix} ab\,\mathbf{e}_1 - (a+b)\mathbf{e}_2 + \mathbf{e}_3 \\ ab\,\mathbf{e}_2 - (a+b)\mathbf{e}_3 + \mathbf{e}_4 \end{bmatrix}$$

Morally, we compute only 1 element : $ab\,\mathbf{e}_i - (a+b)\mathbf{e}_{i+1} + \mathbf{e}_{i+2}$.

Towards a divide-and-conquer algorithm

Suppose:

1. $\mathcal{M}_2 \subset \mathcal{M}_1 \subset K[\mathbf{X}]^m$ are $K[\mathbf{X}]$−modules.

$\mathcal{M}_2 = \langle X^4, Y^2\rangle \subset \langle X^2, Y^2\rangle = \mathcal{M}_1$

2. $\mathscr{G}_1 = \{P_1, \ldots, P_{m_1}\}$: $\langle \mathscr{G}_1 \rangle = \mathrm{Rel}_{\mathcal{M}_1}(\boldsymbol{F})$

$P_1\boldsymbol{F} \in \langle X^2, Y^2\rangle, \ldots, P_{m_1}\boldsymbol{F} \in \langle X^2, Y^2\rangle$

3. $\mathscr{G}_2 = \{Q_1, \ldots, Q_{m_2}\}$ such that $\langle \mathscr{G}_2 \rangle = \mathrm{Rel}_{\mathcal{M}_2}(\mathscr{G}_1\boldsymbol{F})$

Then $\langle \mathscr{G}_2\mathscr{G}_1 \rangle = \mathrm{Rel}_{\mathcal{M}_2}(\boldsymbol{F})$. Indeed, for $R \in \mathrm{Rel}_{\mathcal{M}_2}(\boldsymbol{F})$:

$Q_iP_j\boldsymbol{F} \in \langle X^4, Y^2\rangle$

$$R\boldsymbol{F} \in \mathcal{M}_2 \subset \mathcal{M}_1 \Rightarrow R = \Lambda\mathscr{G}_1 = \xi\mathscr{G}_2\mathscr{G}_1.$$

An example

$$\boldsymbol{F} = \begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = \begin{bmatrix} X^2 - 1 \\ Y - X^3 \end{bmatrix} \qquad \mathcal{M}_2 = \langle X^4, Y^2 \rangle \subset \langle X^2, Y^2 \rangle = \mathcal{M}_1$$

One has

$$\mathscr{G}_1 = \begin{bmatrix} Y & 1 \\ X^2 & 0 \\ 0 & Y \\ 0 & X^2 \end{bmatrix} \qquad \mathscr{G}_1 \boldsymbol{F} = \begin{bmatrix} YX^2 - X^3 \\ X^4 - X^2 \\ Y^2 - YX^3 \\ X^2Y - X^5 \end{bmatrix} \overset{\mathcal{M}_2}{=} \begin{bmatrix} YX^2 - X^3 \\ -X^2 \\ -YX^3 \\ X^2Y \end{bmatrix}$$

and

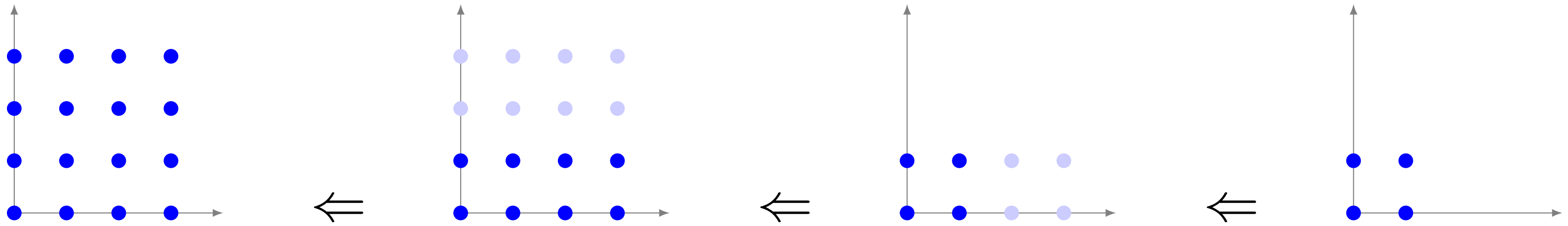
$$\mathscr{G}_2 = \begin{bmatrix} Y & 0 & -1 & 0 \\ X & 0 & 1 & 0 \\ 0 & Y & 0 & 1 \\ -1 & X & 0 & 1 \\ 0 & 0 & Y & 0 \\ 0 & 0 & X & 0 \\ 0 & 0 & 0 & Y \\ 0 & 0 & 1 & X \end{bmatrix} \qquad \mathscr{G}_2\mathscr{G}_1 = \begin{bmatrix} Y^2 & 0 \\ XY & X+Y \\ X^2Y & X^2 \\ X^3-Y & X^2-1 \\ 0 & Y^2 \\ 0 & XY \\ 0 & X^2Y \\ 0 & X^3+Y \end{bmatrix}$$

In this special case:

- $\mathscr{G}_1$ and $\mathscr{G}_2$ are TOP-GRLEX GB
- $\mathscr{G}_2\mathscr{G}_1$ is a (not reduced) TOP-GRLEX GB

We used a strategy that works for the case $r = 1$ (shifts)

Bivariate divide-and-conquer



Sketch of the algorithm (Groebner basis of $\mathrm{Rel}_{\langle X^d,Y^e\rangle}(\boldsymbol{F})$)

```
GBRel($(d,e)$,$\boldsymbol{F}$,$\prec$)                                      # top algorithm
    If $d = e = 1$ then BaseCase($\boldsymbol{F}$,$\prec$)        # base case mod $\langle X, Y\rangle$
    Else if $d > e$ then $\mathscr{G}_1 \leftarrow$ GBRel($(d/2,e)$,$\boldsymbol{F}$,$\prec$)    # recursion
                         $\boldsymbol{G} \leftarrow X^{-d/2}\mathscr{G}_1\boldsymbol{F}$                   # residual
                         $\prec_2 \leftarrow$ TO($\prec$)                # update term order
                         $\mathscr{G}_2 \leftarrow$ GBRel($(d/2,e)$,$\boldsymbol{G}$,$\prec_2$)      # residual
                         Return $\mathscr{G}_2\mathscr{G}_1$.
        Else $\mathscr{G}_1 \leftarrow$ GBRel($(d,e/2)$,$\boldsymbol{F}$,$\prec$)               # recursion
             $\boldsymbol{G} \leftarrow Y^{-e/2}\mathscr{G}_1\boldsymbol{F}$                              # residual
             ...
Return $\mathscr{G}_2\mathscr{G}_1$.
```

Moment problem

Given a multi-sequence $y = (y_\alpha)_{\alpha \in \mathbb{N}^n}$, compute a set $S \subset \mathbb{R}^n$ and a measure μ with support in S and such that

$$y_\alpha = \int_S X_1^{\alpha_1} \cdots X_n^{\alpha_n} \, \mathrm{d}\mu \quad \forall \, \alpha \in \mathbb{N}^n$$

Inverse problem with origin in *functional analysis*, crucial applications in *polynomial optimization*, *control theory*...

Example : $\mu = \delta_a + \delta_b$ will give the sequence of moments

$$y = (2, a+b, a^2+b^2, a^3+b^3, \ldots)$$

that can be represented with the rank-2 polynomial matrix

$$\left(\int_S X^{i+j} \, \mathrm{d}\mu \right) = \begin{bmatrix} 2 & a+b & a^2+b^2 & a^3+b^3 \\ a+b & a^2+b^2 & a^3+b^3 & a^4+b^4 \\ a^2+b^2 & a^3+b^3 & a^4+b^4 & a^5+b^5 \\ a^3+b^3 & a^4+b^4 & a^5+b^5 & a^6+b^6 \end{bmatrix}$$

Moment problem (continued)

In our context, we computed the GB of the rows of the matrix:

$$ab\,\mathbf{e}_1 - (a+b)\mathbf{e}_2 + \mathbf{e}_3$$

This element of the GB corresponds to the univariate polynomial that vanishes over the support of the solution measure :

$$T \mapsto ab - (a+b)T + T^2 = (T-a)(T-b)$$

Algebraic relation = solution to the **symbolic moment problem**

Open questions :

Size of the GB for the symbolic moment problem ?

Sufficient to solve it modulo a special $\mathcal{M} \subset K[a,b]^4$?

Complexity of the symbolic (modular) MP ?

Conclusion: What to retain?

Main problem : computing GB bases of relations mod $\mathcal{M}$

Contains as special case classical problems such as Hermite-Padé approximation, interpolation, modular inversion problems.

Some approaches that yield advances in the univariate case could be extended in many variables, for instance divide-and-conquer techniques in boxes $(K[\mathbf{X}]/\langle X^d, Y^d\rangle)^n$.

Open questions concern complexity bounds for the general bivariate or multi-variate problem (hoped $O\left((\#\mathscr{G})^{\omega-1}\, D\right)$), or structured situations such as the modular MP.

Special cases

Bivariate interpolation $[r = 2, n = 1]$

given $\{(x_1, y_1), \ldots, (x_D, y_D)\} \subset K^2$, $x_i \neq x_j$:

$$\text{find } Q(X,Y) \text{ s.t. } \quad Q(x_i, y_i) = 0, i = 1, \ldots, D$$

In the basis $\{\prod(X - x_i), Y - Lag(X)\}$ but the bi-degrees of the polynomials are unbalanced: $(D, 0)$ and $(D - 1, 1)$.

Can we get Q with $\deg Q \leq (\sqrt{D}, \sqrt{D})$?

This can be cast as a problem of type : find $Q_i(X)$ s.t.

$$Q_0 + Q_1(X)L(X) + \cdots + Q_\ell(X)L(X)^\ell \mod \langle \prod(X - x_i) \rangle .$$