Moment problems and border bases

B. Mourrain
GALAAD
INRIA Méditerranée

March 4, 2010

Notations:

- Monomials: $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for $\alpha \in \mathbb{N}^n$.
- Polynomials: $p = \sum_{\alpha \in A} p_\alpha \mathbf{x}^\alpha$ with coefficients p_α in $\mathbb{K}$ ($= \mathbb{R}$ or $\mathbb{C}$).
- Ring of polynomials: $R = \mathbb{K}[\mathbf{x}]$.
- Vector space of polynomials of degree $\leqslant t$: R_t.

Problem: *Given $f_1, \ldots, f_m \in R$, solve the equations $f_1(\mathbf{x}) = 0, \ldots, f_m(\mathbf{x}) = 0$ in $\mathbb{R}^n$ or $\mathbb{C}^n$.*

- Which minimal degree for linear algebra on the multiples of $f_1, \ldots, f_m$?
- Which systems of generator for $I = (f_1, \ldots, f_m)$?
- Which basis for $\mathcal{A} = R/I$?
- **Which representation for $\mathcal{A}^* = \mathrm{Hom}_{\mathbb{K}}(\mathcal{A}, \mathbb{K})$?**

Moment problems

Moment problem

We consider $\mathbb{K} = \mathbb{R}$.

Problem: *Given* $(\lambda_\alpha)_{\alpha\in A} \in \mathbb{R}^A$ *with* $A \subset \mathbb{N}^n$, $\lambda_{\mathbf{0}} > 0$ *and* S **a closed subset of** $\mathbb{R}^n$, *is there* **a Borel (positive) measure** μ *such that* $\forall \alpha \in A$,

$$\lambda_\alpha = \int \mathbf{x}^\alpha d\mu$$

and $\mathrm{supp}(\mu) \subset S$.

Global moment problem: $A = \mathbb{N}^n$

We associate to $(\lambda_\alpha)_{\alpha\in\mathbb{N}^n}$, $\Lambda \in \mathbb{R}[\mathbf{x}]^* := \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}[\mathbf{x}], \mathbb{R})$ defined by

$$\Lambda : p = \sum_{\alpha\in\mathbb{N}^n} p_\alpha \mathbf{x}^\alpha \mapsto \sum_{\alpha\in\mathbb{N}^n} p_\alpha \lambda_\alpha$$

Theorem (Riesz 1923, Haviland 1935)

If

$$\forall p \in \mathbb{R}[\mathbf{x}] \text{ s.t. } p_{|S} \geqslant 0, \Lambda(p) \geqslant 0$$

then there exists a Borel measure μ on $\mathbb{R}^n$ such that $\forall \alpha \in \mathbb{N}^n$, $\lambda_\alpha = \int \mathbf{x}^\alpha d\mu$ *and* $\mathrm{supp}(\mu) \subset S$.

Suppose that $S = \{x \in \mathbb{R}^n; g_1(x) \geqslant 0, \ldots, g_s(x) \geqslant 0\}$ for some polynomials $g_1, \ldots, g_s \in \mathbb{R}[\mathbf{x}]$.

Definition

The quadratic module of S is

$$\mathcal{M}(S) = \{\sigma_0 + \sigma_1 g_1 + \cdots + \sigma_s g_s \text{ for } \sigma_i \in \Sigma R^2\}$$

where ΣR^2 is the set of finite sums of squares of polynomials in R.

Theorem (Putinar 1993)

Suppose that $\rho - \|\mathbf{x}\|^2 \in \mathcal{M}(S)$ *for some* $\rho > 0$*. If* $\Lambda(1) = 1$ *and*

$$\forall p \in \mathcal{M}(S), \quad \Lambda(p) \geqslant 0$$

then there exists a probability measure μ *such that* $\forall \alpha \in \mathbb{N}^n$, $\lambda_\alpha = \int \mathbf{x}^\alpha d\mu$ *and* $\mathrm{supp}(\mu) \subset S$.

Truncated moment problems

Truncated moment problem $A_{2t} = \{\alpha \in \mathbb{N}^n; |\alpha| \leq 2t\}$.

Given $(\lambda_\alpha)_{\alpha \in A_{2t}}$, define $\Lambda \in \mathrm{Hom}_{\mathbb{K}}(R_{2t}, \mathbb{K}) = R_{2t}^*$ by $\Lambda(\mathbf{x}^\alpha) = \lambda_\alpha$.

Given $\Lambda \in \mathrm{Hom}_{\mathbb{K}}(R_{2t}, \mathbb{K}) = R_{2t}^*$, we define

$$\begin{array}{rcl} H_\Lambda^t : R_t & \to & R_t^* \\ q & \mapsto & q \cdot \Lambda \end{array}$$

where $q \cdot \Lambda \in \mathrm{Hom}_{\mathbb{K}}(R_t, \mathbb{K})$ is defined by

$$\forall p \in R_t, \quad q \cdot \Lambda(p) = \Lambda(pq).$$

The matrix of H_Λ^t in the monomial basis $(\mathbf{x}^\alpha)_{|\alpha| \leqslant t}$ and its dual basis $(\mathbf{d}^\alpha)_{|\alpha| \leqslant t}$ is

$$[H_\Lambda^t] = (\Lambda(\mathbf{x}^{\alpha+\beta}))_{|\alpha|,|\beta| \leqslant t}$$

If the truncated moment problem has a solution $\Lambda \in R^*$

Define

$$\begin{array}{rcl} H_\Lambda : R & \rightarrow & R^* \\ p & \mapsto & p \cdot \Lambda \end{array}$$

Properties:

- H_Λ extend H_Λ^t.
- $I_\Lambda := \ker H_\Lambda$ is an ideal of R.
- rank $H_\Lambda = r$ iff $\mathcal{A}_\Lambda = R/I_\Lambda$ is an algebra of dimension r over $\mathbb{K}$.
- If rank $H_\Lambda = r$, $\mathcal{A}_\Lambda$ is a Gorenstein algebra:
  1. $\mathcal{A}_\Lambda^* = \mathcal{A}_\Lambda \cdot \Lambda$ (free module of rank 1).
  2. $(a, b) \mapsto \Lambda(ab)$ is non-degenerate in $\mathcal{A}_\Lambda$.
  3. $\mathrm{Hom}_{\mathcal{A}_\Lambda}(\mathcal{A}_\Lambda^*, \mathcal{A}_\Lambda) = \mathcal{D} \cdot \mathcal{A}_\Lambda$ where $\mathcal{D} = \sum_{i=1}^r b_i \otimes \omega_i$ for $(b_i)_{1 \leqslant i \leqslant r}$ a basis of $\mathcal{A}_\Lambda$ and $(\omega_i)_{1 \leqslant i \leqslant r}$ its dual basis for Λ.

- If rank $H_\Lambda = r$, then

$$\Lambda : p \mapsto \sum_{i=1}^{r'} \delta_{\zeta_i} \cdot \theta_i(\partial_{x_1}, \ldots, \partial_{x_n})(p)$$

  for some $\zeta_i \in \mathbb{C}^n$ and some differential polynomials θ_i with
  - $r = \sum_{i=1}^{r'} \dim(\langle \partial_\partial^\alpha(\theta_i) \rangle)$
  - $V_\mathbb{C}(I_\Lambda) = \{\zeta_1, \ldots, \zeta_{r'}\}$.
- $H_\Lambda \succcurlyeq 0$ iff I_Λ is a real radical ideal.
- rank $H_\Lambda = r$ and $H_\Lambda \succcurlyeq 0$ iff $\Lambda = \sum_{i=1}^{r} \gamma_i \delta_{\zeta_i}$ with $\gamma_i > 0$ and ζ_i are distinct points of $\mathbb{R}^n$.
- If rank $H_\Lambda = r$, $(b_i)_{1 \leqslant i \leqslant r}$ a basis of $\mathcal{A}_\Lambda$ and $(\omega_i)_{1 \leqslant i \leqslant r}$ its dual basis for Λ then

$$\sqrt{I_\Lambda} = \ker H_{\Delta \cdot \Lambda}$$

  where $\Delta = \sum_{i=1}^{r} b_i \omega_i$.

Theorem (Curto-Fialkov 1996)

If

$$\mathrm{rank} H_\Lambda^t = \mathrm{rank} H_\Lambda^{t+1} = r, H_\Lambda^t \succcurlyeq 0$$

then there exists $\mu = \sum_{i=1}^r \gamma_i \delta_{\zeta_i}$ *where* $\gamma_i > 0$, $\zeta_i \in \mathbb{R}^n$ *such that* $\forall \alpha \in \mathbb{N}^n |\alpha| \leqslant 2t$, $\lambda_\alpha = \int \mathbf{x}^\alpha d\mu$.

The measure μ is supported in S iff $H_{g_i \cdot \Lambda}^t \succcurlyeq 0$, $i = 1, \ldots, s$.

For a vector space $E \subset R$,

- $E^+ := E + x_1 \cdot E + \cdots + x_n \cdot E$.
- E is connected to 1 if $\forall e \in E$, either $e \in \mathbb{K}$ or $e = e_0 + \sum_{i=1} x_i e_i$ with $\deg e_i < \deg e$.

Theorem (Laurent-M. 2009)

Let E be connected to 1 and $\Lambda \in \mathrm{Hom}_{\mathbb{K}}(\langle E^+ \cdot E^+ \rangle, \mathbb{K})$. If

$$\mathrm{rank} H_\Lambda^E = \mathrm{rank} H_\Lambda^{E^+} = r$$

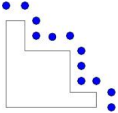
then there exists a unique element $\tilde{\Lambda} \in R^* = \mathrm{Hom}_{\mathbb{K}}(R, \mathbb{K})$ which extends Λ.

We have the following properties:

- rank $H_{\tilde{\Lambda}} = r$;
- ker $H_{\tilde{\Lambda}} = (\ker H_\Lambda^{E^+})$;
- For $\mathbb{K} = \mathbb{R}$, $H_\Lambda^{E^+} \succcurlyeq 0$ implies that
  - $H_{\tilde{\Lambda}} \succcurlyeq 0$.
  - $\mu = \sum_{i=1}^r \gamma_i \delta_{\zeta_i}$ where $\gamma_i > 0$, $\zeta_i \in \mathbb{R}^n$.

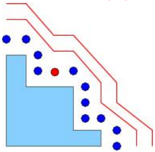
Border basis

Notations:



- $I = (f_1, \ldots, f_s)$, $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$,
- B a set of monomials **connected** to 1
  $(m \in B\text{-}\{1\} \Rightarrow \exists m' \in B,\ i \in [1, n]$ st. $m = m' x_i)$.
- $B^+ = B \cup x_1 B \cup \cdots \cup x_n B$, $\partial B = B^+ - B$.

Suppose B is a basis of $\mathcal{A}$, then



- Each $\mathbf{x}^\alpha \in \partial B$ yields a rewritting rule
  $$f_\alpha = \mathbf{x}^\alpha - \sum_{\beta \in B} \lambda_{\alpha,\beta} \mathbf{x}^\beta.$$
- The rewritting rules of ∂B allow to reduce any $p \in \mathbb{K}[\mathbf{x}]$ to $\langle B \rangle$.

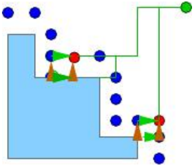
Definition

A **border basis** of B for I is a set of relations of the form f_α for $\alpha \in \partial B$, such that

- $I = (f_\alpha)$,
- $\langle B \rangle \cap I = \{0\}$.

Normal form criterion

☞ The rewritting family defines a projection $N : \langle B^+ \rangle \to \langle B \rangle$.



- Many possible reductions of m on $\langle B \rangle$, not necessarly $\mathbb{K}[\mathbf{x}] = \langle B \rangle \oplus I$ (or $\langle B \rangle \cap I = \{0\}$).
- **How to check normal form ?**

Theorem ('99)

Let B be connected * *to* 1 *and $M_i : \langle B \rangle \to \langle B \rangle$ such that $M_i(b) = N(x_i b)$.*

$$N \text{ normal form modulo } I = (Ker(N))$$
$$\Leftrightarrow B \text{ basis of } \mathcal{A} = R/I$$
$$\Leftrightarrow M_i \circ M_j = M_j \circ M_i, i, j = 1, \ldots, n.$$

* B is connected to 1 iff $\forall m \in B$ either $m = 1$ or $\exists m' \in B$, $i \in [1, n]$ s.t. $m = x_i\, m'$.

Let B be a set of monomials $\subset R$.
Assume that $H_\Lambda^{B,B}$ invertible and define

$$M_i := H_\Lambda^{B,x_i B}(H_\Lambda^{B,B})^{-1}.$$

Proposition

If Λ extend to R^* and $H_\Lambda^{B,B}$ is of rank $r = |B|$, then M_i is the matrix of multiplication by x_i in $\mathcal{A}_\Lambda$ is M_i.

Theorem

If B is connected to 1, then Λ known on B^+ extends uniquely to R

- *iff $M_i \circ M_j = M_j \circ M_i$ $(1 \leq i, j \leq n)$.*
- *iff $\operatorname{rank} H_\Lambda^B = \operatorname{rank} H_\Lambda^{B^+} = r$ and $|B| = r$.*

Then $\Lambda \in R^*$ is such that $\operatorname{rank} H_\Lambda = r$.

Applications

Decomposition of symmetric tensors

Joint work with J. Brachat, P. Comon, E. Tsigaridas.

❒ **Waring problem:** Given $f = \sum_{|\alpha| \leqslant d} f_\alpha x_0^{d-|\alpha|} \mathbf{x}^\alpha$ a honomgeneous polynomial of degree d in the variables $x_0, x_1, \ldots, x_n$,
find a minimal decomposition of f of the form

$$f = \sum_{i=1}^{r} \gamma_i (x_0 + \zeta_{i,1} x_1 + \cdots + \zeta_{i,n} x_n)^d$$

for $\zeta_i = (\zeta_{i,1}, \ldots, \zeta_{i,n}) \in \mathbb{C}^n$, $\gamma_i \in \mathbb{C}$.

❒ **Tensor decomposition:**
Given a symmetric tensor $T = (a_{i_1,\ldots,i_d})_{0 \le i_j \le n}$ with
$a_{\sigma(i_1),\ldots,\sigma(i_d)} = a_{i_1,\ldots,i_d} \in \mathbb{K}$ ($\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$)
find a minimal decomposition of T as a sum of symmetric tensors of rank 1:

$$T = \sum_{i=1}^{r} \gamma_i \zeta_i \otimes \cdots \otimes \zeta_i .$$

☞ If T is of order 2, r is its usual rank.

❒ Secant varieties of the Veronese:

Given a element T of $\mathbb{P}(S^d(\mathbb{K}^{n+1}))$,
find the smallest r such that $T \in \mathcal{S}_{r-1}(\mathcal{V}_n)$ where

- $\mathcal{V}_n := \{(\zeta^\alpha)_{|\alpha|=d}; \zeta \in \mathbb{K}^{n+1} - \{0\}\} \subset \mathbb{P}^n$.
- $\mathcal{S}_{r-1}(\mathcal{V}_{n+1}) := \{X = \sum_{k=1}^r \lambda_k X_k \in \mathbb{P}^{n+1}; X_k \in \mathbb{P}^n\}$.

❒ Moment matrix problem:

Given $\lambda_\alpha = \binom{d}{\alpha}^{-1} f_\alpha$ for $|\alpha| \leq d$,
find $\Lambda \in \mathrm{Hom}(\mathbb{C}[\mathbf{x}], \mathbb{C})$ such that $\Lambda = \sum_{i=1}^r \gamma_i \delta_{\zeta_i}$ and for all $\alpha \in A_d$, $\Lambda(\mathbf{x}^\alpha) = \binom{d}{\alpha}^{-1} f_\alpha = \lambda_\alpha$.

- $x^\alpha \mapsto \lambda_\alpha$ defines a linear form $\tilde{\Lambda} \in Hom_{\mathbb{K}}(R_d, \mathbb{K})$.
- $x^\alpha \mapsto \zeta^\alpha$ corresponds to the evaluation $\mathbf{1}_\zeta : p \mapsto p(\zeta)$.
- $f = \sum_{i=1}^r \gamma_i (x_0 + \zeta_{i,1} x_1 + \cdots + \zeta_{i,n} x_n)^d$ means that $\tilde{\Lambda}$ coincide with $\sum_{i=1}^r \gamma_i \delta_{\zeta_i}$ up to degree d.

- The minimal r is called the *rank* of T.
- The set of T with rank r is denoted $\mathcal{Y}_r$.
- For $d = 2$, r is the usual rank of the quadratic form $T(\mathbf{x})$.
- For $r = 1$, $T(\mathbf{x}) = \sum_{|\alpha|=d} c_\alpha \, \mathbf{x}^\alpha$ with $c_\alpha = \binom{d}{\alpha} u_0^{\alpha_0} \cdots u_n^{\alpha_n}$.

  $\mathcal{Y}_1$ is a closed subvariety of $\mathbb{K}[\mathbf{x}]_d$.

  The best rank 1 approximation of the tensor T corresponds to its maximizer on $S_n := \{x_0^2 + \cdots + x_n^2 = 1\}$.
- Generic rank over $\mathbb{C}$ is $\lceil \frac{\binom{n+d-1}{d}}{n} \rceil$ except $(d, n) \in \{(3, 5), (4, 3), (4, 4), (4, 5)\}$ [Alexander-Hirshowitz'95].
- Maximal rank unknown.

Sylvester'method (1886)

We consider a binary form $T(x_0, x_1) = \sum_{i=0}^{d} c_i \binom{d}{i} x_0^{d-i} x_1^i$.

Theorem

The polynomial T can be decomposed as a sum of r powers of linear forms $T = \sum_{k=1}^{r} \lambda_k (\alpha_k x_0 + \beta_k x_1)^d$ iff there exists a polynomial q such that

$$\begin{bmatrix} c_0 & c_1 & \dots & c_r \\ c_1 & & & c_{r+1} \\ \vdots & & & \vdots \\ c_{d-r} & \dots & c_{d-1} & c_d \end{bmatrix} \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_r \end{bmatrix} = 0$$

and of the form

$$q(x_0, x_1) := \mu \prod_{k=1}^{r} (\beta_k x_0 - \alpha_k x_1).$$

Truncated moment matrices (Λ known up to degree d).

If an extension $\Lambda = \sum_{i=1}^{r} \lambda_i \mathbf{1}_{\zeta_i} \in \mathrm{Hom}(\mathbb{C}[\mathbf{x}], \mathbb{C})$ exists, then

- $\mathcal{A}_\Lambda = \mathbb{K}[\mathbf{x}]/\ker H_\Lambda$ is of finite dimension r over $\mathbb{K}$.
- The zeros of I_Λ are the simple roots $\zeta_1, \ldots, \zeta_r \in \mathbb{C}^n$.
- If B is of size r connected to 1, and $H_\Lambda^{B,B})$ invertible , the matrices $M_i := H_\Lambda^{B,x_iB}(H_\Lambda^{B,B})^{-1}$ are the matrix M_i of multiplication by x_i in $\mathcal{A}_\Lambda$.
- The matrices M_i commute.

$$\begin{array}{rcl} M_a : \mathcal{A}_\Lambda & \to & \mathcal{A}_\Lambda \\ u & \mapsto & a\, u \end{array} \qquad \begin{array}{rcl} M_a^{\mathsf{t}} : \widehat{\mathcal{A}_\Lambda} & \to & \widehat{\mathcal{A}_\Lambda} \\ \Lambda & \mapsto & a \cdot \Lambda = \Lambda \circ M_a \end{array}$$

Theorem

- *The eigenvalues of M_a are $\{a(\zeta_1), \ldots, a(\zeta_d)\}$.*
- *The eigenvectors of all $(M_a^{\mathsf{t}})_{a \in \mathcal{A}}$ are (up to a scalar) $\mathbf{1}_{\zeta_i} : p \mapsto p(\zeta_i)$.*

Algorithm:

For $r = 1, \ldots,$

1. Compute B of size r, connected to 1;
2. If needed, complete the matrix $H_{\Lambda}^{B^+,B^+}$ s.t. the operators $M_i = H_{\Lambda}^{x_i B,B}(H_{\Lambda}^{B,B})^{-1}$ commute.
3. If this is not possible, start again with $r := r + 1$.
4. Compute the $n \times r$ eigenvalues s.t. $M_i \mathbf{v}_j = \zeta_{i,j} \mathbf{v}_j$, $i = 1, \ldots, n$, $j = 1, \ldots, r$.
5. Solve the linear system in $(\lambda_j)_{j=1,\ldots,k}$: $\Lambda = \sum_{j=1}^{r} \lambda_j \mathbf{1}_{\zeta_j}$ where $\zeta_j \in \mathbb{C}^n$ are the vectors of eigenvalues found in (4).

Example

The polynomial (homogeneous in 3 variables, of degree 5):

$f =$

$-1549440\, x_0 x_1 x_2{}^3 + 2417040\, x_0 x_1{}^2 x_2{}^2 + 166320\, x_0{}^2 x_1 x_2{}^2 - 829440\, x_0 x_1{}^3 x_2 - 5760\, x_0{}^3 x_1 x_2 - 222480\, x_0{}^2 x_1{}^2 x_2 +$

$38\, x_0{}^5 - 497664\, x_1{}^5 - 1107804\, x_2{}^5 - 120\, x_0{}^4 x_1 + 180\, x_0{}^4 x_2 + 12720\, x_0{}^3 x_1{}^2 + 8220\, x_0{}^3 x_2{}^2 - 34560\, x_0{}^2 x_1{}^3 -$

$59160\, x_0{}^2 x_2{}^3 + 831840\, x_0 x_1{}^4 + 442590\, x_0 x_2{}^4 - 5591520\, x_1{}^4 x_2 + 7983360\, x_1{}^3 x_2{}^2 - 9653040\, x_1{}^2 x_2{}^3 + 5116680\, x_1 x_2{}^4$

The moment matrix:

	1	x_1	x_2	x_1^2	x_1x_2	x_2^2	x_1^3	$x_1^2x_2$	x_1x
1	38	−24	36	1272	−288	822	−3456	−7416	554
x_1	−24	1272	−288	−3456	−7416	5544	166368	−41472	8056
x_2	36	−288	822	−7416	5544	−5916	−41472	80568	−7747
x_1^2	1272	−3456	−7416	166368	−41472	80568	−497664	−1118304	79833
x_1x_2	−288	−7416	5544	−41472	80568	−77472	−1118304	798336	−96530
x_2^2	822	5544	−5916	80568	−77472	88518	798336	−965304	102333
x_1^3	−3456	166368	−41472	−497664	−1118304	798336	$h_{6,0,0}$	$h_{5,1,0}$	$h_{4,2,}$
$x_1^2x_2$	−7416	−41472	80568	−1118304	798336	−965304	$h_{5,1,0}$	$h_{4,2,0}$	$h_{3,3,}$
$x_1x_2^2$	5544	80568	−77472	798336	−965304	1023336	$h_{4,2,0}$	$h_{3,3,0}$	$h_{2,4,}$
x_2^3	−5916	−77472	88518	−965304	1023336	−1107804	$h_{3,3,0}$	$h_{2,4,0}$	$h_{1,5,}$

The first leading and shift minors:

$$\Delta_0 = \begin{bmatrix} 38 & -24 & 36 & 1272 \\ -24 & 1272 & -288 & -3456 \\ 36 & -288 & 822 & -7416 \\ 1272 & -3456 & -7416 & 166368 \end{bmatrix}, \Delta_1 = \begin{bmatrix} -24 & 1272 & -288 & -3456 \\ 1272 & -3456 & -7416 & 166368 \\ -288 & -7416 & 5544 & -41472 \\ -3456 & 166368 & -41472 & -497664 \end{bmatrix}$$

The normalized vectors of eigenvalues:

$$\begin{bmatrix} 1 \\ -12 \\ -3 \end{bmatrix}, \begin{bmatrix} 1 \\ 12 \\ -13 \end{bmatrix}, \begin{bmatrix} 1 \\ -2 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$$

We solve the linear system in λ_i:

$$f = \lambda_1(x_0 - 12x_1 - 3x_2)^5 + \lambda_2(x_0 + 12x_1 - 13x_2)^5 + \lambda_3(x_0 - 2x_1 + 3x_2)^5 + \lambda_4(x_0 + 2x_1 + 3x_2)^5$$

and get the minimum decomposition (rank 4):

$$\frac{1}{3}(x_0 - 12\,x_1 - 3\,x_2)^5 + \frac{1}{5}(x_0 + 12\,x_1 - 13\,x_2)^5 + (x_0 - 2\,x_1 + 3\,x_2)^5 + +(x_0 + 2\,x_1 + 3\,x_2)^5.$$

Real radical computation

Joint work with J. Lassere, M. Laurent, Ph. Rostalski, Ph. Trébuchet.

Given $F = (f_1, \ldots, f_s) \subset R := \mathbb{R}[\mathbf{x}]$, compute a set of generators of

- $I(V_{\mathbb{C}}(F)) = \sqrt{F} = \{f \in R, \exists m > 0 \mid f^m \in F\}$,
- $I(V_{\mathbb{R}}(F)) = \sqrt[\mathbb{R}]{F} = \{f \in R, \exists m > 0 \mid f^{2m} + SoS \in F\}$.

❒ **Dual real radical problem:**

Find $\Lambda \in R^*$ st.

- $\Lambda \succcurlyeq 0$ **ie.** $H_\Lambda \succcurlyeq 0$ **ie.** $\forall p \in R, \Lambda(p^2) \geq 0$.
- $f_1, \ldots, f_s \in \ker H_\Lambda$.
- H_Λ **of maximal rank.**

If $\mathrm{rank} H_\Lambda = r$ and $H_\Lambda \succcurlyeq 0$, then $\Lambda = \sum_{i=1}^r \gamma_i \delta_{\zeta_i}$ with
$\zeta_i \in \mathbb{R}^n, \gamma_i > 0$.
$\{\zeta_1, \ldots, \zeta_r\} \subset V_{\mathbb{R}}(F)$ with equality for maximal rank.
$\sqrt[\mathbb{R}]{F} \subset \ker H_\Lambda$ with equality for maximal rank.

Let $S \subset R = \mathbb{R}[\mathbf{x}]$ with $1 \in S$, $G \subseteq S \cdot S$, and

$$\begin{array}{rcl} \mathcal{L}_{S,G} & := & \{\Lambda \in \mathrm{Hom}_{\mathbb{R}}(S \cdot S, \mathbb{R}) \mid \Lambda(g) = 0,\ \forall g \in G\}, \\ \mathcal{L}_{S,G,\succcurlyeq} & := & \{\Lambda \in \mathcal{L}_{S,G} \mid \Lambda(p^2) \geq 0,\ \forall p \in S\}. \end{array}$$

Theorem

(i) *Let $\Lambda^* \in \mathcal{L}_{S,G}$ for which $\mathrm{rank} H^S_\Lambda$ is maximum. Then* $\ker H^S_{\Lambda^*} \subset \sqrt{(G)}$.

(ii) *Let $\Lambda^* \in \mathcal{L}_{S,G,\succcurlyeq}$ for which $\mathrm{rank} H^S_\Lambda$ is maximum. Then* $\ker H^S_{\Lambda^*} \subset \sqrt[\mathbb{R}]{(G)}$.

(iii) $\ker H^E_{\Lambda^*} \subset \ker H^E_\Lambda$ *for all* $\Lambda \in \mathcal{L}_{E,F,\succcurlyeq}$.

Theorem

$\exists t_0 \in \mathbb{N}$ *such that* $\forall t \geqslant t_0$, $(\ker H^{R_t}_{\Lambda^*}) = \sqrt[\mathbb{R}]{(F)}$.

☞ **How to find $\tilde{\Lambda} \in \mathcal{L}_{S,G}$ with H_{Λ}^{S} of maximum rank ?**

Take a generic element in $\mathcal{L}_{S,G}$.

☞ **How to find $\tilde{\Lambda} \in \mathcal{L}_{S,G,\succcurlyeq}$ with H_{Λ}^{S} of maximum rank ?**

Solve the SemiDefinite Programming problem:

- $H = (h_{\alpha,\beta})_{\alpha,\beta \in S} \succcurlyeq 0$
- H satisfies the Hankel constraints $h_0 = 1$, $h_{\alpha,\beta} = h_{\alpha',\beta'}$ if $\alpha + \beta = \alpha' + \beta'$.
- H satisfies the linear constraints $\sum_{\alpha} h_{\alpha} g_{\alpha} = 0$ for $g = \sum_{\alpha} g_{\alpha} \mathbf{x}^{\alpha} \in G$.

and minimize a generic linear form.

Existing tools: SeDuMi, CSDP, ...

☞ How to construct new relations in the radical?

Given a rewritting family P with respect to B connected to 1 such that support$(P) \subset B^+$ and $\forall p \in P$, p has only one monomial in $\partial B = B^+ \setminus B$,

- Solve the SDP problem for $S = B^+$ and $G = B^+ \cdot P$ to compute a generic $\Lambda^* \in \mathcal{L}_{S,G,\succcurlyeq}$;
- Compute $\langle \tilde{P} \rangle = \ker H_{\Lambda^*}$.

Then $\langle P \rangle \subset \langle \tilde{P} \rangle \subset \sqrt[\mathbb{R}]{(G)}$.

Algorithm:

INPUT: generators (f_i) of an ideal I such that $V_{\mathbb{R}}(I)$ is finite.

- Initialize $B = B_0$ a set of monomials connected to 1; $F = (f_i)$; Λ^* a generic element in $\mathcal{L}_{B^+,F,\succcurlyeq}$ (resp. $\mathcal{L}_{B^+,F}$);
- While rank $H^B_{\Lambda^*} \neq$ rank $H^{B^+}_{\Lambda^*}$ do
  - Extend F with $\ker H^{B^+}_{\Lambda^*}$ and update B;
  - If $\ker H^B_{\Lambda^*} = \{0\}$ and F is not a border basis for B then extend B in B^+;
  - *[If* $\ker H^B_{\Lambda^*} = \{0\}$ *and* F *is a border basis of* B *then compute a basis of* $\ker H^B_{\Delta\cdot\Lambda^*}$ *and extend* F *with it.]*
  - Compute a generic element Λ^* in $\mathcal{L}_{B^+,F,\succcurlyeq}$ (resp. $\mathcal{L}_{B^+,F}$);
- Compute a basis of $\ker H^{B^+}_{\Delta\cdot\Lambda^*}$ and insert it in F

OUTPUT: B a basis of $R/\sqrt[\mathbb{R}]{I}$ and F border basis of $\sqrt[\mathbb{R}]{I}$ for B.

A very simple example

☞ $f_1 = x^2 + y^2$.
$B = (1) - (y^2)$
$S = \{1, x, y\}$ with $S \cdot S \supset f_1$.

$$H = \begin{pmatrix} 1 & \lambda_x & \lambda_y \\ \lambda_x & \lambda_{x^2} & \lambda_{x\,y} \\ \lambda_y & \lambda_{x\,y} & -\lambda_{x^2} \end{pmatrix} \succcurlyeq 0$$

implies

- $\lambda_{x^2} = 0$,
- $\lambda_x = 0, \lambda_y = 0, \lambda_{x\,y} = 0$,
- $\ker H = x, y$.

Happy end: $\sqrt[\mathbb{R}]{(x^2 + y^2)} = (x, y)$.