Moments Matrices, border bases and real radical computation

B. Mourrain
GALAAD
INRIA Méditerranée

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

May 30, 2011

Solving $\mathbf{f} = 0$ reduces to describe $\mathcal{A} = \mathbb{K}[\mathbf{x}]/(\mathbf{f})$

Hypothesis: **the number of complex roots of $\{f_1 = 0, \ldots, f_s = 0\}$ is finite $\Leftrightarrow$ $\mathcal{A} = \mathbb{K}[\mathbf{x}]/(f_1, \ldots, f_s)$ is a finite dimensional vector space.**

In practice, we compute

- a set $B = \{b_1, \ldots, b_D\}$ of polynomials (monomials) which is a **basis** of $\mathcal{A}$;
- the **tables of multiplications** $M_a = (m^a_{j,k})$ by a modulo $f_1, \ldots, f_s$:

$$a\, b_j := \sum_{k=1}^{D} m^a_{k,j} b_k.$$

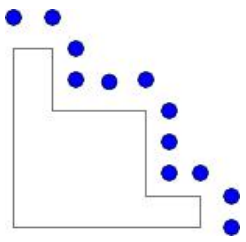
for $a = x_1, \ldots$ (using Gröbner basis, Border basis, Resultants, ...)

Theorem

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

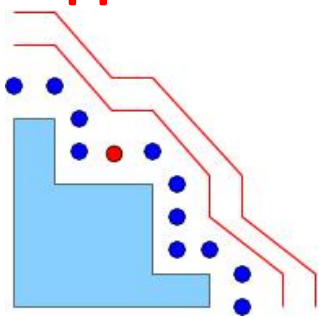
Border bases

Border basis



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

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



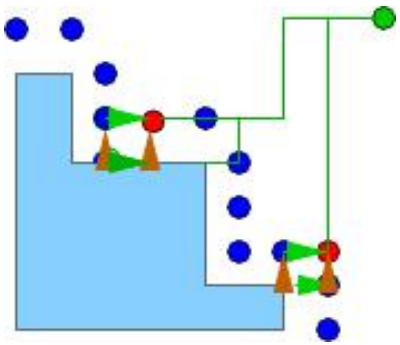
- Each $\mathbf{x}^\alpha \in \partial B$ yields a **rewritting rule**
  $$f_\alpha = \mathbf{x}^\alpha - \sum_{\beta \in B} \lambda_{\alpha,\beta} \mathbf{x}^\beta.$$
- The rewritting rules of ∂B allow to reduce any $p \in \mathbb{K}[\mathbf{x}]$ to $\langle B \rangle$.

Definition

A **border basis** of B for I is a set of relations of the form $f_\alpha = \mathbf{x}^\alpha - \sum_{\beta \in B} \lambda_{\alpha,\beta} \mathbf{x}^\beta$ for $\alpha \in \partial B$, such that

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

Normal form criterion



How to check normal form ? We want

- a unique reduction of any $m \in R$ in $\langle B \rangle$.
- $\mathbb{K}[\mathbf{x}] = \langle B \rangle \oplus I$ (or $\langle B \rangle \cap I = \{0\}$).

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

Theorem (M'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 is a normal form modulo $I = (Ker(N))$
$\Leftrightarrow$ *B 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. $m = x_i\, m'$.

Algorithm

Input: *a set of polynomials* $F \subset \mathbb{K}[\mathbf{x}]$ *defining a zero dimensional variety.*

$B :=$ *monomial set connected to* 1, *not containing the supports of* F;
commuting $:=$ *false;*

While not commuting do

- *Compute the commuting relations for* F *with respect to* B;
- *Reduce them by the existing relations* F;
- *Add the non-zero reduced relations to* F *and update* B;
- *If they all reduce to zero, commuting* $:=$ *true;*

Output: *A basis* B *of* $\mathcal{A} = R/I$ *and border relations* F.

Our objectives

- Generate efficiently new elements to describe the (real) radical.
- Optimize the size of the linear algebra or relaxation problem.
- Provide efficient implementation.

Moments

Duality

- **The dual de $\mathbb{K}[\mathbf{x}]$** is $\mathbb{K}[\mathbf{x}]^* = \{\Lambda : \mathbb{K}[\mathbf{x}] \to \mathbb{K}, \text{ linear } \}$.
- $\mathbb{K}[[\mathbf{x}]]^* = \mathbb{K}[[\mathbf{d}_1, \ldots, \mathbf{d}_n]]$.

$$\Lambda = \sum_{\alpha \in \mathbb{N}^n} \Lambda(\mathbf{x}^\alpha)\mathbf{d}^\alpha$$

where $(\mathbf{d}^\alpha)_{\alpha \in \mathbb{N}^n}$ is the dual basis of $(\mathbf{x}^\alpha)_{\alpha \in \mathbb{N}^n}$.

Example: $\mathbf{1}_\zeta : p \mapsto p(\zeta)$ is of the form $\mathbf{1}_\zeta = \sum_{\alpha \in \mathbb{N}^n} \zeta^\alpha \, \mathbf{d}^\alpha$

- **The $\mathbb{K}[\mathbf{x}]$-module structure:**

$\forall a \in \mathbb{K}[\mathbf{x}], \forall \Lambda \in \mathbb{K}[\mathbf{x}]^*$,

$$a \cdot \Lambda : b \mapsto a \cdot \Lambda(b) = \Lambda(ab)$$

Example: $x_1 \cdot \mathbf{d}_1^{\alpha_1}\mathbf{d}^{\alpha_2} \cdots \mathbf{d}^{\alpha_n} = \mathbf{d}_1^{\alpha_1 - 1}\mathbf{d}^{\alpha_2} \cdots \mathbf{d}^{\alpha_n}$ if $\alpha_1 > 0$ and 0 otherwise.

- **The dual of $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$** for an ideal I is

$$\mathcal{A}^* = \{\Lambda : \mathbb{K}[\mathbf{x}] \to \mathbb{K} \mid \Lambda(I) = 0\} = I^\perp.$$

Hankel operators

$$\begin{array}{rcl} H_\Lambda : \mathbb{K}[\mathbf{x}] & \to & \mathbb{K}[\mathbf{x}]^* \\ p & \mapsto & p \cdot \Lambda \end{array}$$

where $p \cdot \Lambda : q \mapsto \Lambda(p\,q)$.

Properties:

- $I_\Lambda := \ker H_\Lambda$ is an ideal of $\mathbb{K}[\mathbf{x}]$.
- $I_\Lambda^\perp = \mathcal{A}_\Lambda^* = \mathrm{im}\, H_\Lambda$ where $\mathcal{A}_\Lambda = R/I_\Lambda$.

Linear forms "supported" on points

Definition

Λ is supported on points if I_Λ is zero-dimensional.

Properties:

- $\mathrm{rank} H_\Lambda = r$ iff $\mathcal{A}_\Lambda = R/I_\Lambda$ is an algebra of dimension r over $\mathbb{K}$.
- If $\mathrm{rank} H_\Lambda = r$, then

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

  for some $\zeta_i \in \mathbb{C}^n$ and some differential polynomials θ_i with
  - $r = \sum_{i=1}^{r'} \dim(\langle \partial_\partial^\alpha(\theta_i) \rangle)$
  - $V_\mathbb{C}(I_\Lambda) = \{\zeta_1, \ldots, \zeta_{r'}\}$.
- If $\mathrm{rank} H_\Lambda = r$, $\mathcal{A}_\Lambda$ is a Gorenstein algebra.
- 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 $\Delta = \sum_{i=1}^{r} b_i \omega_i$.

Positive linear forms

Definition

$\Lambda \in \mathbb{R}[\mathbf{x}]^*$ is positive if $\Lambda(p^2) \geqslant 0$ for all $p \in \mathbb{R}[\mathbf{x}]$.

Properties:

- $\Lambda \in \mathbb{R}[\mathbf{x}]^*$ is positive iff $H_\Lambda \succcurlyeq 0$
- If $\Lambda \succcurlyeq 0$ then $I_\Lambda = \ker H_\Lambda$ is a real radical ideal.
- $\mathrm{rank} H_\Lambda = r$ and $H_\Lambda \succcurlyeq 0$ iff $\Lambda = \sum_{i=1}^{r} \gamma_i \mathbf{1}_{\zeta_i}$ with $\gamma_i > 0$ and ζ_i are distinct points of $\mathbb{R}^n$.

Real radical problem

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

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

Dual Gorenstein-radical formulation
Find $\Lambda \in R^*$ st.

- $f_1, \ldots, f_s \in \ker H_\Lambda$.
- H_Λ **of maximal rank.**

and compute $\ker H_{\Delta \cdot \Lambda}$.

If $\mathrm{rank} H_\Lambda = r$ and $H_\Lambda \succcurlyeq 0$, then $\Lambda = \sum_{i=1}^{r} \gamma_i \mathbf{1}_{\zeta_i}$ 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.

Some practical exercise:

- Take $f = x^4 - x^3 - x + 1 = (x-1)^2(x^2+x+1)$.
- Compute a linear form Λ such that $\Lambda(x^4) = \Lambda(x^3) + \Lambda(x) - \Lambda(1)$, $\Lambda(x^5) = \Lambda(x^3) + \Lambda(x^2) - \Lambda(1)$, $\Lambda(x^6) = 2\Lambda(x^3) - \Lambda(1)$, ...

$$H_\Lambda := \begin{pmatrix} 1 & a & b & c & \cdots \\ a & b & c & c+a-1 & \cdots \\ b & c & c+a-1 & c+b-1 & \cdots \\ c & c+a-1 & c+b-1 & 2c-1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \end{pmatrix}.$$

where $a = \Lambda(x), b = \Lambda(x^2), c = \Lambda(x^3), \ldots$.

- Find the (unique) solution, such that $H_\Lambda \succcurlyeq 0$:

$$H_\Lambda = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots \\ 1 & 1 & 1 & 1 & \cdots \\ 1 & 1 & 1 & 1 & \cdots \\ 1 & 1 & 1 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \end{pmatrix}$$

- Compute its kernel: $\langle x-1, x^2-x, x^3-x^2, \ldots \rangle$.

Truncated moment problems

☞ **Moments $\lambda_\alpha \in \mathbb{K}$ are given for $\alpha \in A \subset \mathbb{N}^n$.**

Definitions:

- $x^\alpha \mapsto \lambda_\alpha$ defines a linear form $\Lambda \in E^*$ where $E = \langle \mathbf{x}^A \rangle$.
- For E_1, E_2 such that $E_1 \cdot E_2 \subset E$ and $\Lambda \in E^*$, we define

$$\begin{array}{rccc} H_\Lambda^{E_1,E_2} : & E_1 & \to & E_2^* \\ & p & \mapsto & p \cdot \Lambda \end{array}$$

where $p \cdot \Lambda \in E_2^*$ is defined by

$$\forall q \in E_2, \quad p \cdot \Lambda(q) = \Lambda(pq).$$

Remark: the matrix of $H_\Lambda^{E_1,E_2}$ in the monomial basis $(\mathbf{x}^\alpha)_{\alpha \in E_1}$ and its dual basis $(\mathbf{d}^\alpha)_{\alpha \in E_2}$ is the **Hankel matrix** (also called **moment matrix**):

$$[H_\Lambda^k] = (\Lambda(\mathbf{x}^{\alpha+\beta}))_{\alpha \in E_1, \beta \in E_2}$$

For a set $B \subset R$ (of monomials),

- $B^+ := B \cup x_1 \cdot B \cup \cdots \cup x_n \cdot B$.
- B is connected to 1 if $\forall m \in B$, either $m = 1$ or $m = x_{i_0}\, m'$ with $m' \in B$.

Theorem (LM'09, BCMT'10, BBCM'11)

Let B, B' be connected to 1 and $\Lambda \in Hom_{\mathbb{K}}(\langle B^+ \cdot B'^+ \rangle, \mathbb{K})$. If

$$\mathrm{rank} H_\Lambda^{B,B'} = \mathrm{rank} H_\Lambda^{B^+,B'^+} = r$$

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

Let B be a set of monomials $\subset R$ (connected to 1).
Assume that $H_\Lambda^{B,B'}$ invertible and define $M_i := H_\Lambda^{B,x_i B'} (H_\Lambda^{B,B'})^{-1}$.

Theorem (LM'09, BCMT'10, BBCM'11)

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

$$M_i \circ M_j = M_j \circ M_i \quad (1 \leq i, j \leq n).$$

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

☞ **based on the characterisation of border bases by the commutation of tables of multiplication [M'99], [MT'05].**

Real radical computation

Border basis algorithm for (real) radical

Input: *a set of polynomials* $F \subset \mathbb{R}[\mathbf{x}]$ *defining a zero dimensional variety (***over** $\mathbb{R}$*).*

B := monomial set connected to 1*, not containing the supports of F;*
commuting := false;

While not commuting do

- *Compute the commuting relations for F with respect to B;*
- *Reduce them by the existing relations F;*
- *Add the non-zero reduced relations to F and update B;*
- **Add non-zero elements in the (real) radical with support in** B**;**
- *If they all reduce to zero, commuting := true;*

Output: *A basis B of* $\mathcal{A} = R/\sqrt[\mathbb{R}]{I}$ *and border relations F.*

Generating new relations

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

$$\begin{aligned} \mathcal{L}_{S,G} &:= \{\Lambda \in \langle S \cdot S \rangle^* \mid \Lambda(g) = 0,\ \forall g \in G\}, \\ \mathcal{L}_{S,G,\succcurlyeq} &:= \{\Lambda \in \mathcal{L}_{S,G} \mid \Lambda(p^2) \geq 0,\ \forall p \in S\}. \end{aligned}$$

Theorem

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

(ii) *Let* $\Lambda^* \in \mathcal{L}_{S,G,\succcurlyeq}$ *for which* $\operatorname{rank} H^S_\Lambda$ *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 (LLR'08)

$\exists k_0 \in \mathbb{N}$ *such that* $\forall k \geqslant k_0$, $(\ker H^{R_k}_{\Lambda^*}) = \sqrt[\mathbb{R}]{(F)}$.

☞ How to find $\Lambda^* \in \mathcal{L}_{S,G,\succcurlyeq}$ with $H^S_{\Lambda^*}$ 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 O.

Existing tools: SeDuMi, CSDP, ...

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

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

Easy example

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

$$H_\Lambda = \begin{pmatrix} 1 & \Lambda(x) & \Lambda(y) \\ \Lambda(x) & \Lambda(x^2) & \Lambda(x\,y) \\ \Lambda(y) & \Lambda(x\,y) & -\Lambda(x^2) \end{pmatrix} \succcurlyeq 0$$

implies

- $\Lambda(x^2) = 0$,
- $\Lambda(x) = 0, \Lambda(y) = 0, \Lambda(x\,y) = 0$,
- $\ker H_\Lambda = \langle x, y \rangle$.

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

First experimentation

Katsura 4				
Degree	*n.sdp*	*n.constraints*	*t*	*n.sdp grad. rel.*
2	5	5	2	56
4	11	67	2	56
6	16	176	2	56

Katsura 5				
Degree	*n.sdp*	*n.constraints*	*t*	*n.sdp grad. rel.*
2	6	6	3	84
4	16	146	3	84
6	26	479	3	84

bifur				
Degree	*n.sdp*	*n.constraints*	*t*	*n.sdp grad. rel.*
2	4	2	8	165
4	9	32	8	165
6	16	150	8	165
8	25	446	8	165
8	16	152	8	165
8	16	153	8	165
6	16	158	8	165
6	16	162	8	165
4	9	34	8	165
6	16	168	8	165
6	16	169	8	165
4	9	36	8	165
6	16	177	8	165
4	4	3	8	165
4	8	37	8	165

Implementation based on

- `newmac` (Ph. Trébuchet) package of MATHEMAGIX,
- and CSDP (B. Borchers).

Example	$Time_{\mathbb{R}}$	*CSDP*	*SVD Drop*	*Deg*	$Deg_{\mathbb{C}}$	$N_{\mathbb{R}}$	$N_{\mathbb{C}}$	$\mathrm{Time}_{\mathbb{C}}$
Precision 90								
*kat*4	22.479*s*	22.1645	1*e* − 12	4	4	12	16	0.06*s*
*kat*5	146.49*s*	145.64*s*	1*e* − 12	5	5	16	32	0.165*s*
cyclo	10.839*s*	10.6243*s*	1*e* − 20	5	5	4	16	0.03*s*
robot	41.84*s*	41.26*s*	1*e* − 19	6	8	4	40	1.3*s*
Precision 120								
*kat*4	22.557*s*	22.16	1*e* − 14	4	4	12	16	0.06*s*
*kat*5	146.59*s*	145.1*s*	1*e* − 12	5	5	16	32	0.17*s*
cyclo	10.839*s*	10.6243*s*	1*e* − 20	5	5	4	16	0.03*s*
robot	42.884*s*	42.2447*s*	1*e* − 19	6	8	4	40	1.4*s*

Warning: problem currently in the number of iterations in the extension of csdp over bigfloats, not solved in these results.

Issues and perspectives

- Integration of SDP solvers with algebraic tools.
- Numerical stability and basis representation.
- Extension to global polynomial optimisation problems.

Thanks for your attention