Moment matrices for root finding

B. Mourrain
GALAAD, INRIA Méditerranée, Sophia Antipolis
Bernard.Mourrain@inria.fr

GEOLMI
10-14 Septembre

Algebraic method for solving polynomial equations

- $\mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}] = R$ the multivariate polynomial ring over the field $\mathbb{K}$.
- $(f_1, \ldots, f_s) = I$ the ideal generated by the polynomials $f_1, \ldots, f_s$ to solve.

Algebraic method for solving polynomial equations

- $\mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}] = R$ the multivariate polynomial ring over the field $\mathbb{K}$.
- $(f_1, \ldots, f_s) = I$ the ideal generated by the polynomials $f_1, \ldots, f_s$ to solve.

Objective: construct

- $A \subset R$ described by a basis B,
- a **projection** $\pi : R \to A$ such that the following sequence is exact:

$$0 \to I \to R \xrightarrow{\pi} A \to 0.$$

Algebraic method for solving polynomial equations

- $\mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}] = R$ the multivariate polynomial ring over the field $\mathbb{K}$.
- $(f_1, \ldots, f_s) = I$ the ideal generated by the polynomials $f_1, \ldots, f_s$ to solve.

Objective: construct

- $A \subset R$ described by a basis B,
- a **projection** $\pi : R \to A$ such that the following sequence is exact:

$$0 \to I \to R \stackrel{\pi}{\to} A \to 0.$$

Then $R = A \oplus I$ and $\mathcal{A} = R/I \sim A = \mathrm{im}\,\pi$, $I = \ker \pi$.
For $p \in R$, $\pi(p) \in A$ is the **normal form** of p.

Algebraic method for solving polynomial equations

- $\mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}] = R$ the multivariate polynomial ring over the field $\mathbb{K}$.
- $(f_1, \ldots, f_s) = I$ the ideal generated by the polynomials $f_1, \ldots, f_s$ to solve.

Objective: construct

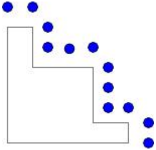
- $A \subset R$ described by a basis B,
- a **projection** $\pi : R \rightarrow A$ such that the following sequence is exact:

$$0 \rightarrow I \rightarrow R \xrightarrow{\pi} A \rightarrow 0.$$

Then $R = A \oplus I$ and $\mathcal{A} = R/I \sim A = \mathrm{im}\, \pi$, $I = \ker \pi$.
For $p \in R$, $\pi(p) \in A$ is the **normal form** of p.
Normal form algorithms: **Gröbner basis**, **H-basis**, **Janet basis**, **Border basis** ...

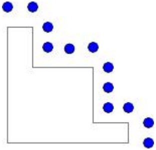
Border basis

Border basis



- B a set of monomials **connected** to 1 ($1 \in B$, $\forall m \in B \setminus \{1\}$ $\exists m' \in B$, $i \in [1, n]$ st. $m = m' x_i$).
- $B^+ = B \cup x_1 B \cup \cdots \cup x_n B$, $\partial B = B^+ - B$.

Border basis



- B a set of monomials **connected** to 1 ($1 \in B$, $\forall m \in B \setminus \{1\}$ $\exists m' \in B$, $i \in [1, n]$ st. $m = m' x_i$).
- $B^+ = B \cup x_1 B \cup \cdots \cup x_n B$, $\partial B = B^+ - B$.

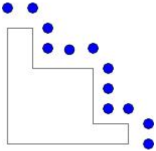
Theorem

Let $d \geq 2$, let B be a subset of $\mathcal{M}$ connected to 1, let $\pi : \langle B^+ \rangle_{\leq d} \to \langle B \rangle_{\leq d}$ be a projection and let F be the rewriting family of π.

The following conditions are equivalent:

1. $(M_i \circ M_j - M_j \circ M_i)_{|\langle B \rangle_{\leq d-2}} = 0$ *for* $1 \leq i < j \leq n$,
2. *there exists a unique projection* $\tilde{\pi} : R_{\leq d} \to \langle B \rangle_{\leq d}$ *such that the restriction of* $\tilde{\pi}$ *to* $\langle B^+ \rangle_{\leq d}$ *is* π *and* $\ker \tilde{\pi} = \langle F^{\langle \leq d \rangle} \rangle$,

Border basis



- B a set of monomials **connected** to 1 ($1 \in B$, $\forall m \in B \setminus \{1\}\ \exists m' \in B$, $i \in [1, n]$ st. $m = m' x_i$).
- $B^{+} = B \cup x_1 B \cup \cdots \cup x_n B$, $\partial B = B^{+} - B$.

Theorem

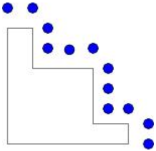
Let $d \geq 2$, let B be a subset of $\mathcal{M}$ connected to 1, let $\pi : \langle B^{+} \rangle_{\leq d} \to \langle B \rangle_{\leq d}$ be a projection and let F be the rewriting family of π.

The following conditions are equivalent:

1. $(M_i \circ M_j - M_j \circ M_i)_{|\langle B \rangle_{\leq d-2}} = 0$ *for* $1 \leq i < j \leq n$,
2. *there exists a unique projection* $\tilde{\pi} : R_{\leq d} \to \langle B \rangle_{\leq d}$ *such that the restriction of* $\tilde{\pi}$ *to* $\langle B^{+} \rangle_{\leq d}$ *is* π *and* $\ker \tilde{\pi} = \langle F^{\langle \leq d \rangle} \rangle$,

☞ Can be checked easily by reducing the **commutation polynomials**.

Border basis



- B a set of monomials **connected** to 1 ($1 \in B$, $\forall m \in B \setminus \{1\}$ $\exists m' \in B$, $i \in [1, n]$ st. $m = m' x_i$).
- $B^+ = B \cup x_1 B \cup \cdots \cup x_n B$, $\partial B = B^+ - B$.

Theorem

Let $d \geq 2$, let B be a subset of $\mathcal{M}$ connected to 1, let $\pi : \langle B^+ \rangle_{\leq d} \to \langle B \rangle_{\leq d}$ be a projection and let F be the rewriting family of π.

The following conditions are equivalent:

1. $(M_i \circ M_j - M_j \circ M_i)_{|\langle B \rangle_{\leq d-2}} = 0$ *for* $1 \leq i < j \leq n$,
2. *there exists a unique projection* $\tilde{\pi} : R_{\leq d} \to \langle B \rangle_{\leq d}$ *such that the restriction of* $\tilde{\pi}$ *to* $\langle B^+ \rangle_{\leq d}$ *is* π *and* $\ker \tilde{\pi} = \langle F^{\langle \leq d \rangle} \rangle$,

☞ Can be checked easily by reducing the **commutation polynomials**.

☞ Border basis iff (1) applies for any $d \geq 2$.

Recovering the roots by eigenvector computation

Recovering the roots by eigenvector computation

Hypothesis: $\mathcal{V}_{\overline{\mathbb{K}}}(I) = \{\zeta_1, \ldots, \zeta_r\} \Leftrightarrow \mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ of dimension $D < \infty$ over $\mathbb{K}$.

Operators of multiplication:

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

Recovering the roots by eigenvector computation

Hypothesis: $\mathcal{V}_{\overline{\mathbb{K}}}(I) = \{\zeta_1, \ldots, \zeta_r\} \Leftrightarrow \mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ of dimension $D < \infty$ over $\mathbb{K}$.

Operators of multiplication:

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

Their representation in the basis $B = \{b_1, \ldots, b_D\}$ of A:

$$M_a = [\pi(a\,b_j)_i]_{1 \le i,j \le D}, \quad M_a^t = [\pi(a\,b_i)_j]_{1 \le i,j \le D}.$$

Recovering the roots by eigenvector computation

Hypothesis: $\mathcal{V}_{\mathbb{K}}(I) = \{\zeta_1, \ldots, \zeta_r\} \Leftrightarrow \mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ of dimension $D < \infty$ over $\mathbb{K}$.

Operators of multiplication:

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

Their representation in the basis $B = \{b_1, \ldots, b_D\}$ of A:

$$M_a = [\pi(a\, b_j)_i]_{1 \le i,j \le D}, \quad M_a^t = [\pi(a\, b_i)_j]_{1 \le i,j \le D}.$$

Theorem

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

Recovering the roots by eigenvector computation

Hypothesis: $\mathcal{V}_{\mathbb{K}}(I) = \{\zeta_1, \ldots, \zeta_r\} \Leftrightarrow \mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ of dimension $D < \infty$ over $\mathbb{K}$.

Operators of multiplication:

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

Their representation in the basis $B = \{b_1, \ldots, b_D\}$ **of** A**:**

$$M_a = [\pi(a\,b_j)_i]_{1 \le i,j \le D}, \quad M_a^t = [\pi(a\,b_i)_j]_{1 \le i,j \le D}.$$

Theorem

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

In practice, take some a in $\langle x_1, \ldots, x_n \rangle$.

Duality

Duality

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

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 $(\mathbf{x}^\alpha)_{\alpha \in \mathbb{N}^n}$.

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 $(\mathbf{x}^\alpha)_{\alpha \in \mathbb{N}^n}$.

❒ **The $\mathbb{K}[\mathbf{x}]$-module structure:**
$\forall a \in \mathbb{K}[\mathbf{x}], \forall \Lambda \in \mathbb{K}[\mathbf{x}]^*$,

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

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 $(\mathbf{x}^\alpha)_{\alpha\in\mathbb{N}^n}$.

❒ **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: $x_1 \cdot \mathbf{d}_1^{\alpha_1}\mathbf{d}_2^{\alpha_2}\cdots\mathbf{d}_n^{\alpha_n} = \mathbf{d}_1^{\alpha_1-1}\mathbf{d}_2^{\alpha_2}\cdots\mathbf{d}_n^{\alpha_n}$ if $\alpha_1 > 0$ and 0 otherwise.

Examples

- $p \mapsto p(\zeta)$ represented by the series $\mathbf{1}_\zeta = \sum_{\alpha\in\mathbb{N}^n} \zeta^\alpha\, \mathbf{d}^\alpha$.
- $p \mapsto \partial_1^{\alpha_1} \cdots \partial_n^{\alpha_n}(p)(0)$ represented by $\alpha!\, \mathbf{d}^\alpha$.
- $p \mapsto$ coefficient of x^α in $\pi(p)$.
- $p \mapsto \int_\Omega p\, d\mu$.

Our objective

Exploit the properties of the dual

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

of $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ to find the roots $\mathcal{V}(I) = \{\zeta_1, \ldots, \zeta_r\}$.

Our objective

Exploit the properties of the dual

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

of $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ to find the roots $\mathcal{V}(I) = \{\zeta_1, \ldots, \zeta_r\}$.

Outline

1. Properties
2. Applications

Moment matrices and Hankel operators

Moment matrices and Hankel operators

- For $\Lambda \in E^*$ where $E = \langle \mathbf{x}^A \rangle$, the **moments** are $\Lambda(x^\alpha) \in \mathbb{K}$ for $\alpha \in A \subset \mathbb{N}^n$.

Moment matrices and Hankel operators

- For $\Lambda \in E^*$ where $E = \langle \mathbf{x}^A \rangle$, the **moments** are $\Lambda(x^\alpha) \in \mathbb{K}$ for $\alpha \in A \subset \mathbb{N}^n$.
- For E_1, E_2 such that $E_1 \cdot E_2 \subset E$ and $\Lambda \in E^*$, the associated **truncated Hankel operator** is

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

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

Moment matrices and Hankel operators

- For $\Lambda \in E^*$ where $E = \langle \mathbf{x}^A \rangle$, the **moments** are $\Lambda(x^\alpha) \in \mathbb{K}$ for $\alpha \in A \subset \mathbb{N}^n$.
- For E_1, E_2 such that $E_1 \cdot E_2 \subset E$ and $\Lambda \in E^*$, the associated **truncated Hankel operator** is

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

  where $p \cdot \Lambda : q \mapsto \Lambda(p\, q)$.
- Its matrix in the monomial basis $(\mathbf{x}^\alpha)_{\alpha \in E_1}$ and the dual basis $(\mathbf{d}^\alpha)_{\alpha \in E_2}$ is the **moment matrix**:

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

Moment matrices and Hankel operators

- For $\Lambda \in E^*$ where $E = \langle \mathbf{x}^A \rangle$, the **moments** are $\Lambda(x^\alpha) \in \mathbb{K}$ for $\alpha \in A \subset \mathbb{N}^n$.
- For E_1, E_2 such that $E_1 \cdot E_2 \subset E$ and $\Lambda \in E^*$, the associated **truncated Hankel operator** is

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

  where $p \cdot \Lambda : q \mapsto \Lambda(p\,q)$.
- Its matrix in the monomial basis $(\mathbf{x}^\alpha)_{\alpha \in E_1}$ and the dual basis $(\mathbf{d}^\alpha)_{\alpha \in E_2}$ is the **moment matrix**:

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

- If $E = \mathbb{K}[x_1, \ldots, x_n]$, we define the **Hankel operator**:

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

Linear forms "supported" on points

Definition: Λ is **supported on points** if $I_\Lambda = \ker H_\Lambda$ is zero-dimensional.

Linear forms "supported" on points

Definition: Λ is **supported on points** if $I_\Lambda = \ker H_\Lambda$ is zero-dimensional.

Properties:

Linear forms "supported" on points

Definition: Λ is **supported on points** if $I_\Lambda = \ker H_\Lambda$ is zero-dimensional.

Properties:

- Λ is supported on points iff $\mathrm{rank} H_\Lambda = r < \infty$.

Linear forms "supported" on points

Definition: Λ is **supported on points** if $I_\Lambda = \ker H_\Lambda$ is zero-dimensional.

Properties:

- Λ is supported on points iff $\mathrm{rank} H_\Lambda = r < \infty$.
- If Λ is supported on points, 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

- $r = \sum_{i=1}^{r'} \dim(\langle \partial_\partial^\alpha(\theta_i) \rangle)$
- $V_\mathbb{C}(I_\Lambda) = \{\zeta_1, \ldots, \zeta_{r'}\}$.

Linear forms “supported” on points

Definition: Λ is **supported on points** if $I_\Lambda = \ker H_\Lambda$ is zero-dimensional.

Properties:

- Λ is supported on points iff $\mathrm{rank} H_\Lambda = r < \infty$.
- If Λ is supported on points, 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 Λ is supported on points, then $\mathcal{A}_\Lambda = R/I_\Lambda$ is a Gorenstein algebra:

Linear forms "supported" on points

Definition: Λ is **supported on points** if $I_\Lambda = \ker H_\Lambda$ is zero-dimensional.

Properties:

- Λ is supported on points iff $\mathrm{rank} H_\Lambda = r < \infty$.
- If Λ is supported on points, 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 Λ is supported on points, then $\mathcal{A}_\Lambda = R/I_\Lambda$ 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.

Positive linear forms

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

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:

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 $H_\Lambda \succcurlyeq 0$.

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.

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.
- Λ supported on points and positive iff $\Lambda = \sum_{i=1}^{r} \gamma_i \mathbf{1}_{\zeta_i}$ with $\gamma_i > 0$ and ζ_i are distinct points of $\mathbb{R}^n$.

Flat extension

Flat extension

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

Let B, B' be connected to 1 of size r and $\Lambda \in \langle B^+ \cdot B'^+ \rangle^*$. The following conditions are equivalent:

1. *there exists a unique element $\tilde{\Lambda} \in R^*$ which extends Λ and such that B and B' are basis of $\mathcal{A}_\Lambda = R/I_\Lambda$.*
2. $$\mathrm{rank} H_\Lambda^{B,B'} = \mathrm{rank} H_\Lambda^{B^+,B'^+} = r.$$
3. *$H_\Lambda^{B,B'}$ is invertible and the matrices $M_i := H_\Lambda^{B,x_i B'}(H_\Lambda^{B,B'})^{-1}$ satisfy*
$$M_i \circ M_j = M_j \circ M_i \quad (1 \leq i, j \leq n).$$

In this case, $\tilde{\Lambda}$ is supported on points.

Flat extension

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

Let B, B' be connected to 1 of size r and $\Lambda \in \langle B^+ \cdot B'^+ \rangle^*$. The following conditions are equivalent:

1. *there exists a unique element $\tilde{\Lambda} \in R^*$ which extends Λ and such that B and B' are basis of $\mathcal{A}_\Lambda = R/I_\Lambda$.*
2. $$\mathrm{rank} H_\Lambda^{B,B'} = \mathrm{rank} H_\Lambda^{B^+,B'^+} = r.$$
3. *$H_\Lambda^{B,B'}$ is invertible and the matrices $M_i := H_\Lambda^{B,x_i B'}(H_\Lambda^{B,B'})^{-1}$ satisfy*
$$M_i \circ M_j = M_j \circ M_i \quad (1 \leq i, j \leq n).$$

In this case, $\tilde{\Lambda}$ is supported on points.

☞ If $H_\Lambda^{B,B'} \succcurlyeq 0$ then $\tilde{\Lambda} \succcurlyeq 0$.

Applications

Roots with no multiplicity

Let $f = x^d + f_{d-1}x^{d-1} + \cdots + f_0 \in \mathbb{C}[x]$.

1. Compute a generic sequence $(h_i)_{0\leq i\leq 3d-3}$ such that
$$h_{d+j} = -f_{d-1}\, h_{d-j-1} - \cdots - f_0\, h_j.$$
2. Compute $(h'_i)_{0\leq i\leq 2d-2} = f' \cdot (h_j)$ such that $h'_j = \sum_{i=1}^{d} i\, h_{j+i-1}\, f_i$.
3. Compute the kernel of
$$H_{f'} = (h'_{i+j})_{0\leq i,j\leq d-1}.$$

Roots with no multiplicity

Let $f = x^d + f_{d-1}x^{d-1} + \cdots + f_0 \in \mathbb{C}[x]$.

1. Compute a generic sequence $(h_i)_{0 \le i \le 3d-3}$ such that
$$h_{d+j} = -f_{d-1}\, h_{d-j-1} - \cdots - f_0\, h_j.$$
2. Compute $(h'_i)_{0 \le i \le 2d-2} = f' \cdot (h_j)$ such that $h'_j = \sum_{i=1}^{d} i\, h_{j+i-1}\, f_i$.
3. Compute the kernel of
$$H_{f'} = (h'_{i+j})_{0 \le i,j \le d-1}.$$

☞ The polynomial of smallest degree of $\ker H_{f'}$ has the same roots as f, but with multiplicity 1.

Roots with no multiplicity

Let $f = x^d + f_{d-1}x^{d-1} + \cdots + f_0 \in \mathbb{C}[x]$.

1. Compute a generic sequence $(h_i)_{0\le i\le 3d-3}$ such that
$$h_{d+j} = -f_{d-1}h_{d-j-1} - \cdots - f_0\, h_j.$$
2. Compute $(h'_i)_{0\le i\le 2d-2} = f' \cdot (h_j)$ such that $h'_j = \sum_{i=1}^{d} i\, h_{j+i-1}\, f_i$.
3. Compute the kernel of
$$H_{f'} = (h'_{i+j})_{0\le i,j\le d-1}.$$

☞ The polynomial of smallest degree of ker $H_{f'}$ has the same roots as f, but with multiplicity 1.

☞ Another way to compute $f/gcd(f, f')$ ...

Roots with no multiplicity

Let $f = x^d + f_{d-1}x^{d-1} + \cdots + f_0 \in \mathbb{C}[x]$.

1. Compute a generic sequence $(h_i)_{0\leq i\leq 3d-3}$ such that
$$h_{d+j} = -f_{d-1}h_{d-j-1} - \cdots - f_0\, h_j.$$
2. Compute $(h'_i)_{0\leq i\leq 2d-2} = f' \cdot (h_j)$ such that $h'_j = \sum_{i=1}^{d} i\, h_{j+i-1}\, f_i$.
3. Compute the kernel of
$$H_{f'} = (h'_{i+j})_{0\leq i,j\leq d-1}.$$

☞ The polynomial of smallest degree of $\ker H_{f'}$ has the same roots as f, but with multiplicity 1.

☞ Another way to compute $f/gcd(f, f')$ ...

☞ Fast algorithm: $\tilde{\mathcal{O}}(d)$.

Real roots of univariate polynomials

Let $f = x^d + f_{d-1}x^{d-1} + \cdots + f_0 \in \mathbb{R}[x]$.

1. Compute a generic sequence $(h_i)_{0\leq i\leq 2d-2}$ such that
   - $h_{d+j} = -f_{d-1}h_{d-j-1} - \cdots - f_0\, h_j$ and
   - $H_{f,\succcurlyeq} = (h_{i+j})_{0\leq i,j\leq d-1} \succcurlyeq 0$;
2. Compute the kernel of $H_{f,\succcurlyeq}$.

Real roots of univariate polynomials

Let $f = x^d + f_{d-1}x^{d-1} + \cdots + f_0 \in \mathbb{R}[x]$.

1. Compute a generic sequence $(h_i)_{0 \le i \le 2d-2}$ such that
   - $h_{d+j} = -f_{d-1} h_{d-j-1} - \cdots - f_0\, h_j$ and
   - $H_{f,\succcurlyeq} = (h_{i+j})_{0 \le i,j \le d-1} \succcurlyeq 0$;
2. Compute the kernel of $H_{f,\succcurlyeq}$.

☞ The polynomial of smallest degree of $\ker H_{f,\succcurlyeq}$ has the same **real** roots as f, with multiplicity 1.

Real roots of univariate polynomials

Let $f = x^d + f_{d-1}x^{d-1} + \cdots + f_0 \in \mathbb{R}[x]$.

1. Compute a generic sequence $(h_i)_{0\leq i\leq 2d-2}$ such that
   - $h_{d+j} = -f_{d-1}h_{d-j-1} - \cdots - f_0\, h_j$ and
   - $H_{f,\succcurlyeq} = (h_{i+j})_{0\leq i,j\leq d-1} \succcurlyeq 0$;
2. Compute the kernel of $H_{f,\succcurlyeq}$.

☞ The polynomial of smallest degree of ker $H_{f,\succcurlyeq}$ has the same **real** roots as f, with multiplicity 1.

☞ Numerical algorithm, no good complexity bound yet;

Example:

- Take $f = x^4 - x^3 - x + 1 = (x-1)^2(x^2+x+1)$.

Example:

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

$\Lambda(x^5) = \Lambda(x^3) + \Lambda(x^2) - \Lambda(1)$, $\Lambda(x^6) = 2\,\Lambda(x^3) - \Lambda(1)$, ...

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

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

Example:

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

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

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

- Find Λ such that $H_\Lambda \succcurlyeq 0$:

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

Example:

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

$\Lambda(x^5) = \Lambda(x^3) + \Lambda(x^2) - \Lambda(1)$, $\Lambda(x^6) = 2\,\Lambda(x^3) - \Lambda(1)$, ...

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

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

- Find Λ such that $H_\Lambda \succcurlyeq 0$:

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

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

Solving exponential polynomials

Given $f(u_1, \ldots, u_n) = \sum_{i=1}^{r} \lambda_i e^{u_1\gamma_{i,1}+\cdots+u_n\gamma_{i,n}} = \sum_{i=1}^{r} \lambda_i \zeta_{i,1}^{u_1} \cdots \zeta_{i,n}^{u_n}$ $(\zeta_{i,j} = e^{\gamma_{i,j}})$, find the points $(\zeta_{i,1}, \ldots, \zeta_{i,n}) \in \mathbb{C}^n$ and $\lambda_i \in \mathbb{C}$ for $i = 1 \ldots, r$.

Solving exponential polynomials

Given $f(u_1,\ldots,u_n) = \sum_{i=1}^{r} \lambda_i e^{u_1\gamma_{i,1}+\cdots+u_n\gamma_{i,n}} = \sum_{i=1}^{r} \lambda_i \zeta_{i,1}^{u_1}\cdots\zeta_{i,n}^{u_n}$ $(\zeta_{i,j} = e^{\gamma_{i,j}})$,

find the points $(\zeta_{i,1},\ldots,\zeta_{i,n}) \in \mathbb{C}^n$ and $\lambda_i \in \mathbb{C}$ for $i = 1\ldots,r$.

1. Find sets of monomials $B_1 = \left\{\mathbf{x}^{\beta_1},\ldots,\mathbf{x}^{\beta_r}\right\}$, $B_2 = \left\{\mathbf{x}^{\beta'_1},\ldots,\mathbf{x}^{\beta'_r}\right\} = \{1, x_1, x_2, \ldots\} \subset \mathbb{N}^n$ s.t. $H_f^{B_1,B_2} = \left(f\left(\beta_i + \beta'_j\right)\right)_{1\leqslant i,j\leqslant r}$ is invertible;

Solving exponential polynomials

Given $f(u_1, \ldots, u_n) = \sum_{i=1}^{r} \lambda_i e^{u_1 \gamma_{i,1} + \cdots + u_n \gamma_{i,n}} = \sum_{i=1}^{r} \lambda_i \zeta_{i,1}^{u_1} \cdots \zeta_{i,n}^{u_n}$ $(\zeta_{i,j} = e^{\gamma_{i,j}})$,

find the points $(\zeta_{i,1}, \ldots, \zeta_{i,n}) \in \mathbb{C}^n$ and $\lambda_i \in \mathbb{C}$ for $i = 1 \ldots, r$.

1. Find sets of monomials $B_1 = \left\{\mathbf{x}^{\beta_1}, \ldots, \mathbf{x}^{\beta_r}\right\}$, $B_2 = \left\{\mathbf{x}^{\beta'_1}, \ldots, \mathbf{x}^{\beta'_r}\right\} = \{1, x_1, x_2, \ldots\} \subset \mathbb{N}^n$ s.t. $H_f^{B_1,B_2} = \left(f\left(\beta_i + \beta'_j\right)\right)_{1 \leqslant i,j \leqslant r}$ is invertible;
2. Compute the generalize eigenvalues $\zeta_{i,1}$ and eigenvectors $\mathbf{v}_i$ of $(H_f^{B_1, x_1 B_2}, H_f^{B_1,B_2})$;

Solving exponential polynomials

Given $f(u_1, \dots, u_n) = \sum_{i=1}^{r} \lambda_i e^{u_1\gamma_{i,1}+\cdots+u_n\gamma_{i,n}} = \sum_{i=1}^{r} \lambda_i \zeta_{i,1}^{u_1} \cdots \zeta_{i,n}^{u_n}$ $(\zeta_{i,j} = e^{\gamma_{i,j}})$,

find the points $(\zeta_{i,1}, \dots, \zeta_{i,n}) \in \mathbb{C}^n$ and $\lambda_i \in \mathbb{C}$ for $i = 1 \dots, r$.

1. Find sets of monomials $B_1 = \left\{\mathbf{x}^{\beta_1}, \dots, \mathbf{x}^{\beta_r}\right\}$, $B_2 = \left\{\mathbf{x}^{\beta'_1}, \dots, \mathbf{x}^{\beta'_r}\right\} = \{1, x_1, x_2, \dots\} \subset \mathbb{N}^n$ s.t. $H_f^{B_1,B_2} = \left(f\left(\beta_i + \beta'_j\right)\right)_{1\leqslant i,j\leqslant r}$ is invertible;
2. Compute the generalize eigenvalues $\zeta_{i,1}$ and eigenvectors $\mathbf{v}_i$ of
$$(H_f^{B_1,x_1 B_2}, H_f^{B_1,B_2});$$
3. Deduce from $\mathbf{w}_i = H_f^{B_1,B_2}\mathbf{v}_i = \mathbf{w}_{i,1}[1, \zeta_{i,1}, \zeta_{i,2}, \dots]$ the coordinates $\zeta_{i,1}, \dots, \zeta_{i,n}$ of the "roots".

Solving exponential polynomials

Given $f(u_1, \ldots, u_n) = \sum_{i=1}^{r} \lambda_i e^{u_1\gamma_{i,1}+\cdots+u_n\gamma_{i,n}} = \sum_{i=1}^{r} \lambda_i \zeta_{i,1}^{u_1} \cdots \zeta_{i,n}^{u_n}$ $(\zeta_{i,j} = e^{\gamma_{i,j}})$,

find the points $(\zeta_{i,1}, \ldots, \zeta_{i,n}) \in \mathbb{C}^n$ and $\lambda_i \in \mathbb{C}$ for $i = 1\ldots, r$.

1. Find sets of monomials $B_1 = \left\{\mathbf{x}^{\beta_1}, \ldots, \mathbf{x}^{\beta_r}\right\}$, $B_2 = \left\{\mathbf{x}^{\beta'_1}, \ldots, \mathbf{x}^{\beta'_r}\right\} = \{1, x_1, x_2, \ldots\} \subset \mathbb{N}^n$ s.t. $H_f^{B_1,B_2} = \left(f\left(\beta_i + \beta'_j\right)\right)_{1\leqslant i,j\leqslant r}$ is invertible;
2. Compute the generalize eigenvalues $\zeta_{i,1}$ and eigenvectors $\mathbf{v}_i$ of $$(H_f^{B_1,x_1\,B_2}, H_f^{B_1,B_2});$$
3. Deduce from $\mathbf{w}_i = H_f^{B_1,B_2}\,\mathbf{v}_i = \mathbf{w}_{i,1}\,[1, \zeta_{i,1}, \zeta_{i,2}, \ldots]$ the coordinates $\zeta_{i,1}, \ldots, \zeta_{i,n}$ of the "roots".

(Generalized Prony's method)

Example

- Let $f(u_1, u_2) = 1 + 2^{u_1+u_2} + 3^{u_2}$.
- Take $B = \{1, x_1, x_2\}$ (or $\{(0,0),(1,0),(0,1)\}$).

$$H_f^{B,B} = \begin{bmatrix} f(0,0) & f(1,0) & f(0,1) \\ f(1,0) & f(2,0) & f(1,1) \\ f(0,1) & f(1,1) & f(0,2) \end{bmatrix} = \begin{bmatrix} 3 & 6 & 4 \\ 6 & 14 & 8 \\ 4 & 8 & 6 \end{bmatrix},$$

$$H_f^{B,x_1B} = \begin{bmatrix} 6 & 14 & 8 \\ 14 & 36 & 18 \\ 8 & 18 & 12 \end{bmatrix}.$$

- Compute the generalized eigenvectors for the eigenvalues $(1, 2, 3)$

$$V = \begin{bmatrix} 2 & -1 & 0 \\ -1/2 & 0 & 1/2 \\ -1/2 & 1 & -1/2 \end{bmatrix} \text{ and } H_f^{B,B} V = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 2 & 1 \end{bmatrix}.$$

- This yields the roots $(1,1),(2,2),(3,1)$.

Real radical computation

Let $F = \{f_1, \ldots, f_s\} \subset \mathbb{R}[\mathbf{x}]$.
Let $S \subset R = \mathbb{R}[\mathbf{x}]$ with $1 \in S$, $G \subseteq \langle S \cdot S \rangle$, and

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

Real radical computation

Let $F = \{f_1, \dots, f_s\} \subset \mathbb{R}[\mathbf{x}]$.
Let $S \subset R = \mathbb{R}[\mathbf{x}]$ with $1 \in S$, $G \subseteq \langle S \cdot S \rangle$, and

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

Repeat

1. Compute a rewriting family $G \subset (F)$ and choose S in a basis for G;
2. Compute a generic element Λ^* of $\mathcal{L}_{S,G,\succcurlyeq}$;
3. Compute $\ker H_{\Lambda^*}^{S,S}$ and add its generators to F;
4. Update the rewriting family G of F;

until $\ker H_{\Lambda^*} = \{0\}$ and G is a border basis for $B = S$.

Real radical computation

Let $F = \{f_1, \ldots, f_s\} \subset \mathbb{R}[\mathbf{x}]$.
Let $S \subset R = \mathbb{R}[\mathbf{x}]$ with $1 \in S$, $G \subseteq \langle S \cdot S \rangle$, and

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

Repeat

1. Compute a rewriting family $G \subset (F)$ and choose S in a basis for G;
2. Compute a generic element Λ^* of $\mathcal{L}_{S,G,\succcurlyeq}$;
3. Compute $\ker H_{\Lambda^*}^{S,S}$ and add its generators to F;
4. Update the rewriting family G of F;

until $\ker H_{\Lambda^*} = \{0\}$ and G is a border basis for $B = S$.

☞ Computation of Λ^* by solving of a SDP problem by an interior point method (SeDuMi, CSDP, SDPA, ...)

Real radical computation

Let $F = \{f_1, \dots, f_s\} \subset \mathbb{R}[\mathbf{x}]$.
Let $S \subset R = \mathbb{R}[\mathbf{x}]$ with $1 \in S$, $G \subseteq \langle S \cdot S \rangle$, and

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

Repeat

1. Compute a rewriting family $G \subset (F)$ and choose S in a basis for G;
2. Compute a generic element Λ^* of $\mathcal{L}_{S,G,\succcurlyeq}$;
3. Compute $\ker H_{\Lambda^*}^{S,S}$ and add its generators to F;
4. Update the rewriting family G of F;

until $\ker H_{\Lambda^*} = \{0\}$ and G is a border basis for $B = S$.

☞ Computation of Λ^* by solving of a SDP problem by an interior point method (SeDuMi, CSDP, SDPA, ...)

☞ Applies for zero-dimensional real radical.

Real radical computation

Let $F = \{f_1, \ldots, f_s\} \subset \mathbb{R}[\mathbf{x}]$.
Let $S \subset R = \mathbb{R}[\mathbf{x}]$ with $1 \in S$, $G \subseteq \langle S \cdot S \rangle$, and

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

Repeat

1. Compute a rewriting family $G \subset (F)$ and choose S in a basis for G;
2. Compute a generic element Λ^* of $\mathcal{L}_{S,G,\succcurlyeq}$;
3. Compute $\ker H_{\Lambda^*}^{S,S}$ and add its generators to F;
4. Update the rewriting family G of F;

until $\ker H_{\Lambda^*} = \{0\}$ and G is a border basis for $B = S$.

☞ Computation of Λ^* by solving of a SDP problem by an interior point method (SeDuMi, CSDP, SDPA, ...)
☞ Applies for zero-dimensional real radical.
☞ Output a border basis of $\sqrt[\mathbb{R}]{(F)}$.

Bezoutian

- $f_0, f_1, \ldots, f_n \in R = \mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}]$.

Bezoutian

- $f_0, f_1, \ldots, f_n \in R = \mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}]$.
- $R \otimes R = \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n] = \mathbb{K}[\mathbf{x}, \mathbf{y}]$.
- $X_{(0)} = (x_1, \ldots, x_n)$, $X_{(1)} = (y_1, x_2 \ldots, x_n)$, ..., $X_{(n)} = (y_1, \ldots, y_n)$.
- $\partial_i(P) = \frac{P(X_{(i)}) - P(X_{(i-1)})}{y_i - x_i}$.

Bezoutian

- $f_0, f_1, \ldots, f_n \in R = \mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}]$.
- $R \otimes R = \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n] = \mathbb{K}[\mathbf{x}, \mathbf{y}]$.
- $X_{(0)} = (x_1, \ldots, x_n)$, $X_{(1)} = (y_1, x_2 \ldots, x_n), \ldots, X_{(n)} = (y_1, \ldots, y_n)$.
- $\partial_i(P) = \frac{P(X_{(i)}) - P(X_{(i-1)})}{y_i - x_i}$.

Bezoutian polynomial:

$$\Theta_{f_0, f_1, \ldots, f_n} = \begin{vmatrix} f_0(X_{(0)}) & \partial_1(f_0) & \cdots & \partial_n(f_0) \\ \vdots & \vdots & & \vdots \\ f_n(X_{(0)}) & \partial_1(f_n) & \cdots & \partial_n(f_n) \end{vmatrix} = \sum_{\alpha,\beta} \theta_{\alpha,\beta}\, \mathbf{x}^{\alpha} \mathbf{y}^{\beta}$$

Bezoutian

- $f_0, f_1, \ldots, f_n \in R = \mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}]$.
- $R \otimes R = \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n] = \mathbb{K}[\mathbf{x}, \mathbf{y}]$.
- $X_{(0)} = (x_1, \ldots, x_n)$, $X_{(1)} = (y_1, x_2 \ldots, x_n), \ldots$, $X_{(n)} = (y_1, \ldots, y_n)$.
- $\partial_i(P) = \frac{P(X_{(i)}) - P(X_{(i-1)})}{y_i - x_i}$.

Bezoutian polynomial:

$$\Theta_{f_0, f_1, \ldots, f_n} = \begin{vmatrix} f_0(X_{(0)}) & \partial_1(f_0) & \cdots & \partial_n(f_0) \\ \vdots & \vdots & & \vdots \\ f_n(X_{(0)}) & \partial_1(f_n) & \cdots & \partial_n(f_n) \end{vmatrix} = \sum_{\alpha,\beta} \theta_{\alpha,\beta}\, \mathbf{x}^{\alpha} \mathbf{y}^{\beta}$$

Bezoutian matrix: $B_{f_0, \ldots, f_n} = B_{f_0} = (\theta_{\alpha,\beta})_{\alpha,\beta}$.

Reduction

Apply the pencil reduction algorithm applied to $[B_1, B_{x_1}, \ldots, B_{x_n}]$ in order to obtain matrices

$$[\Delta_0, \Delta_1, \ldots, \Delta_n]$$

such that

- Δ_0 inversible,
- $\Delta_i(\mathbf{x}, \mathbf{y}) \equiv x_i \, \Delta_0(\mathbf{x}, \mathbf{y}) \mod I(\mathbf{x}) \qquad \equiv y_i \, \Delta_0(\mathbf{x}, \mathbf{y}) \mod I(\mathbf{y})$.

Reduction

Apply the pencil reduction algorithm applied to $[B_1, B_{x_1}, \ldots, B_{x_n}]$ in order to obtain matrices

$$[\Delta_0, \Delta_1, \ldots, \Delta_n]$$

such that

- Δ_0 inversible,
- $\Delta_i(\mathbf{x}, \mathbf{y}) \equiv x_i \, \Delta_0(\mathbf{x}, \mathbf{y}) \mod I(\mathbf{x}) \qquad \equiv y_i \, \Delta_0(\mathbf{x}, \mathbf{y}) \mod I(\mathbf{y})$.

Let I_0 be the intersection of primary components of the *isolated points* of $I = (f_1, \ldots, f_n)$.

Reduction

Apply the pencil reduction algorithm applied to $[B_1, B_{x_1}, \ldots, B_{x_n}]$ in order to obtain matrices

$$[\Delta_0, \Delta_1, \ldots, \Delta_n]$$

such that

- Δ_0 inversible,
- $\Delta_i(\mathbf{x}, \mathbf{y}) \equiv x_i \, \Delta_0(\mathbf{x}, \mathbf{y}) \mod I(\mathbf{x}) \qquad \equiv y_i \, \Delta_0(\mathbf{x}, \mathbf{y}) \mod I(\mathbf{y})$.

Let I_0 be the intersection of primary components of the *isolated points* of $I = (f_1, \ldots, f_n)$.

☞ **Bezoutian conjecture:** *The matrices $M_i = \Delta_0^{-1} \Delta_i$ are the matrices of multiplication by x_i in the basis B of R/I_0 where B is the set of monomials indexing the columns of Δ_0.*

(conjecture in [C'95], proved under some hypothesis on B in [M'05]).

Reduction

Apply the pencil reduction algorithm applied to $[B_1, B_{x_1}, \ldots, B_{x_n}]$ in order to obtain matrices

$$[\Delta_0, \Delta_1, \ldots, \Delta_n]$$

such that

- Δ_0 inversible,
- $\Delta_i(\mathbf{x}, \mathbf{y}) \equiv x_i \, \Delta_0(\mathbf{x}, \mathbf{y}) \mod I(\mathbf{x}) \qquad \equiv y_i \, \Delta_0(\mathbf{x}, \mathbf{y}) \mod I(\mathbf{y})$.

Let I_0 be the intersection of primary components of the *isolated points* of $I = (f_1, \ldots, f_n)$.

☞ **Bezoutian conjecture:** *The matrices $M_i = \Delta_0^{-1} \Delta_i$ are the matrices of multiplication by x_i in the basis B of R/I_0 where B is the set of monomials indexing the columns of Δ_0.*

(conjecture in [C'95], proved under some hypothesis on B in [M'05]).

☞ The flat extension theorem applies to a $\tau \in R^*$ such that $H_\tau = \Delta_0$ (another proof of the conjecture).

Reduction

Apply the pencil reduction algorithm applied to $[B_1, B_{x_1}, \ldots, B_{x_n}]$ in order to obtain matrices

$$[\Delta_0, \Delta_1, \ldots, \Delta_n]$$

such that

- Δ_0 inversible,
- $\Delta_i(\mathbf{x}, \mathbf{y}) \equiv x_i \, \Delta_0(\mathbf{x}, \mathbf{y}) \mod I(\mathbf{x}) \quad \equiv y_i \, \Delta_0(\mathbf{x}, \mathbf{y}) \mod I(\mathbf{y})$.

Let I_0 be the intersection of primary components of the *isolated points* of $I = (f_1, \ldots, f_n)$.

☞ **Bezoutian conjecture:** *The matrices $M_i = \Delta_0^{-1} \Delta_i$ are the matrices of multiplication by x_i in the basis B of R/I_0 where B is the set of monomials indexing the columns of Δ_0.*

(conjecture in [C'95], proved under some hypothesis on B in [M'05]).

☞ The flat extension theorem applies to a $\tau \in R^*$ such that $H_\tau = \Delta_0$ (another proof of the conjecture).

☞ The linear form $\tilde{\tau}$ extending τ is the **residue** of $f_1, \ldots, f_n$.

Alessandra Bernardi, Jérôme Brachat, Pierre Comon, and Bernard Mourrain.
General tensor decomposition, moment matrices and applications.
Journal of Symbolic Computation, (0):–, 2012.

Jérôme Brachat, Pierre Comon, Bernard Mourrain, and Elias P. Tsigaridas.
Symmetric tensor decomposition.
Linear Algebra and Applications, 433(11-12):1851–1872, 2010.

Jean-Bernard Lasserre, Monique Laurent, Bernard Mourrain, Philipp Rostalski, and Philippe Trébuchet.
Moment matrices, border bases and real radical computation.
Journal of Symbolic Computation, (0):–, 2012.

Monique Laurent and Bernard Mourrain.
A Sparse Flat Extension Theorem for Moment Matrices.
Archiv der Mathematik, 93:87–98, 2009.

Bernard Mourrain.
Bezoutian and quotient ring structure.
Journal of Symbolic Computation, 39(3-4):397–415, March 2005.

Bernard Mourrain and Victor Y. Pan.
Multivariate polynomials, duality and structured matrices.
Journal of Complexity, 16(1):110–180, 2000.

Thanks for your attention