.5cm.

Real solving polynomial equations with semidefinite programming

Jean Bernard Lasserre - Monique Laurent - Philipp Rostalski

LAAS, Toulouse - CWI, Amsterdam - ETH, Zürich

LAW 2008

The problem

Given polynomials $h_1, \dots, h_m \in \mathbb{R}[\mathbf{x}] = \mathbb{R}[\mathbf{x}_1, \dots, \mathbf{x}_n]$

- Compute all common **real roots** (assuming finitely many), i.e. compute the **real variety** $V_{\mathbb{R}}(I)$ of the ideal $I := (h_1, \dots, h_m)$

- Find a basis of the **real radical ideal** $I(V_{\mathbb{R}}(I))$

$$V_{\mathbb{R}}(I) := \{v \in \mathbb{R}^n \mid f(v) = 0 \; \forall f \in I\}$$

$$I(V_{\mathbb{R}}(I)) := \{f \in \mathbb{R}[\mathbf{x}] \mid f(v) = 0 \; \forall v \in V_{\mathbb{R}}(I)\}$$

$$\underbrace{=}_{\text{Real Nullstellensatz}} \quad \{f \in \mathbb{R}[\mathbf{x}] \mid \exists m \in \mathbb{N} \; s_i \in \mathbb{R}[\mathbf{x}] \;\; f^{2m} + \textstyle\sum_i s_i^2 \in I\}$$

Our contribution

1. A **semidefinite characterization** of $I(V_{\mathbb{R}}(I))$
[as the kernel of some positive semidefinite *moment matrix*]

2. Assuming $|V_{\mathbb{R}}(I)| < \infty$, an algorithm for finding:
- a generating set (**border** or **Gröbner basis**) of $I(V_{\mathbb{R}}(I))$
- the **real variety** $V_{\mathbb{R}}(I)$

Remarks about the method:
- *real algebraic* in nature: no complex roots computed
- works if $V_{\mathbb{R}}(I)$ is finite (even if $V_{\mathbb{C}}(I)$ is not)
- no preliminary Gröbner basis of I is needed
- *numerical*, based on semidefinite programming (SDP)

Plan of the talk

1. The moment-matrix method for $V_{\mathbb{R}}(I)$

2. Adapt the moment-matrix method for $V_{\mathbb{C}}(I)$ [drop PSD]

3. Relate to the ‘prolongation-projection’ algorithm of Zhi and Reid for $V_{\mathbb{C}}(I)$

4. Adapt the prolongation-projection algorithm for $V_{\mathbb{R}}(I)$ [add PSD]

The complex case is well understood

Given an ideal $I \subseteq \mathbb{R}[\mathbf{x}]$ with $|V_{\mathbb{C}}(I)| < \infty$,
find the **(complex) variety** $V_{\mathbb{C}}(I)$ and the **radical ideal** $I(V_{\mathbb{C}}(I))$.

Linear algebra in the finite dimensional space $\mathbb{R}[\mathbf{x}]/I$
$\rightsquigarrow$ Need a linear basis of $\mathbb{R}[\mathbf{x}]/I$ and a normal form algorithm

$V_{\mathbb{C}}(I)$ can be computed e.g. with:
• Linear algebra methods: $\rightsquigarrow$ **Eigenvalue method**
[Stetter-Möller, Stickelberger, Rouillier]
• Homotopy methods [Verschelde] ...

Seidenberg [1974]: $I(V_{\mathbb{C}}(I)) = (I \cup \{q_1, \ldots, q_n\})$, where
q_i is the square-free part of p_i, the monic generator of $I \cap \mathbb{R}[\mathbf{x}_i]$.

The eigenvalue method for $|V_{\mathbb{C}}(I)| < \infty$, i.e. $\dim \mathbb{R}[\mathbf{x}]/I < \infty$

Stickelberger theorem:
Let m_f be the *'multiplication by f' linear operator* in $\mathbb{R}[\mathbf{x}]/I$.

1. The **eigenvalues** of m_f are $\{f(v) \mid v \in V_{\mathbb{C}}(I)\}$.

2. The eigenvectors of m_f^T give the points $v \in V_{\mathbb{C}}(I)$.

$$M_f^T \zeta_{\mathcal{B},v} = f(v)\zeta_{\mathcal{B},v} \quad \forall\, v \in V_{\mathbb{C}}(I)$$

where M_f is the matrix of m_f in a base $\mathcal{B}$ of $\mathbb{R}[\mathbf{x}]/I$ and $\zeta_{\mathcal{B},v} := (b(v))_{b\in\mathcal{B}}$

Moreover, when $\mathcal{B}$ is a set of monomials and $1 \in \mathcal{B}$, a **border basis** of I can be read directly from the multiplication matrices $M_{x_1}, \ldots, M_{x_n}$.

Finding a linear basis $\mathcal{B}$ of $\mathbb{R}[\mathbf{x}]/I$ and a basis G of the ideal I

- Typically: G is a **Gröbner basis** and $\mathcal{B}$ is the set of **standard monomials** for a given monomial ordering (e.g. via Buchberger's algorithm)

- More generally: Assume $\mathcal{B} = \{b_1 = 1, b_2, \ldots, b_N\}$ is a set of monomials with **border** $\partial\mathcal{B} := (\mathbf{x}_1\mathcal{B} \cup \ldots \cup \mathbf{x}_n\mathcal{B}) \setminus \mathcal{B}$.
Write any border monomial

$$\mathbf{x}_i b_j = \underbrace{\sum_{k=1}^{N} a_k^{(ij)} b_k}_{\in \mathrm{Span}(\mathcal{B})} + \underbrace{g^{(ij)}}_{\in I}$$

Then: $G := \{g^{(ij)} \mid \mathbf{x}_i b_j \in \partial\mathcal{B}\}$ is a (border) basis of I and carries the ***same information*** as the multiplication matrices $M_{\mathbf{x}_1}, \ldots, M_{\mathbf{x}_n}$

Counting real roots with the Hermite quadratic form

For $f \in \mathbb{R}[\mathbf{x}]$

Hermite bilinear form:

$$\begin{aligned} H_f : \quad & \mathbb{R}[\mathbf{x}]/I \times \mathbb{R}[\mathbf{x}]/I \to \mathbb{R} \\ & (g,h) \mapsto \mathrm{Tr}(M_{fgh}) \end{aligned}$$

Theorem: For $f = 1$

$$\mathrm{rank}(H_1) = |V_{\mathbb{C}}(I)|, \ \mathrm{Sign}(H_1) = |V_{\mathbb{R}}(I)|, \ \mathrm{Rad}\,(H_1) = I(V_{\mathbb{C}}(I))$$

- $\mathrm{rank}(H_f) = |\{v \in V_{\mathbb{C}}(I) \mid f(v) \neq 0\}|$
- $\mathrm{Sign}(H_f)$

  $= |\{v \in V_{\mathbb{R}}(I) \mid f(v) > 0\}| - |\{v \in V_{\mathbb{R}}(I) \mid f(v) < 0\}|$

To find $V_{\mathbb{R}}(I)$ and a basis of the real radical ideal $I(V_{\mathbb{R}}(I))$ ...

... it suffices to have a **linear basis** $\mathcal{B}$ of $\mathbb{R}[\mathbf{x}]/I(V_{\mathbb{R}}(I))$ and the **multiplication matrices** in $\mathbb{R}[\mathbf{x}]/I(V_{\mathbb{R}}(I))$!

New tool: Moment matrices

$$y \in \mathbb{R}^{\mathbb{N}^n_{2s}} \rightsquigarrow M_s(y) := (y_{\alpha+\beta})_{\alpha,\beta \in \mathbb{N}^n_s}$$

$$\mathbb{N}^n_s := \{\alpha \in \mathbb{N}^n \mid |\alpha| = \sum_i \alpha_i \leq s\}$$

$\rightsquigarrow$ monomials $\mathbf{x}^\alpha$ of degree $\leq s$

Motivation: For $y = (v^\alpha)_{\alpha \in \mathbb{N}^n_{2s}} =: \zeta_{2s,v}$ where $v \in \mathbb{R}^n$

$$M_s(y) = \zeta_{s,v}\zeta_{s,v}^T \succeq 0 \quad \text{and} \quad \text{Ker} M_s(y) \subseteq I(v)$$

Real roots of $I = (h_1, \ldots, h_m)$ and PSD moment matrices

Lemma: For $v \in V_{\mathbb{R}}(I)$ and $t \geq D := \max_j \deg(h_j)$ the vector $y = \zeta_{t,v} = (v^\alpha)_{|\alpha| \leq t}$ satisfies:

- the linear constraints **(LC)**: $[v \in V_{\mathbb{C}}(I)]$

$$y^T(h_j \vec{\mathbf{x}}^\alpha) = 0 \quad \forall j = 1 \ldots m \;\; \forall \alpha \text{ s.t. } |\alpha| + \deg(h_j) \leq t$$

- the PSD constraint: $M_{\lfloor t/2 \rfloor}(y) \succeq 0$ $\quad [v \in \mathbb{R}^n]$

Set: $\mathcal{K}_t := \{ y \in \mathbb{R}^{\mathbb{N}^n_t} \mid \text{(LC)}, \;\; M_{\lfloor t/2 \rfloor}(y) \succeq 0 \}$

Obviously: $\mathcal{K}_t \supseteq \text{cone}(\zeta_{t,v} \mid v \in V_{\mathbb{R}}(I))$

Theorem: $\exists t \geq s \geq D \quad \pi_s(\mathcal{K}_t) = \text{cone}(\zeta_{s,v} \mid v \in V_{\mathbb{R}}(I))$

Semidefinite characterization of $I(V_{\mathbb{R}}(I))$

> **Theorem 1:** Let y be a **generic element** of $\mathcal{K}_t$, i.e. y lies in the **relative interior** of the cone $\mathcal{K}_t$. Then
> $$(\mathrm{Ker} M_{\lfloor t/2 \rfloor}(y)) \subseteq I(V_{\mathbb{R}}(I))$$
> with equality for t large enough.

• **Geometric property of SDP:**
y is generic $\Longleftrightarrow$ $\mathrm{rank} M_{\lfloor t/2 \rfloor}(y)$ is maximum
$\Longleftrightarrow \mathrm{Ker} M_{\lfloor t/2 \rfloor}(y) \subseteq \mathrm{Ker} M_{\lfloor t/2 \rfloor}(z) \;\; \forall z \in \mathcal{K}_t$

Thus: for $v \in V_{\mathbb{R}}(I)$, $\mathrm{Ker} M_{\lfloor t/2 \rfloor}(y) \subseteq \mathrm{Ker} M_{\lfloor t/2 \rfloor}(\zeta_{t,v}) \subseteq I(v)$.

• Let $\{g_1, \ldots, g_L\}$ be a basis of $I(V_{\mathbb{R}}(I))$.
Real Nullstellensatz: $g_l^{2m} + \sum_i s_i^2 = \sum_{j=1}^m u_j h_j$.
This implies: $g_l \in \mathrm{Ker} M_{\lfloor t/2 \rfloor}(y)$ for t large enough.

Stopping criterion when $|V_{\mathbb{R}}(I)| < \infty$

Theorem 2: Let y be a **generic** element of $\mathcal{K}_t$.
Assume one of the following two *flatness conditions* holds:

(F1) $\operatorname{rank} M_s(y) = \operatorname{rank} M_{s-1}(y)$ for some $D \leq s \leq \lfloor t/2 \rfloor$

(Fd) $\operatorname{rank} M_s(y) = \operatorname{rank} M_{s-d}(y)$ for some $d = \lceil D/2 \rceil \leq s \leq \lfloor t/2 \rfloor$.

Then:

- $I(V_{\mathbb{R}}(I)) = (\operatorname{Ker} M_s(y))$
- Any base $\mathcal{B}$ of the column space of $M_{s-1}(y)$ is a base of $\mathbb{R}[\mathbf{x}]/I(V_{\mathbb{R}}(I))$
- The multiplication matrices can be constructed from $M_s(y)$.

Sketch of proof: Assume $\text{rank} M_s(y) = \text{rank} M_{s-1}(y)$

- **Thm** [Curto-Fialkow 1996] $\pi_{2s}(y)$ has a **flat extension** $\tilde{y} \in \mathbb{R}^{\mathbb{N}^n}$, i.e. such that $\text{rank} M(\tilde{y}) = \text{rank} M_s(y)$.

- **Thm** [La 2005] As $M(\tilde{y}) \succeq 0$, $(\text{Ker} M_s(y)) = \text{Ker} M(\tilde{y})$ is a **real radical 0-dimensional ideal.**

- $I \underbrace{\subseteq}_{(LC)} (\text{Ker} M_s(y)) \underbrace{\subseteq}_{y \text{ generic}} I(V_{\mathbb{R}}(I))$

Thus: $(\text{Ker} M_s(y)) = I(V_{\mathbb{R}}(I))$

- $\mathcal{B}$ indexes a base of $M_{s-1}(y) \Longrightarrow \mathcal{B}$ indexes a base of $M(\tilde{y})$ $\Longrightarrow \mathcal{B}$ is a base of $\mathbb{R}[\mathbf{x}]/\text{Ker} M(\tilde{y}) = \mathbb{R}[\mathbf{x}]/I(V_{\mathbb{R}}(I))$

$\rightsquigarrow$ Use linear dependencies in $M_s(y)$ to construct the multiplication matrices.

The moment-matrix algorithm for $V_{\mathbb{R}}(I)$

Input: $h_1, \ldots, h_m \in \mathbb{R}[\mathbf{x}]$
Output: $\mathcal{B}$ base of $\mathbb{R}[\mathbf{x}]/I(V_{\mathbb{R}}(I))$
The multiplication matrices $M_{\mathbf{x}_i}$ in $\mathbb{R}[\mathbf{x}]/I(V_{\mathbb{R}}(I))$

Algorithm: For $t \geq D$

Step 1: Compute a generic element $y \in \mathcal{K}_t$.

Step 2: Check if (F1) or (Fd) holds.

If **yes**, return a column basis $\mathcal{B}$ of $M_{s-1}(y)$ and $M_{\mathbf{x}_i} = M_{\mathcal{B}}^{-1} P_i$,

- $M_{\mathcal{B}}$:= principal submatrix of $M_{s-1}(y)$ indexed by $\mathcal{B}$
- P_i:= submatrix of $M_s(y)$ with rows in $\mathcal{B}$ and columns in $\mathbf{x}_i\mathcal{B}$.

If **no**, go to Step 1 with $t \to t+1$.

Theorem: The algorithm terminates.

The algorithm terminates: (F1) holds for t large enough.

- For $t \geq t_0$, $\mathrm{Ker} M_{\lfloor t/2 \rfloor}(y)$ contains a Gröbner base $\{g_1, \ldots, g_L\}$ of $I(V_{\mathbb{R}}(I))$ for a total degree ordering.

- $\mathcal{B} := \{b_1, \ldots, b_N\}$: set of standard monomials $\rightsquigarrow$ base of $\mathbb{R}[\mathbf{x}]/I(V_{\mathbb{R}}(I))$.

Set: $s := 1 + \max_{b \in \mathcal{B}} \deg(b)$ and assume $t \geq t_0$, $\lfloor t/2 \rfloor > s$.

For $|\alpha| \leq s$, write $x^\alpha = \underbrace{\sum_{i=1}^{N} \lambda_i b_i}_{\deg \leq s-1} + \underbrace{\sum_{l=1}^{L} u_l g_l}_{\deg \leq |\alpha| \leq s < \lfloor t/2 \rfloor}$

Thus: $x^\alpha - \sum_{i=1}^{N} \lambda_i b_i \in \mathrm{Ker} M_{\lfloor t/2 \rfloor}(y)$.

That is: $\mathrm{rank} M_s(y) = \mathrm{rank} M_{s-1}(y)$.

Two small examples

Ex. 1: $I = (h := \mathbf{x}_1^2 + \mathbf{x}_2^2)$

$V_{\mathbb{R}}(I) = \{0\}$, $|V_{\mathbb{C}}(I)| = \infty$.

$M_1(y) \succeq 0,\ 0 = y^T \vec{h} = y_{20} + y_{02} \Longrightarrow y_\alpha = 0 \ \forall \alpha \neq 0$.

$\rightsquigarrow$ Any generic $y \in K_2$ is $y = (y_0, 0, \ldots, 0)$ with $y_0 > 0$.

Thus: $(\mathrm{Ker}\, M_1(y)) = (\mathbf{x}_1, \mathbf{x}_2) = I(V_{\mathbb{R}}(I))$.

Ex. 2: $I = (h_i := \mathbf{x}_i(\mathbf{x}_i^2 + 1) \mid i = 1, \ldots, n)$

$V_{\mathbb{R}}(I) = \{0\}$, $|V_{\mathbb{C}}(I)| = 3^n$.

$M_2(y) \succeq 0,\ 0 = y^T (\mathbf{x}_i \vec{h}_i) = y_{4e_i} + y_{2e_i} \ \forall i \Longrightarrow y_\alpha = 0 \ \forall \alpha \neq 0$.

$\rightsquigarrow$ Any generic $y \in K_4$ is $y = (y_0, 0, \ldots, 0)$ with $y_0 > 0$.

Thus: $(\mathrm{Ker}\, M_1(y)) = (\mathbf{x}_1, \ldots, \mathbf{x}_n) = I(V_{\mathbb{R}}(I))$.

Some algorithmic issues

How to find a generic $y \in \mathcal{K}_t$**, i.e. with** $\mathrm{rank} M_t(y)$ **max. ?**

Solve the SDP program: $\min_{y \in \mathcal{K}_t} 1$ with a SDP solver using the ‘extended self-dual embedding property’.

Then the central path converges to a solution in the relative interior of the optimum face, i.e., to a **generic** point $y \in \mathcal{K}_t$.

How to compute ranks of matrices ?

We use SVD decomposition, but this is a sensitive numerical issue ...

The method may work without (F1) or (Fd):
If $\mathrm{rank} M_{\mathcal{B}}(y) = \mathrm{rank} M_{\mathcal{B} \cup \partial \mathcal{B}}(y)$ and the formal multiplication matrices commute.

Extension of the moment-matrix algorithm to $V_{\mathbb{C}}(I)$

Omit the PSD condition and work with the **linear** space:

$$K_t = \{y \in \mathbb{R}^{\mathbb{N}^n_t} \mid y^T(h_j \vec{\mathbf{x}}^\alpha) = 0 \ \ \forall j, \alpha \text{ with } |\alpha| + \deg(h_j) \le t\}$$

The *same* algorithm applies: For $t \ge D$

- Pick **generic** $y \in K_t$, i.e. $\mathrm{rank} M_s(y)$ maximum $\ \forall s \le \lfloor t/2 \rfloor$
  [choose $y \in K_t$ randomly]
- Check if the flatness condition (F1) or (Fd) holds.
- If yes, find a basis of $\mathbb{R}[\mathbf{x}]/J$ where $J := (\mathrm{Ker} M_s(y))$ satisfies $I \subseteq J \subseteq I(V_{\mathbb{C}}(I))$ and thus $V_{\mathbb{C}}(J) = V_{\mathbb{C}}(I)$.
- If not, iterate with $t + 1$.

Find the ideal $(\mathrm{Ker} M_s(y)) = I$ in the Gorenstein case

The inclusion $I \subseteq (\mathrm{Ker} M_s(y)) \subseteq I(V_{\mathbb{C}}(I))$ may be strict for any generic y.

Example: For $I = (\mathbf{x}_1^2, \mathbf{x}_2^2, \mathbf{x}_1\mathbf{x}_2)$, $V_{\mathbb{C}}(I) = \{0\}$, $I(V_{\mathbb{C}}(I)) = (\mathbf{x}_1, \mathbf{x}_2)$, $\dim \mathbb{R}[\mathbf{x}]/I = 3$, $\dim \mathbb{R}[\mathbf{x}]/I(V_{\mathbb{C}}(I)) = 1$, while $\dim \mathbb{R}[\mathbf{x}]/(\mathrm{Ker} M_s(y)) = 2$ for any generic y !

Recall: The algebra $\mathcal{A} := \mathbb{R}[\mathbf{x}]/I$ is *Gorenstein* if there exists a non-degenerate bilinear form on $\mathcal{A}$ satisfying $(f, gh) = (fg, h)$ $\forall f, g, h \in \mathcal{A}$, i.e. if there exists $y \in K_\infty$ with $I = \mathrm{Ker} M(y)$

Hence: $\exists y \in K_t$ s.t. $\mathrm{rank} M_s(y) = \mathrm{rank} M_{s-1}(y)$ and $I = (\mathrm{Ker} M_s(y))$ IFF $\mathcal{A}$ is Gorenstein.

Example: the moment-matrix algorithm for real/complex roots

$I = (\mathbf{x}_1^2 - 2\mathbf{x}_1\mathbf{x}_3 + 5,\ \mathbf{x}_1\mathbf{x}_2^2 + \mathbf{x}_2\mathbf{x}_3 + 1,\ 3\mathbf{x}_2^2 - 8\mathbf{x}_1\mathbf{x}_3)$, $D = 3$, $d = 2$

Ranks of $M_s(y)$ for generic $y \in K_t$, $\mathcal{K}_t$:

	$t = 2$	3	4	5	6	7	8	9
$s = 0$	1	1	1	1	1	1	1	1
$s = 1$	4	4	4	4	4	4	4	4
$s = 2$			8	8	8	8	8	**8**
$s = 3$					11	10	9	**8**
$s = 4$							12	10

no PSD $\rightsquigarrow$ 8 complex roots

	$t = 2$	3	4	5	6
$s = 0$	1	1	1	1	1
$s = 1$	4	4	4	2	**2**
$s = 2$			8	8	**2**
$s = 3$					10

with PSD $\rightsquigarrow$ extract 2 real roots

8 complex / 2 real roots:

$$v_1 = \left[\; -1.101, -2.878, -2.821 \; \right]$$

$$v_2 = \left[\; 0.07665 + 2.243i, 0.461 + 0.497i, 0.0764 + 0.00834i \; \right]$$

$$v_3 = \left[\; 0.07665 - 2.243i, 0.461 - 0.497i, 0.0764 - 0.00834i \; \right]$$

$$v_4 = \left[\; -0.081502 - 0.93107i, 2.350 + 0.0431i, -0.274 + 2.199i \; \right]$$

$$v_5 = \left[\; -0.081502 + 0.93107i, 2.350 - 0.0431i, -0.274 - 2.199i \; \right]$$

$$v_6 = \left[\; 0.0725 + 2.237i, -0.466 - 0.464i, 0.0724 + 0.00210i \; \right]$$

$$v_7 = \left[\; 0.0725 - 2.237i, -0.466 + 0.464i, 0.0724 - 0.00210i \; \right]$$

$$v_8 = \left[\; 0.966, -2.813, 3.072 \; \right]$$

Extracting real roots without (F1) or (Fd)

$I = (5\mathbf{x}_1^9 - 6\mathbf{x}_1^5\mathbf{x}_2 + \mathbf{x}_1\mathbf{x}_2^4 + 2\mathbf{x}_1\mathbf{x}_3, -2\mathbf{x}_1^6\mathbf{x}_2 + 2\mathbf{x}_1^2\mathbf{x}_2^3 + 2\mathbf{x}_2\mathbf{x}_3, \mathbf{x}_1^2 + \mathbf{x}_2^2 - 0.265625)$

$D = 9$, $d = 5$, $|V_{\mathbb{R}}(I)| = 8$, $|V_{\mathbb{C}}(I)| = 20$

order t	rank sequence of $M_s(y)$ $(1 \leq s \leq \lfloor t/2 \rfloor)$	extract. order s MON/SVD	accuracy MON/SVD	comm. error MON/SVD
10	1 4 8 16 25 34	—	—	—
12	1 3 9 15 22 26 32	—	—	—
14	1 3 8 10 12 16 20 24	3(3)/—(—)	0.12786/—	0.00019754/—
16	1 4 8 8 8 12 16 20 24	4(3)/3(3)	4.6789e-5/0.00013406	4.7073e-5/0.00075005

Quotient basis: $\mathcal{B} = \{1, \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_1^2, \mathbf{x}_1\mathbf{x}_2, \mathbf{x}_1\mathbf{x}_3, \mathbf{x}_2\mathbf{x}_3\}$ $\rightsquigarrow$ border basis G of size 10

Real solutions:

$$\begin{cases} x_1 = (-0.515, -0.000153, -0.0124) & x_2 = (-0.502, 0.119, 0.0124) \\ x_3 = (0.502, 0.119, 0.0124) & x_4 = (0.515, -0.000185, -0.0125) \\ x_5 = (0.262, 0.444, -0.0132) & x_6 = (-2.07\text{e-}5, 0.515, -1.27\text{e-}6) \\ x_7 = (-0.262, 0.444, -0.0132) & x_8 = (-1.05\text{e-}5, -0.515, -7.56\text{e-}7) \end{cases}$$

Link with the elimination method of Zhi and Reid

Theorem: If (F1) holds, i.e. for some $D \leq s \leq \lfloor t/2 \rfloor$

$$\mathrm{rank} M_s(y) = \mathrm{rank} M_{s-1}(y) \quad \text{for generic } y \in K_t,$$

then

$$\boxed{\dim \pi_{2s}(K_t) = \dim \pi_{2s-1}(K_t) = \dim \pi_{2s}(K_{t+1})}$$

Theorem (based on [Zhi-Reid 2004]): If for some $D \leq s \leq t$

$$\boxed{\text{(ZR)} \quad \dim \pi_s(K_t) = \dim \pi_{s-1}(K_t) = \dim \pi_s(K_{t+1})}$$

then one can construct a base of $\mathbb{R}[\mathbf{x}]/I$ and the multiplication matrices in $\mathbb{R}[\mathbf{x}]/I$ [and thus extract $V_{\mathbb{C}}(I)$].

Hence: The Zhi-Reid criterion (ZR) may be satisfied earlier than the flatness criterion (F1).

Example: $I = (\mathbf{x}_1^2 - 2\mathbf{x}_1\mathbf{x}_3 + 5, \mathbf{x}_1\mathbf{x}_2^2 + \mathbf{x}_2\mathbf{x}_3 + 1, 3\mathbf{x}_2^2 - 8\mathbf{x}_1\mathbf{x}_3)$

	$t=2$	3	4	5	6	7	8	9
$s=0$	1	1	1	1	1	1	1	1
$s=1$	4	4	4	4	4	4	4	4
$s=2$			8	8	8	8	8	**8**
$s=3$					11	10	9	**8**
$s=4$							12	10

$\text{rank} M_3(y) = \text{rank} M_2(y)$

for $y \in K_9$

	$t=3$	4	5	6	7	8	9
$s=1$	4	4	4	4	4	4	4
$s=2$	8	8	8	8	8	8	8
$s=3$	11	10	9	8	8	8	8
$s=4$		12	10	9	8	8	8
$s=5$			12	10	9	8	8
$s=6$				12	10	9	8
$s=7$					12	10	9
$s=8$						12	10
$s=9$							12

$\dim \pi_3(\mathcal{K}_6)$

$= \dim \pi_2(\mathcal{K}_6)$

$= \dim \pi_3(\mathcal{K}_7)$

Extending the Zhi-Reid criterion to the real case

- In the **complex** case, $K_t = \mathcal{H}_t{}^{\perp}$ where

$$\mathcal{H}_t := \{h_j \mathbf{x}^\alpha \quad \forall j, \alpha \text{ with } \deg(h_j \mathbf{x}^\alpha) \leq t\}.$$

- In the **real** case, $\mathcal{K}_t$ is a cone, contained in the linear space $\mathcal{P}_t^{\perp}$, with the same dimensions: $\dim \mathcal{K}_t = \dim \mathcal{P}_t^{\perp}$, where

$$\mathcal{P}_t := \mathcal{H}_t \cup \{f \mathbf{x}^\alpha \mid f \in \operatorname{Ker} M_{\lfloor t/2 \rfloor}(y),\ \deg(\mathbf{x}^\alpha) \leq \lfloor t/2 \rfloor\}$$

Theorem: If for some $D \leq s \leq t$

$$\text{(ZR+)} \quad \dim \pi_s(\mathcal{P}_t^{\perp}) = \dim \pi_{s-1}(\mathcal{P}_t^{\perp}) = \dim \pi_s((\mathcal{P}_t \cup \partial \mathcal{P}_t)^{\perp})$$

then one can construct a base of J with $I \subseteq J \subseteq I(V_{\mathbb{R}}(I))$ and thus extract $V_{\mathbb{R}}(I) = V_{\mathbb{C}}(J) \cap \mathbb{R}^n$.

Link with the flatness criterion

Theorem: In the PSD case, the flatness criterion (F1):

$$\mathrm{rank} M_s(y) = \mathrm{rank} M_{s-1}(y) \quad \text{for generic } y \in \mathcal{K}_t$$

is **equivalent** to the stronger version of the (ZR) criterion:

$$\text{(ZR++)} \quad \dim \pi_{s-1}(\mathcal{P}_t^{\perp}) = \dim \pi_{2s}(\mathcal{P}_t^{\perp}) = \dim \pi_{2s}((\mathcal{P}_t \cup \partial \mathcal{P}_t)^{\perp})$$

in which case we find the real radical ideal $J = I(V_{\mathbb{R}}(I))$.

Hence: the algorithm based on (ZR) may stop earlier than the moment-matrix algorithm, based on (F1).

Future work: Adapt other known efficient algorithms for complex roots to *real* roots by incorporating SDP conditions.