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 $h_1, \ldots, h_m \in \mathbb{R}[x] = \mathbb{R}[x_1, \ldots, x_n]$

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

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

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

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

\[
= \{ f \in \mathbb{R}[x] \mid \exists m \in \mathbb{N} \ s_i \in \mathbb{R}[x] \ f^{2m} + \sum_i s_i^2 \in I \}
\]

**Real Nullstellensatz**
Our contribution

1. A semidefinite characterization of $I(V_R(I))$
   [as the kernel of some positive semidefinite moment matrix]

2. Assuming $|V_R(I)| < \infty$, an algorithm for finding:
   • a generating set (border or Gröbner basis) of $I(V_R(I))$
   • the real variety $V_R(I)$

Remarks about the method:
• real algebraic in nature: no complex roots computed
• works if $V_R(I)$ is finite (even if $V_C(I)$ 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 $V_R(I)$

2. Adapt the moment-matrix method for $V_C(I)$ [drop PSD]

3. Relate to the ‘prolongation-projection’ algorithm of Zhi and Reid for $V_C(I)$

4. Adapt the prolongation-projection algorithm for $V_R(I)$ [add PSD]
The complex case is well understood

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

Linear algebra in the finite dimensional space \( \mathbb{R}[x]/I \)

\( \sim \) Need a linear basis of \( \mathbb{R}[x]/I \) and a normal form algorithm

\( V_C(I) \) can be computed e.g. with:

- Linear algebra methods: \( \sim \) **Eigenvalue method** [Stetter-Möller, Stickelberger, Rouillier]

- Homotopy methods [Verschelde] . . .

**Seidenberg [1974]:** \( I(V_C(I)) = (I \cup \{q_1, \ldots, q_n\}) \), where \( q_i \) is the square-free part of \( p_i \), the monic generator of \( I \cap \mathbb{R}[x_i] \).
The eigenvalue method for $|V_{\mathbb{C}}(I)| < \infty$, i.e. $\dim \mathbb{R}[x]/I < \infty$

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

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 $v \in V_{\mathbb{C}}(I)$.

\[
M_f^T \zeta_B,v = f(v)\zeta_B,v \quad \forall \, v \in V_{\mathbb{C}}(I)
\]

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

Moreover, when $B$ is a set of monomials and $1 \in B$, a **border basis** of $I$ can be read directly from the multiplication matrices $M_{x_1}, \ldots, M_{x_n}$.
Finding a linear basis $B$ of $\mathbb{R}[x]/I$ and a basis $G$ of the ideal $I$

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

- More generally: Assume $B = \{b_1 = 1, b_2, \ldots, b_N\}$ is a set of monomials with **border** $\partial B := (x_1B \cup \ldots \cup x_nB) \setminus B$.

Write any border monomial $xib_j = \sum_{k=1}^{N} a_{k}^{(ij)} b_k + \underbrace{g^{(ij)} \in I}_{\in \text{Span}(B)}$

Then: $G := \{g^{(ij)} \mid xib_j \in \partial B\}$ is a (border) basis of $I$ and carries the **same information** as the multiplication matrices $M_{x_1}, \ldots, M_{x_n}$
Counting real roots with the Hermite quadratic form

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

Hermite bilinear form:

$$H_f : \mathbb{R}[x]/I \times \mathbb{R}[x]/I \to \mathbb{R}$$

$$(g, h) \mapsto \text{Tr}(M_{fgh})$$

Theorem: For $f = 1$

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


- $\text{rank}(H_f) = |\{v \in V_\mathbb{C}(I) \mid f(v) \neq 0\}|$
- $\text{Sign}(H_f)$
  $$= |\{v \in V_\mathbb{R}(I) \mid f(v) > 0\}| - |\{v \in V_\mathbb{R}(I) \mid f(v) < 0\}|$$
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 $\mathbb{R}[x]/I(V_{\mathbb{R}}(I))$ and the **multiplication matrices** in $\mathbb{R}[x]/I(V_{\mathbb{R}}(I))$!

**New tool: Moment matrices**

$$y \in \mathbb{R}^{N_{2s}} \leadsto M_s(y) := (y^{\alpha + \beta})_{\alpha, \beta \in \mathbb{N}^s}$$

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

$\leadsto$ monomials $x^\alpha$ of degree $\leq s$

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

$$M_s(y) = \zeta_{s,v}^T \zeta_{s,v} \succeq 0 \quad \text{and} \quad \text{Ker} M_s(y) \subseteq I(v)$$
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):
  \[
y^T(\hat{h}_jx^\alpha) = 0 \quad \forall j = 1 \ldots m \quad \forall \alpha \text{ s.t. } |\alpha| + \deg(h_j) \leq t
  \]

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

Set:
\[
\mathcal{K}_t := \{ y \in \mathbb{R}^{N_t^n} | \text{(LC), } M_{\lfloor t/2 \rfloor}(y) \succeq 0 \}
\]

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

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

**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

$$(\text{Ker} M_{\lfloor t/2 \rfloor}(y)) \subseteq I(V_R(I))$$

with equality for $t$ large enough.

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

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

- Let $\{g_1, \ldots, g_L\}$ be a basis of $I(V_R(I))$.
  **Real Nullstellensatz:** $g_l^{2m} + \sum_i s_i^2 = \sum_{j=1}^m u_j h_j$.
  This implies: $g_l \in \text{Ker} M_{\lfloor t/2 \rfloor}(y)$ 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) $\text{rank} M_s(y) = \text{rank} M_{s-1}(y)$ for some $D \leq s \leq \lfloor t/2 \rfloor$

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

Then:

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

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

- **Thm** [Curto-Fialkow 1996] $\pi_{2s}(y)$ has a flat extension $\tilde{y} \in \mathbb{R}^{N^n}$, 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.

- $I \subset (\text{Ker}M_s(y)) \subset I(\mathbb{V}_\mathbb{R}(I))$
  
  (LC') $y$ generic

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

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

  $\leadsto$ Use linear dependencies in $M_s(y)$ to construct the multiplication matrices.
The moment-matrix algorithm for $V_\mathbb{R}(I)$

**Input:** $h_1, \ldots, h_m \in \mathbb{R}[x]$

**Output:** $\mathcal{B}$ base of $\mathbb{R}[x]/I(V_\mathbb{R}(I))$

The multiplication matrices $M_{x_i}$ in $\mathbb{R}[x]/I(V_\mathbb{R}(I))$

**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 $M_{x_i} = M_{\mathcal{B}}^{-1} P_i$,  
- $M_{\mathcal{B}}$ := 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 $x_i \mathcal{B}$.

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

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

- For \( t \geq t_0 \), \( \text{Ker} M_{\lfloor t/2 \rfloor}(y) \) 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 \( \mathbb{R}[x]/I(V_{\mathbb{R}}(I)) \).

**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 \( x^\alpha = \sum_{i=1}^{N} \lambda_i b_i + \sum_{l=1}^{L} u_l g_l \)

\[ \begin{align*}
\text{deg} \leq s - 1 & \quad \text{deg} \leq |\alpha| \leq s < \lfloor t/2 \rfloor
\end{align*} \]

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

That is: \( \text{rank} M_s(y) = \text{rank} M_{s-1}(y) \).
Two small examples

**Ex. 1:** \( I = (h := x_1^2 + x_2^2) \)

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

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

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

**Thus:** \((\text{Ker}M_1(y)) = (x_1, x_2) = I(V_\mathbb{R}(I)).\)

**Ex. 2:** \( I = (h_i := x_i(x_i^2 + 1) \mid i = 1, \ldots, n) \)

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

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

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

**Thus:** \((\text{Ker}M_1(y)) = (x_1, \ldots, x_n) = I(V_\mathbb{R}(I)).\)
Some algorithmic issues

How to find a generic $y \in \mathcal{K}_t$, i.e. with $\text{rank} M_t(y)$ 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 $\text{rank} M_B(y) = \text{rank} M_{B \cup \partial B}(y)$ and the formal multiplication matrices commute.
Extension of the moment-matrix algorithm to $V_C(I)$

Omit the PSD condition and work with the linear space:

$$K_t = \{ y \in \mathbb{R}^{N_t^n} | y^T (h_j \tilde{x}^\alpha) = 0 \ \forall j, \alpha \text{ with } |\alpha| + \text{deg}(h_j) \leq t \}$$

The same algorithm applies: For $t \geq D$

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

Real solving polynomial equations with semidefinite programming – p.18
Find the ideal \((\text{Ker}\, M_s(y)) = I\) in the Gorenstein case

The inclusion \(I \subseteq (\text{Ker}\, M_s(y)) \subseteq I(\text{V}_C(I))\) may be strict for any generic \(y\).

**Example:** For \(I = (x_1^2, x_2^2, x_1 x_2)\), \(V_C(I) = \{0\}\), \(I(\text{V}_C(I)) = (x_1, x_2)\), \(\dim \mathbb{R}[x]/I = 3\), \(\dim \mathbb{R}[x]/I(\text{V}_C(I)) = 1\), while \(\dim \mathbb{R}[x]/(\text{Ker}\, M_s(y)) = 2\) for any generic \(y\)!

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

**Hence:** \(\exists y \in K_t\) s.t. \(\text{rank}\, M_s(y) = \text{rank}\, M_{s-1}(y)\) and \(I = (\text{Ker}\, M_s(y))\) IFF \(A\) is Gorenstein.
Example: the moment-matrix algorithm for real/complex roots

\[ I = (x_1^2 - 2x_1x_3 + 5, x_1x_2^2 + x_2x_3 + 1, 3x_2^2 - 8x_1x_3), \quad D = 3, \ d = 2 \]

**Ranks of** \( M_s(y) \) **for generic** \( y \in K_t, \ K_t \):

<table>
<thead>
<tr>
<th>( s = 0 )</th>
<th>( t = 2 )</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( s = 1 )</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>( s = 2 )</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>( s = 3 )</td>
<td>11</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( s = 4 )</td>
<td>12</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

no PSD \( \leadsto \) 8 complex roots

<table>
<thead>
<tr>
<th>( s = 0 )</th>
<th>( t = 2 )</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( s = 1 )</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>( s = 2 )</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>( s = 3 )</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

with PSD \( \leadsto \) extract 2 real roots
8 complex / 2 real roots:

\begin{align*}
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]
\end{align*}
Extracting real roots without (F1) or (Fd)

\[ I = (5x_1^9 - 6x_1^5x_2 + x_1x_2^4 + 2x_1x_3, -2x_1^6x_2 + 2x_1^2x_2^3 + 2x_2x_3, x_1^2 + x_2^2 - 0.265625) \]

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

<table>
<thead>
<tr>
<th>order ( t )</th>
<th>rank sequence of ( M_s(y) ) (1 ≤ s ≤ ([t/2]))</th>
<th>extract. order ( s )</th>
<th>accuracy</th>
<th>comm. error</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1 4 8 16 25 34</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>12</td>
<td>1 3 9 15 22 26 32</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>14</td>
<td>1 3 8 10 12 16 20 24</td>
<td>3(3)/—(—)</td>
<td>0.12786/—</td>
<td>0.00019754/—</td>
</tr>
<tr>
<td>16</td>
<td>1 4 8 8 8 12 16 20 24</td>
<td>4(3)/3(3)</td>
<td>4.6789e-5/0.00013406</td>
<td>4.7073e-5/0.00075005</td>
</tr>
</tbody>
</table>

Quotient basis: \( \mathcal{B} = \{1, x_1, x_2, x_3, x_1^2, x_1x_2, x_1x_3, x_2x_3\} \mapsto \) border basis \( \mathcal{G} \) of size 10

Real solutions:

\[
\begin{align*}
x_1 &= (-0.515, -0.000153, -0.0124) & x_2 &= (-0.502, 0.119, 0.0124) \\
x_3 &= (0.502, 0.119, 0.0124) & x_4 &= (0.515, -0.000185, -0.0125) \\
x_5 &= (0.262, 0.444, -0.0132) & x_6 &= (-2.07e-5, 0.515, -1.27e-6) \\
x_7 &= (-0.262, 0.444, -0.0132) & x_8 &= (-1.05e-5, -0.515, -7.56e-7)
\end{align*}
\]
Theorem: If (F1) holds, i.e. for some $D \leq s \leq \lfloor t/2 \rfloor$

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

then

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

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

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

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

Hence: The Zhi-Reid criterion (ZR) may be satisfied earlier than the flatness criterion (F1).
Example: $I = (x_1^2 - 2x_1 x_3 + 5, x_1 x_2^2 + x_2 x_3 + 1, 3x_2^2 - 8x_1 x_3)$

<table>
<thead>
<tr>
<th></th>
<th>$t = 2$</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s = 0$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$s = 1$</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>$s = 2$</td>
<td></td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>$s = 3$</td>
<td></td>
<td>11</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$s = 4$</td>
<td></td>
<td></td>
<td>12</td>
<td>10</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

for $y \in K_9$

<table>
<thead>
<tr>
<th></th>
<th>$t = 3$</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s = 1$</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>$s = 2$</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>$s = 3$</td>
<td>11</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>$s = 4$</td>
<td>12</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>$s = 5$</td>
<td>12</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>$s = 6$</td>
<td></td>
<td>12</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$s = 7$</td>
<td></td>
<td></td>
<td>12</td>
<td>10</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$s = 8$</td>
<td></td>
<td></td>
<td></td>
<td>12</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$s = 9$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$\text{dim} \pi_3(K_6) = \text{dim} \pi_2(K_6)

= \text{dim} \pi_3(K_7)$
Extending the Zhi-Reid criterion to the real case

• In the complex case, \( K_t = \mathcal{H}_t^\perp \) where
  \[
  \mathcal{H}_t := \{ h_j x^\alpha \; \forall j, \alpha \text{ with } \deg(h_j x^\alpha) \leq t \}.
  \]

• 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
  \[
  \mathcal{P}_t := \mathcal{H}_t \cup \{ f x^\alpha | f \in \text{Ker} M_{t/2}(y), \deg(x^\alpha) \leq \lfloor t/2 \rfloor \}
  \]

**Theorem:** If for some \( D \leq s \leq t \)

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

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):

\[ \text{rank} M_s(y) = \text{rank} M_{s-1}(y) \] 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.