.5cm.

Computing real radical ideals and real roots of polynomial equations with semidefinite programming

Jean Bernard Lasserre - Monique Laurent - Philipp Rostalski

LAAS, Toulouse - CWI, Amsterdam - UC Berkeley

Convex Algebraic geometry, Optimization, and Applications

AIM, September 2009

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** $\sqrt[\mathbb{R}]{I}$

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

$$\sqrt[\mathbb{R}]{I} \quad := \{f \in \mathbb{R}[x] \mid \exists m \in \mathbb{N}\; s_j \in \mathbb{R}[x] \;\; f^{2m} + \textstyle\sum_j s_j^2 \in I\}$$

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

Real Nullstellensatz: $\sqrt[\mathbb{R}]{I} = I(V_{\mathbb{R}}(I))$

A small example

Let $I = ((x_1^2 + x_2^2)^2) \subseteq \mathbb{R}[x_1, x_2]$

$V_{\mathbb{R}}(I) = \{(0,0)\}$

Real radical ideal: $\mathcal{I}(V_{\mathbb{R}}(I)) = (x_1, x_2)$

$V_{\mathbb{C}}(I) = \{(x_1, \pm i x_1) \mid x_1 \in \mathbb{C}\}$

Radical ideal: $\mathcal{I}(V_{\mathbb{C}}(I)) = (x_1^2 + x_2^2)$

Hilbert Nullstellensatz:

$$\mathcal{I}(V_{\mathbb{C}}(I)) = \sqrt{I} := \{f \in \mathbb{R}[x] \mid \exists m \in \mathbb{N}\ f^m \in I\}$$

Our contribution

1. A **semidefinite characterization** of $\sqrt[\mathbb{R}]{I}$
[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 $\sqrt[\mathbb{R}]{I}$
- 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]

5. Extensions?

The complex case is well understood

Problem: Given an ideal $I \subseteq \mathbb{R}[x]$ with $|V_{\mathbb{C}}(I)| < \infty$

- Compute the **(complex) variety** $V_{\mathbb{C}}(I)$
- Find a basis of the **radical ideal** $\sqrt{I}$

$V_{\mathbb{C}}(I)$ can be computed e.g. with:

- **Homotopy methods** [Sommese, Verschelde, Wampler, ...]

- **Elimination methods:** Find polynomials in I in '*triangular form*' $f_1 \in \mathbb{R}[x_1]$, $f_2 \in \mathbb{R}[x_1, x_2]$, $\ldots$, $f_n \in \mathbb{R}[x_1, \ldots, x_n]$ (via a Gröbner basis for a lexicographic monomial ordering [Buchberger,...])

• **Linear algebra methods:** Find the multiplication matrices in $\mathbb{R}[x]/I$ and compute their eigenvalues
$\rightsquigarrow$ The *eigenvalue method* [Stetter, Möller, Stickelberger,...]

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

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

Basic fact: $\dim \mathbb{R}[x]/I < \infty \Longleftrightarrow |V_{\mathbb{C}}(I)| < \infty$

The eigenvalue method: The univariate case

- Let $h = x^d - a_{d-1}x^{d-1} - \ldots - a_1 x - a_0$ and $I = (h)$
- $\mathcal{B} = \{1, x, \ldots, x^{d-1}\}$ is a linear basis of $\mathbb{R}[x]/I$
- The matrix of the '*multiplication (by x) operator*' in $\mathbb{R}/I$ is:

$$M_x = \begin{array}{c} \\ 1 \\ x \\ \vdots \\ x^{d-1} \end{array} \begin{array}{c} \begin{array}{cccc} x & \ldots & x^{d-1} & x^d \end{array} \\ \begin{pmatrix} 0 & \ldots & 0 & a_0 \\ 1 & & & a_1 \\ & \ddots & & \vdots \\ & & 1 & a_{d-1} \end{pmatrix} \end{array}$$

$$\det(M_x - tI) = (-1)^d h(t)$$

Hence: The eigenvalues of M_x are the **roots** of h.

The eigenvalue method: The multivariate case [for $|V_{\mathbb{C}}(I)| < \infty$]

$$\begin{array}{rccc} m_f : & \mathbb{R}[x]/I & \longrightarrow & \mathbb{R}[x]/I \\ & [p] & \longmapsto & [fp] \end{array}$$

is the '*multiplication by f*' linear operator in $\mathbb{R}[x]/I$ and let M_f be the matrix of m_f in a base $\mathcal{B}$ of $\mathbb{R}[x]/I$.

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

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

where $\zeta_v := (b(v))_{b\in\mathcal{B}}$

3. When $\mathcal{B}$ is a monomial basis of $\mathbb{R}[x]/I$ with $1 \in \mathcal{B}$, 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 $\mathbb{R}[x]/I$ and a basis G of the ideal I

• Typically, $\mathcal{B}$ is the set of **standard monomials** and G is a **Gröbner basis** 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** $\partial\mathcal{B} := (x_1\mathcal{B} \cup \ldots \cup x_n\mathcal{B}) \setminus \mathcal{B}$.
Write any border monomial

$$x_i b_j = \underbrace{r^{(ij)}}_{\in \text{Span}(\mathcal{B})} + \underbrace{g^{(ij)}}_{\in I}$$

Then $G := \{g^{(ij)} \mid x_i b_j \in \partial\mathcal{B}\}$ is a (border) basis of I and carries the ***same information*** as the multiplication matrices $M_{x_1}, \ldots, M_{x_n}$

To remember:

To find $V_{\mathbb{R}}(I)$ and a basis of $\sqrt[\mathbb{R}]{I}$ ...

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

Counting real roots with the Hermite quadratic form

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

Hermite bilinear form:

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

Theorem: For $f = 1$

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

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

Idea: Work on the dual (moment) side

$v \in V_{\mathbb{R}}(I) \rightsquigarrow L_v \in \mathbb{R}[x]^*$ [set of linear functionals on $\mathbb{R}[x]$]

L_v is the **evaluation at** v, defined by $L_v(p) := p(v) \quad \forall p \in \mathbb{R}[x]$

Properties of L_v:

- L_v vanishes on I: $L_v(h_j x^\alpha) = 0 \ \forall j \ \forall \alpha$
- L_v is positive on squares: $L_v(p^2) \geq 0 \ \forall p \in \mathbb{R}[x]$

The **moment matrix** $M(L_v) := (L_v(x^\alpha x^\beta))_{\alpha,\beta}$ is positive semidefinite

Note: $\mathrm{Ker} M(L_v) = I(v)$

Work with truncated moment matrices

For $t \in \mathbb{N}$ and $L \in \mathbb{R}[x]_t^*$, consider the 'truncated' conditions:

(LC) L vanishes on $\mathcal{H}_t$, where

$$\mathcal{H}_t := \{h_j x^\alpha \ \text{ with degree at most } t\} \subseteq I \cap \mathbb{R}[x]_t$$

(PSD) L is positive on the squares of degree at most t, i.e.

$$\boxed{M_{\lfloor t/2 \rfloor}(L) \succeq 0}$$

$$\boxed{\mathcal{K}_t := \{L \in \mathbb{R}[x]_t^* \mid L(p) = 0 \ \forall p \in \mathcal{H}_t, \ M_{\lfloor t/2 \rfloor}(L) \succeq 0\}}$$

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

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

A geometric property of the cone $\mathcal{K}_t$

Lemma: The following are equivalent for $L \in \mathcal{K}_t$:

(1) L lies in the relative interior of $\mathcal{K}_t$ (L is **generic**)

(2) $\mathrm{rank} M_{\lfloor t/2 \rfloor}(L)$ is maximum

(3) $\mathrm{Ker} M_{\lfloor t/2 \rfloor}(L)$ is minimum, i.e.

$$\underbrace{\mathrm{Ker} M_{\lfloor t/2 \rfloor}(L)}_{=: \mathcal{N}_t \;\; \textit{generic kernel}} \subseteq \mathrm{Ker} M_{\lfloor t/2 \rfloor}(L') \quad \forall L' \in \mathcal{K}_t$$

Lemma: $\boxed{\mathcal{N}_t \subseteq \mathcal{N}_{t+1} \subseteq \ldots \subseteq \sqrt[\mathbb{R}]{I}}$

Proof: $\mathcal{N}_t \subseteq \mathrm{Ker} M_{\lfloor t/2 \rfloor}(L_v) \subseteq I(v) \quad \forall v \in V_{\mathbb{R}}(I)$

Semidefinite characterization of $\sqrt[\mathbb{R}]{I}$

Theorem 1: $\sqrt[\mathbb{R}]{I} = (\mathcal{N}_t)$ for t large enough.

Idea of proof: Show that, for t large enough, $\mathcal{N}_t$ contains a given basis $\{g_1, \ldots, g_L\}$ of $\sqrt[\mathbb{R}]{I}$

- Real Nullstellensatz: $g_l^{2m} + \sum_i s_i^2 = \sum_{j=1}^m u_j h_j$
- $\mathcal{N}_t$ is "real ideal like": $g_l^{2m} + \sum_i s_i^2 \in \mathcal{N}_t \Longrightarrow g_l \in \mathcal{N}_t$

Question: How to recognize when $\mathcal{N}_t$ generates $\sqrt[\mathbb{R}]{I}$?

Next: An answer in the case $|V_{\mathbb{R}}(I)| < \infty$

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

Theorem 2: Let L be a *generic* element of $\mathcal{K}_t$, $D := \max \deg(h_j)$.
Assume one of the following two **flatness conditions** holds:

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

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

Then: • $\sqrt[\mathbb{R}]{I} = (\mathrm{Ker} M_s(L))$

• Any column base $\mathcal{B}$ of $M_{s-1}(L)$ is a base of $\mathbb{R}[x]/\sqrt[\mathbb{R}]{I}$

• The multiplication matrices can be constructed from $M_s(y)$

• $\pi_{2s}(\mathcal{K}_t) \ = \ \mathrm{cone}\{\pi_{2s}(L_v) \mid v \in V_{\mathbb{R}}(I)\}$
$= \mathrm{cone}\{(v^\alpha)_{|\alpha| \leq 2s} \mid v \in V_{\mathbb{R}}(I)\}$.

Properties of moment matrices

Lemma: Let $L \in \mathbb{R}[x]^*$.

- $\mathrm{Ker} M(L)$ is an ideal.
- If $M(L) \succeq 0$, then $\mathrm{Ker} M(L)$ is real radical.

> **Flat Extension theorem** [Curto-Fialkow 1996]
> Let $L \in \mathbb{R}[x]^*_{2s}$.
> If $\mathrm{rank} M_s(L) = \mathrm{rank} M_{s-1}(L)$, then
> there exists a *flat extension* $\tilde{L} \in \mathbb{R}[x]^*$ of L,
> i.e., satisfying $\mathrm{rank} M(\tilde{L}) = \mathrm{rank} M_s(L)$.

Idea of proof: We know how to construct the extension using the polynomials in $(\mathrm{Ker} M_s(L))$.

Finite Rank Moment Matrix theorem [Curto-Fialkow 1996]

Let $L \in \mathbb{R}[x]^*$. If $M(L) \succeq 0$ and $\text{rank} M(L) = r < \infty$,
then L has a *finite r-atomic representing measure*, i.e.
$L = \sum_{i=1}^{r} \lambda_i L_{v_i}$, where $\lambda_i > 0$ and
$\{v_1, \ldots, v_r\} = V(\text{Ker} M(L)) \subseteq \mathbb{R}^n$.

Proof: • $I := \text{Ker} M(L)$ is a real radical ideal

• I is 0-dimensional, as $\dim \mathbb{R}[x]/I = r$

• $V(I) = \{v_1, \ldots, v_r\} \subseteq \mathbb{R}^n$

Then, $L = \sum_{i=1}^{r} L(p_i^2) L_{v_i}$, where p_i are interpolation polynomials at v_i.

Proof of the stopping criterion

Assume $\text{rank} M_s(L) = \text{rank} M_{s-1}(L)$.
Show $(\text{Ker} M_s(L)) = \sqrt[\mathbb{R}]{I}$.

- By the Flat Extension theorem, $\pi_{2s}(L)$ has a **flat extension** $\tilde{L} \in \mathbb{R}[x]^*$, **i.e.** $\text{rank} M(\tilde{L}) = \text{rank} M_s(L)$.

- $\text{Ker} M(\tilde{L}) \;=\; (\text{Ker} M_s(L))$.

- As $M(\tilde{L}) \succeq 0$, $\;\text{Ker} M(\tilde{L})$ is a **real radical ideal.**

We have: $I \underbrace{\subseteq}_{(LC)} (\text{Ker} M_s(L)) \underbrace{\subseteq}_{L \text{ generic}} \sqrt[\mathbb{R}]{I}$

This implies: $(\text{Ker} M_s(L)) = \sqrt[\mathbb{R}]{I}$

Remains to show: $\pi_{2s}(\mathcal{K}_t) = \text{cone}\{L_v \mid v \in V_{\mathbb{R}}(I)\}$.

Let $L \in \mathcal{K}_t$.

- (F1) holds: $\text{rank} M_s(L) = \text{rank} M_{s-1}(L) =: r' \ (\leq r)$.

- Thus $\pi_{2s}(L)$ has a flat extension $\tilde{L}$.

- By the Finite Rank Moment Matrix theorem, $\tilde{L}$ has a finite r'-atomic measure:

$\tilde{L} = \sum_{i=1}^{r'} \lambda_i L_{v_i}$, where $\lambda_i > 0$ and

$\{v_1, \ldots, v_{r'}\} = V(\text{Ker} M_s(L)) \subseteq V_{\mathbb{R}}(I)$.

Thus, $\pi_{2s}(L) \in \text{cone}\{L_v \mid v \in V_{\mathbb{R}}(I)\}$.

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

Input: $h_1, \ldots, h_m \in \mathbb{R}[x]$
Output: $\mathcal{B}$ base of $\mathbb{R}[x]/\sqrt[\mathbb{R}]{I}$
The multiplication matrices M_{x_i} in $\mathbb{R}[x]/\sqrt[\mathbb{R}]{I}$

Algorithm: For $t \geq D$

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

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

If **yes**, return a column basis $\mathcal{B}$ of $M_{s-1}(L)$ and $M_{x_i} = M_{\mathcal{B}}^{-1} P_i$,
- $M_{\mathcal{B}}$:= principal submatrix of $M_{s-1}(L)$ indexed by $\mathcal{B}$
- P_i:= submatrix of $M_s(L)$ with rows in $\mathcal{B}$ and columns in $x_i\mathcal{B}$.

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

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

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

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

A small example

Consider $I = (x_1^2 + x_2^2)$.

Thus, $|V_{\mathbb{C}}(I)| = \infty$, $V_{\mathbb{R}}(I) = \{(0,0)\}$, $\sqrt[\mathbb{R}]{I} = (x_1, x_2)$.

Any $L \in \mathcal{K}_2$ satisfies:

(LC) $L(x_1^2 + x_2^2) = 0$.

(PSD) $$M_1(L) = \begin{array}{c} \\ 1 \\ x_1 \\ x_2 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & x_1 & x_2 \end{array} \\ \begin{pmatrix} L(1) & L(x_1) & L(x_2) \\ & L(x_1^2) & L(x_1 x_2) \\ & & L(x_2^2) \end{pmatrix} \end{array} \succeq 0$$

Thus, $L(x_1^2) = L(x_2^2) = 0 \rightsquigarrow L(x_1) = L(x_2) = L(x_1 x_2) = 0$

Hence, $\mathrm{Ker} M_1(L)$ is spanned by x_1, x_2 for generic $L \in \mathcal{K}_2$.

Some algorithmic issues

How to find a generic $L \in \mathcal{K}_t$?

Solve the SDP program: $\min_{L \in \mathcal{K}_t} 1$ with an interior-point algorithm 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 $L \in \mathcal{K}_t$.

How to compute ranks of matrices ?

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

Some remarks

- Try to extract roots as soon as a set $\mathcal{B}$ of independent columns is found for which $\mathrm{rank} M_{\mathcal{B}}(L) = \mathrm{rank} M_{\mathcal{B}^+}(L)$, where $\mathcal{B}^+ = \mathcal{B} \cup x_1\mathcal{B} \cup \ldots \cup x_n\mathcal{B}$.

- If the multiplication matrices commute, one can extract $V(J)$, where J is a 0-dimensional ideal with $I \subseteq J \subseteq \sqrt[\mathbb{R}]{I}$.

- If $\mathcal{B}$ is *connected to 1*, then $J = \sqrt[\mathbb{R}]{I}$ (and commutativity is for free).

Generalized flat extension theorem [La-Mourrain 09]
If $\mathrm{rank} M_{\mathcal{B}}(L) = \mathrm{rank} M_{\mathcal{B}^+}(L)$, where $\mathcal{B}$ is connected to 1, then L has a flat extension to $\mathbb{R}[x]^*$.

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

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

$$K_t = \mathcal{H}_t^{\perp} = \{L \in \mathbb{R}[x]_t{}^* \mid L(h_j x^\alpha) = 0 \ \text{ if } \deg(h_j x^\alpha) \leq t\}$$

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

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

Note: Equality $J = I$ when $\mathbb{R}[x]/I$ is a Gorenstein algebra.

Equality $(\mathrm{Ker} M_s(L)) = I$ **in the Gorenstein case**

The inclusion $I \subseteq (\mathrm{Ker} M_s(L)) \subseteq \sqrt{I}$ may be strict for any generic L.

Example: For $I = (x_1^2, x_2^2, x_1x_2)$, $V_{\mathbb{C}}(I) = \{0\}$, $\sqrt{I} = (x_1, x_2)$, $\dim \mathbb{R}[x]/I = 3$, $\dim \mathbb{R}[x]/\sqrt{I} = 1$, while $\dim \mathbb{R}[x]/(\mathrm{Ker} M_s(y)) = 2$ for any generic y and any $s \geq 1$!

Recall: The algebra $\mathcal{A} := \mathbb{R}[x]/I$ 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 $L \in K_\infty$ with $I = \mathrm{Ker} M(L)$

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

Example 1: the moment-matrix algorithm for real/complex roots

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

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 $\rightsquigarrow$ 2 real roots

8 complex roots / 2 real roots:

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

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

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

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

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

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

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

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

Another example for real roots

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

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

order t	rank sequence of $M_s(y)$ $(0 \le s \le \lfloor t/2 \rfloor)$	extract. order s	accuracy	comm. error
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	0.12786	0.00019754
16	1 4 8 8 8 12 16 20 24	4	4.6789e-5	4.7073e-5

Linear basis: $\mathcal{B} = \{1, x_1, x_2, x_3, x_1^2, x_1x_2, x_1x_3, x_2x_3\}$ $\rightsquigarrow$ 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 prolongation-projection algorithm of Zhi-Reid

Theorem: If (F1) holds, i.e.

$\mathrm{rank} M_s(L) = \mathrm{rank} M_{s-1}(L)$ for generic $L \in K_t$, $D \leq s \leq \lfloor t/2 \rfloor$

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 $D \leq s \leq t$

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

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

Hence: The stopping criterion (D) is satisfied earlier than (F1).

Example 1: $I = (x_1^2 - 2x_1x_3 + 5, x_1x_2^2 + x_2x_3 + 1, 3x_2^2 - 8x_1x_3)$

	$t=2$	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

Complex roots

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

for $L \in K_9$

	$t=3$	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

$\dim \pi_3(K_6)$

$= \dim \pi_2(K_6)$

$= \dim \pi_3(K_7)$

Extension to the real case

- In the **complex** case, (D) compares the dimensions of $\pi_s(\mathcal{H}_t^\perp)$, $\pi_{s-1}(\mathcal{H}_t^\perp)$, and $\pi_s((\mathcal{H}_t^+)^\perp)$.

Notation: $\mathcal{H}_t^+ := \mathcal{H}_t \cup x_1\mathcal{H}_t \cup \ldots \cup x_n\mathcal{H}_t = \mathcal{H}_{t+1}$

- In the **real** case, $\dim(\mathcal{K}_t) = \dim(\mathcal{G}_t^\perp)$, where

$$\mathcal{G}_t := \mathcal{H}_t \cup \{f x^\alpha \mid f \in \mathcal{N}_t, \deg(x^\alpha) \leq \lfloor t/2 \rfloor\}$$

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

$$\text{(D+)} \quad \dim \pi_s(\mathcal{G}_t^\perp) = \dim \pi_{s-1}(\mathcal{G}_t^\perp) = \dim \pi_s((\mathcal{G}_t^+)^\perp)$$

then one can construct the multiplication matrices of $\mathbb{R}[x]/J$, where $I \subseteq J \subseteq \sqrt[\mathbb{R}]{I}$, and extract $V_\mathbb{R}(I) = V_\mathbb{C}(J) \cap \mathbb{R}^n$. Moreover, $J = \sqrt[\mathbb{R}]{I}$ if $\dim \pi_s(\mathcal{G}_t^\perp) = |V_\mathbb{R}(I)|$.

Link with the flatness criterion

Theorem: The flatness criterion (F1):

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

is **equivalent** to the strong version of the (D+) criterion:

$$\text{(D++)} \quad \dim \pi_{2s}(\mathcal{G}_t^{\perp}) = \dim \pi_{s-1}(\mathcal{G}_t^{\perp}) = \dim \pi_{2s}((\mathcal{G}_t^{+})^{\perp})$$

Thus: the stopping criterion (D+) is satisfied earlier than (F1).

But: the algorithm still needs to be improved ... as it handles large matrices (indexed by the full set of degree t monomials)

Example 1: $I = (x_1^2 - 2x_1x_3 + 5, x_1x_2^2 + x_2x_3 + 1, 3x_2^2 - 8x_1x_3)$

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

Real roots

$\text{rank} M_2(L) = \text{rank} M_1(L)$

for $L \in \mathcal{K}_6$

	$\mathcal{G}_3$	$\mathcal{G}_3^+$	$\mathcal{G}_4$	$\mathcal{G}_4^+$	$\mathcal{G}_5$	$\mathcal{G}_5^+$	$\mathcal{G}_6$	$\mathcal{G}_6^+$
$s=1$	4	4	4	4	2	2	2	2
$s=2$	8	8	8	8	2	2	2	2
$s=3$	11	10	10	9	2	2	2	2
$s=4$			12	10	3	3	2	2

$\dim \pi_2(\mathcal{G}_5^\perp)$

$= \dim \pi_1(\mathcal{G}_5^\perp)$

$= \dim \pi_2((\mathcal{G}_5^+)^\perp)$

Extensions ?

- Inspect ‘sparse’ sets of monomials instead of full degree sets.

- Use a better stopping criterion - e.g. use the sparse flatness condition.

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

For instance, combine with Gröbner/border bases methods: add polynomials of $\sqrt[\mathbb{R}]{I}$ (coming from kernels) on the fly...

- Extension to the positive dimensional case ?