Solving polynomial equations in reals with semidefinite programming

Jean Bernard Lasserre - Monique Laurent - Philipp Rostalski

LAAS, Toulouse - CWI, Amsterdam - ETH, Zurich

INTEGER PROGRAMMING AT CORE

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 $I := (h_1, \ldots, h_m)$

$$I = \{\sum_{j=1}^m f_j h_j \mid f_j \in \mathbb{R}[x]\}$$

- Find a basis (generating set) of the **real radical ideal** $\sqrt[\mathbb{R}]{I}$

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

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

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

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

A small example

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

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

Vanishing ideal: $\mathcal{I}(V_{\mathbb{R}}(I)) = (x_1, x_2)$ [= real radical ideal $\sqrt[\mathbb{R}]{I}$]

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

Vanishing ideal: $\mathcal{I}(V_{\mathbb{C}}(I)) = (x_1^2 + x_2^2)$ [= radical ideal $\sqrt{I}$]

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. Recap on the eigenvalue method for complex roots

2. The moment-matrix method for real roots

3. Adapt the moment-matrix method for complex roots
[Drop the PSD condition !]

4. Possible 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: $\dim \mathbb{R}[x]/I < \infty \iff |V_{\mathbb{C}}(I)| < \infty$

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 $|V_{\mathbb{C}}(I)| < \infty$]

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

: *'multiplication by f'* operator

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

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

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 $M_{x_1}, \ldots, M_{x_n}$.

Summarizing, we should remember that:

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

Theorem: For $f = 1$

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

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

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

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

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

Real roots of $I = (h_1, \ldots, h_m)$ via 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: $\exists t \geq s \geq D \quad \pi_s(\mathcal{K}_t) = \text{cone}(L_v \mid v \in V_{\mathbb{R}}(I)\}$

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.

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

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: Let $\{g_1, \ldots, g_L\}$ be a basis of $\sqrt[\mathbb{R}]{I}$.

We show that, for t large enough, $\mathcal{N}_t$ contains $\{g_1, \ldots, g_L\}$.

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

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

Then:

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

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

• **Flat extension thm** [Curto-Fialkow 1996] $\pi_{2s}(L)$ has a *flat extension* $\tilde{L} \in \mathbb{R}[x]^*$, i.e. such that $\mathrm{rank} M(\tilde{L}) = \mathrm{rank} M_s(L)$.

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

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

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

• $\mathcal{B}$ indexes a base of $M_{s-1}(L) \Longrightarrow \mathcal{B}$ indexes a base of $M(\tilde{L})$
$\Longrightarrow \mathcal{B}$ is a base of $\mathbb{R}[x]/\mathrm{Ker} M(\tilde{L}) = \mathbb{R}[x]/\sqrt[\mathbb{R}]{I}$

• Use linear dependencies in $M_s(L)$ 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 $\mathbb{R}[x]/\sqrt[\mathbb{R}]{I}$

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

$$\text{(PSD)}\ M_1(L) = \begin{array}{c} \\ 1 \\ x_1 \\ x_2 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & x_1 & x_2 \end{array} \\ \begin{pmatrix} L(1) & L(x_1) & L(x_2) \\ & L(x_1^2) & L(x_1x_2) \\ & & L(x_2^2) \end{pmatrix} \end{array} \succeq 0$$

Thus, $L(x_1^2) = L(x_2^2) = 0 \rightsquigarrow L(x_1) = L(x_2) = L(x_1x_2) = 0$

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: $\min_{\{L \in \mathcal{K}_t,\ L(1)=1\}} 1$ 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 ...

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

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

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

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

- Pick **generic** $L \in K_t$ [i.e. $\mathrm{rank} M_s(L)$ 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 $J := (\mathrm{Ker} M_s(L))$ satisfies $I \subseteq J \subseteq \sqrt{I}$ and thus $V_{\mathbb{C}}(J) = V_{\mathbb{C}}(I)$.
- If not, iterate with $t + 1$.

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:

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

Another stopping criterion (inspired by the algorithm of Zhi-Reid [2004] for complex roots)

The smallest linear space containing the cone $\mathcal{K}_t$ is $\mathcal{G}_t^\perp$, where

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

Set: $\mathcal{G}_t^+ := \mathcal{G}_t \cup x_1 \mathcal{G}_t \cup \ldots \cup x_n \mathcal{G}_t$

Theorem: Assume that, for some $D \leq s \leq t$, the following **dimension condition** holds:

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

Then one can construct the multiplication matrices of $\mathbb{R}[x]/J$, where J is a 0-dimensional ideal s.t. $I \subseteq J \subseteq \sqrt[\mathbb{R}]{I}$, and one can 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 dimension criterion (D):

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

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

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

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 ?

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

A first step: *A sparse flatness condition* [L-Mourrain 09] extending the *flat extension theorem* of Curto-Fialkow.

> Let $\mathcal{C}$ be a set of monomials **connected to 1**, i.e.
> $\forall m \in \mathcal{C} \;\; \exists m_1 \in \mathcal{C} \; \exists i \quad \text{s.t.} \;\; m = x_i m_1$
> If $\text{rank} M_{\mathcal{C}^+}(L) = \text{rank} M_{\mathcal{C}}(L)$, then L has a flat extension $\tilde{L} \in \mathbb{R}[x]^*$ such that $\text{rank} M(\tilde{L}) = \text{rank} M_{\mathcal{C}}(L)$.

Idea: Use this sparse criterion instead of (F1).
But how to search for such sparse set of monomials?