Symbolic-Numeric Computation: Polynomial Root Certification

Tülay Ayyıldız

Department of Computer Engineering
Gebze Technical University

◇

Koç University
Mathematics Seminar
2023

Symbolic-Numeric Computation

My research interest is

- constructing (theory- pure math),
- designing (math $\rightarrow$ computer science),
- analyzing (computer science $\rightarrow$ math)

algorithms to solve problems on polynomials using the integration of **numerical and symbolic** techniques.

The goal:

Finding robust and efficient algorithms to solve problems, and then analyze the computational complexity of the algorithms and implement them.

Numerical and Symbolic tools from:

- (Computational) Algebraic Geometry
- Abstract Algebra (Ring Theory, Finite Fields etc.)
- Linear Algebra
- Matrix Theory
- Numerical Analysis
- Algorithms
- Complexity Theory
- Optimization
- Programming (Maple, SageMath, Python, Matlab, Bertini)

We take advantage of both approaches!

Numerical vs Symbolic

Let's say we want to divide 1 by 3:

Numerical Computation	Symbolic Computation
input: 1/3	input: 1/3
0.33...3	1/3
0.33...3*3	1/3 * 3
0.99...9	1
error	exact
fast	slow
application	theory
"actual world"	"idealized world"

Polynomial root

Example (A toy example)

Let $f(x) = 3x - 1$ be a univariate polynomial, compute the root:

Numerical Computation	Symbolic Computation
Output: $0.33...3$	Output: $1/3$
$f(0.33...3) = -0.00...01$	$f(1/3) = 0$

Polynomial root

Example (A toy example)

Let $f(x) = 3x - 1$ be a univariate polynomial, compute the root:

Numerical Computation	Symbolic Computation
Output: $0.33...3$	Output: $1/3$
$f(0.33...3) = -0.00...01$	$f(1/3) = 0$

How and when we can tell a numerical computation is valid? Can we certify that a numerical result is a root?

Notation

Definition (Monomial)

Let $x_1, \ldots, x_n$ be variables, a monomial in $x_1, \ldots, x_n$ is a product of the variables up to some degree

$$x^d = x_1^{d_1} \cdot x_2^{d_2} \cdots x_n^{d_n}$$

where $d_1, \ldots, d_n$ are nonnegative integers.

Definition (Polynomial)

Let $x_1, \ldots, x_n$ be variables, a polynomial f in $x_1, \ldots, x_n$ with coefficients in $\mathbb{K}$ is a finite linear combination of monomials

$$f = \sum_d a_d x^d \in \mathbb{K}[x_1, \ldots, x_n], \quad a_d \in \mathbb{K}$$

where $d = (d_1, \ldots, d_n)$ is a vector of nonnegative integers and $x^d = x_1^{d_1} \cdot x_2^{d_2} \cdots x_n^{d_n}$.

Notation

Definition (Polynomial system)

Let $f_1, \ldots, f_m$ be polynomials in the variables $x_1, \ldots, x_n$ over $\mathbb{K}$, a set of polynomials

$$f = (f_1, \ldots, f_m) \in \mathbb{K}^m[x_1, \ldots, x_n]$$

is called a polynomial system if we are interested in the common solutions of the given polynomials.

Definition

We denote

$$\mathcal{I} := \langle f_1, \ldots, f_m \rangle$$

as the ideal generated by given polynomials $f_1, \ldots, f_m$.

Certification Problem

Let $f = (f_1, \ldots, f_m) \in \mathbb{K}^m[x_1, \ldots, x_n]$ with common roots

$$V(f) := \{\xi_1, \xi_2, \ldots, \xi_k\} \subset C^n(\text{algebraic closure of } \mathbb{K}),$$

Given:

Approximate roots of f: $\{z_1, z_2, \ldots, z_k\}$, $z_i \in C^n$ for $i = 1, \ldots, k$,
a floating number z^* and a rational number ε.

Goal:

To certify that a solution z^* of f is in the ε neighborhood of an exact root ξ of f.
i.e., whether z^* is in the open ball $\mathcal{B}_\varepsilon(\xi) := \{x : \|x - \xi\| < \varepsilon\}$ for $\varepsilon > 0$.

Some Solution Methods:

Let $f = (f_1, \ldots, f_m) \in \mathbb{K}[x_1, \ldots, x_n]$ and $z_1, \ldots, z_k$ be approximate solutions (we assume f generates a zero dimensional ideal).

- ($\mathbb{K} = \mathbb{R}$) if $n = m$, Smale's α-theory
  Theory by Smale (1986), then implemented (alphaCertified) by Sotille and Hauenstein (2012)
- ($\mathbb{K} = \mathbb{Q}$) if $n < m$, A-,Szanto and Hauenstein (2018)
  Use Rational Univariate Representation of the given overdetermined System
- ($\mathbb{K} = \mathbb{Q}$) if f has singular roots, A-,Szanto and Hauenstein (2018)
  Use determinantal form of isosingular deflation and obtain an overdetermined system

A fascinating application: A computerized proof of a conjecture by Littlewood

Is it possible in 3-space for seven infinite circular cylinders of unit radius each to touch all the others? Seven is the number suggested by constants.

Bozóki, Lee, and Rónyai (2015) proved this conjecture by setting up a well-constrained polynomial system over $\mathbb{Z}$ with real roots corresponding to solutions of the Littlewood conjecture. They approximated the roots using a numerical homotopy continuation method and certified that some roots are real using alphaCertified.

Figure: Seven cylinders can all touch each other!

Some Solution Methods:

Let $f = (f_1, \ldots, f_m) \in \mathbb{K}[x_1, \ldots, x_n]$ and $z_1, \ldots, z_k$ be approximate solutions (we assume f generates a zero dimensional ideal).

- $(\mathbb{K} = \mathbb{R})$ if $n = m$, Smale's α-theory
  Theory by Smale (1986), then implemented (alphaCertified) by Sotille and Hauenstein (2012)
- $(\mathbb{K} = \mathbb{Q})$ if $m > n$, A-,Szanto and Hauenstein (2018)
  Use Rational Univariate Representation of the given overdetermined System
- $(\mathbb{K} = \mathbb{Q})$ if f has singular roots, A-,Szanto and Hauenstein (2018)
  Use determinantal form of isosingular deflation and obtain an overdetermined system
- $(\mathbb{K} = \mathbb{Q})$ Certifying real roots: Zero dimensional Hermite Method, A-, Szanto (2023)

Zero Dimensional Hermite Method [1]

It is a method to certify approximate real roots using Hermite matrices

Given: $f = (f_1, \ldots, f_m) \in \mathbb{Q}^m[x_1, \ldots, x_n]$ and its approximate solutions $\{z_1, \ldots, z_k\} \subset \mathbb{C}^n$
Assumptions: $\mathcal{I}$ is zero dimensional

- It certifies the approximate real roots of a polynomial system over $\mathbb{Q}$
- Completely independent from the α-theory
- Therefore, does not require Newton's method to convergence
- It can work when α-theory does not

[1]This research was supported by TÜBİTAK project 119F211: Zero Dimensional Hermite Method (PI: Tülay Ayyıldız) and partially supported by NSF grant CCF-1813340 (PI: Agnes Szanto, NCSU).

Zero Dimensional Hermite Method

Approach:
Let $f = (f_1, \ldots, f_m) \in \mathbb{Q}^m[x_1, \ldots, x_n]$ such that $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ is a zero dimensional radical ideal.

- Compute approximate roots $z_1, \ldots, z_k \in \mathbb{C}^n$
- Construct an approximate Hermite matrix
- Rationalize the entries
- Certify that the obtained matrix is the exact Hermite Matrix of f
- Compute its signature
- Use the certification theorem to certify a real root
- Can be modified to work on non-radical case

Hermite Matrices (Definition 1)

Let $\xi_1, \xi_2, \ldots, \xi_k \in \mathbb{C}^n$ be the exact common roots of the polynomials in $\mathcal{I}$, roots are listed as many times as their multiplicity. If $\mathcal{I}$ is radical, each root is distinct. We denote approximations to the exact roots by $z_1, \ldots, z_k \in \mathbb{C}^n$.

Definition

Let $g \in \mathbb{R}[x_1, \ldots, x_n]$ and $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ be a set of monomials in $\mathbb{R}[x_1, \ldots, x_n]$. Let $z_1, z_2, \ldots, z_k \in \mathbb{C}^n$ be points, not necessary distinct. Then the **Hermite matrix** of $z_1, z_2, \ldots, z_k$ with respect to g, written in the basis $\mathcal{B}$ is

$$H_g := H_g^{\mathcal{B}}(z_1, z_2, \ldots, z_k) := V^T G V \tag{1}$$

where $V := V_{\mathcal{B}}(z_1, z_2, \ldots, z_k) = [z_i^{\alpha_j}]_{i,j=1}^k$ is the Vandermonde matrix of $z_1, z_2, \ldots, z_k \in \mathbb{C}^n$ with respect to a monomial set $\mathcal{B}$ and G is an $k \times k$ diagonal matrix with $[G]_{i,i} = g(z_i)$ for $i = 1, \ldots, k$.

Hermite Matrices (Definition 2)

Definition

Let $\mathcal{I} \subset \mathbb{R}[x_1, \ldots, x_n]$ be a zero dimensional ideal and denote $A := \mathbb{R}[x_1, \ldots, x_n]/I$, a finite dimensional vectors space over $\mathbb{R}$ with $k := \dim_{\mathbb{R}} A$.
For any $f \in A$, let $\mu_f : A \to A$, $p + \mathcal{I} \mapsto p \cdot f + \mathcal{I}$ be the multiplication map by f on A.
Fix a monomial basis $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ of A, and denote by $M_f^{\mathcal{B}}$ the $k \times k$ matrix of μ_f in the basis $\mathcal{B}$. The *Hermite matrix* of $\mathcal{I}$ with respect to g, written in the basis $\mathcal{B}$ is

$$H_g(\mathcal{I}) := H_g^{\mathcal{B}}(\mathcal{I}) = \left[Tr(M^{\mathcal{B}}_{g \cdot x^{\alpha_i + \alpha_j}}) \right]_{i,j=1}^{k},$$

where Tr denotes the matrix trace.

Extended Hermite Matrix

Definition

Let $\mathcal{B}$ be a finite set of monomials and and assume that $|\mathcal{B}^+| = l$. The **extended Hermite matrix** associated to points $z_1, \ldots, z_k \in \mathbb{C}^n$ (not necessarily distinct) is

$$H_g^+ := H_g^{\mathcal{B}^+}(z_1, \ldots, z_k) := (V^+)^T G V^+ \in \mathbb{C}^{l \times l} \tag{2}$$

where $\mathcal{B}^+ := \mathcal{B} \cup \bigcup_i x_i \mathcal{B} = \{b, x_1 b, \ldots, x_n b \mid b \in \mathcal{B}\}$,
$V^+ = V_{\mathcal{B}^+}(z_1, \ldots, z_k) \in \mathbb{C}^{k \times l}$ and G is the $k \times k$ diagonal matrix with $[G]_{j,j} = g(z_j)$ for $j = 1, \ldots, k$.

Example

Let $f(x) = x^2 - 1$, $g = 1 \in \mathbb{R}[x]$, and $\mathcal{B} = \{1, x, x^2\}$ and $\xi_0 = 1, \xi_1 = i, \xi_2 = -i \in \mathbb{C}$.

$$\mathrm{G} = \begin{bmatrix} g(1) & 0 & 0 \\ 0 & g(i) & 0 \\ 0 & 0 & g(-i) \end{bmatrix} = I_3 \text{ and } \mathrm{V} = \begin{bmatrix} \xi_0 & \xi_0 & \xi_0^2 \\ \xi_1 & \xi_1 & \xi_1^2 \\ \xi_2 & \xi_2 & \xi_2^2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & i & -1 \\ 1 & -i & -1 \end{bmatrix},$$

$$\text{then } H_1 = H_1^{\mathcal{B}}(1, i, -i) = V^T G V = \begin{bmatrix} 3 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 3 \end{bmatrix}$$

Trace definition vs VGV definition over Rationals

VGV definition:

Pros: gives a very efficient way to evaluate the entries of the Hermite matrix, assuming that we know the common roots of $\mathcal{I}$ exactly.
Cons: we need to compute the common roots exactly, which may involve working in field extensions of $\mathbb{Q}$.

Trace Definition:

Pros: can be computed exactly, working with rational numbers only.
Cons: requires the computation of the traces of k^2 matrices.

Signature of Hermite Matrices

Definition

Let A be a real and symmetric matrix. Then the **signature** of A is

$$\sigma(A) := \#\{\text{positive eigenvalues of} A\} - \#\{\text{negative eigenvalues of} A\}.$$

Theorem (Multivariate Hermite Theorem)

Let $\mathcal{I} \subset \mathbb{R}[x_1, \ldots, x_n]$ be zero dimensional and $\mathcal{B}$ be a monomial basis of $\mathbb{R}[x_1, \ldots, x_n]/\mathcal{I}$. If $H_g(\mathcal{I})$ is the Hermite matrix of $\mathcal{I}$ with respect to g in the basis $\mathcal{B}$, then

$$\sigma(H_g(\mathcal{I})) = \#\{x \in V_{\mathbb{R}}(\mathcal{I}) \mid g(x) > 0\} - \#\{x \in V_{\mathbb{R}}(\mathcal{I}) \mid g(x) < 0\}.$$

Special case $g = 1$

Corollary

Using the Hermite Theorem above, its signature gives the number of real roots of f

$$\sigma(H_1) = \#\{x \in V_{\mathbb{R}}(\mathcal{I})\}$$

Moreover:
Consider the univariate case when $g = 1$ and $\mathcal{B} := \{1, x, \ldots, x^{k-1}\}$.
Let $f = (f_1, \ldots, f_m) \in \mathbb{R}[x]$ and $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ be a zero dimensional ideal and exact roots z_l for $l = 1, \ldots, k$

$$H_1 = \left[\sum_{l=1}^{k} z_l^{i+j-2} \right]_{i,j=1,\ldots,k}.$$

The right hand side of the equation is the $(i + j - 2)$-th power sum of the roots, which is an elementary symmetric function of the roots.

Computation

- **Algorithm 1:** Hermite Matrix Computation
  - Returns a rational matrix
- **Algorithm 2:** Hermite Matrix Certification
  - Certifies that the output of the Algorithm 1 is the exact Hermite Matrix
- **Algorithm 3:** Real Root Certification
  - Uses the exact Hermite matrix and a certain g to certify the real roots of the given rational polynomial system

Algorithm 1: Hermite Matrix Computation

Input: $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ and $\mathcal{B}^+$ with $|\mathcal{B}^+| = l$ for $k, l \in \mathbb{N}$. $E, M \in \mathbb{R}_+$ and $z_1, \ldots, z_k \in \mathbb{C}^n$ such that $\|z_i\|_\infty \leq M + E$ for $i = 1, \ldots, k$ and E.

Output: $H_1^+ \in \mathbb{Q}^{l \times l}$ with rows and columns indexed by the elements of $\mathcal{B}^+$.

1: Compute the extended Hermite matrix $H_1^{\mathcal{B}^+}(z_1, z_2, \ldots, z_k)$ using Definition 1 with respect to the auxiliary function $g = 1$ and the monomials in $\mathcal{B}^+$.

Algorithm 1: Hermite Matrix Computation

2: Rationalize each entry of the approximate Hermite matrix $H_1^{\mathcal{B}^+}(z_1, z_2, \ldots, z_k)$ using rational number reconstruction. For the (i, j)-th entry of the $H_1^{\mathcal{B}^+}(z_1, z_2, \ldots, z_k)$, we use the following denominator bound:

$$B_{ij} := \left\lceil (2Eknd_{i,j}M^{d_{i,j}-1})^{-1/2} \right\rceil, \tag{3}$$

where $d_{i,j} = \deg b_i + \deg b_j$ and b_i and b_j are the i-th and j-th elements of $\mathcal{B}^+$ respectively, for $1 \leq i, j \leq l$. Return the resulting rational matrix.

Algorithm 2: Hermite Matrix Certification

Input: $f = (f_1, \ldots, f_m) \in \mathbb{Q}[x_1, \ldots, x_n]^m$ with $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ zero dimensional and radical;
$g \in \mathbb{Q}[x_1, \ldots, x_n]$,
$\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ connected to 1 with $|\mathcal{B}^+| = l$ for some $k, l \in \mathbb{N}$
$H_1^+ \in \mathbb{Q}^{l \times l}$ with rows and columns indexed by the elements of $\mathcal{B}^+$.

Output: The certified $H_1(\mathcal{I})$ and $H_g(\mathcal{I})$, or Fail.

1: $H_1 \leftarrow k \times k$ submatrix of H_1^+ with rows and columns corresponding to $\mathcal{B}$.
$H_1^{x_s} \leftarrow k \times k$ submatrix of H_1^+ with rows corresponding to $\mathcal{B}$ and columns corresponding to $x_s\mathcal{B}$ for $s = 1, \ldots, n$.

2: **If** *rank* $H_1 =$ *rank* $H_1^+ = k$, **then** $M_s \leftarrow H_1^{-1} \cdot H_1^{x_s}$ for $s = 1, \ldots, n$. **else** return Fail.

Algorithm 2: Hermite Matrix Certification

3: **For** $s = 1, \ldots, n,\ i, j = 1, \ldots, k$
if $x_s x^{\alpha_i} = x^{\alpha_j}$ **and** $[M_s]_{i,*} \neq \mathbf{e}_j^T$ **then return** Fail.

4: Let $c_1, \ldots, c_n$ be either new parameters or generic elements of $\mathbb{Q}$.
$p(\lambda) \leftarrow$ characteristic polynomial polynomial to $\sum_{i=1}^{n} c_i M_i$.
if $\gcd(p(\lambda), p'(\lambda)) \neq 1$ **return** Fail.

5: **If**

$$M_i \cdot M_j = M_j \cdot M_i \quad 1 \leq i < j \leq n$$

and

$$f_i(M_1, M_2, \ldots, M_n) = 0 \text{ for } i = 1, \ldots, m,$$

then we certified that M_i is the transpose of the multiplication matrix of $\mathcal{I}$ with respect to x_i in the basis $\mathcal{B}$ for all $i = 1, \ldots, n$.
Else return Fail.

Algorithm 2: Hermite Matrix Certification

6: **For** $i, j = 1, \ldots, l$ **if**

$$\mathrm{Tr}((b_i \cdot b_j)(M_1, M_2, \ldots, M_n)) \neq [H_1]_{i,j}$$

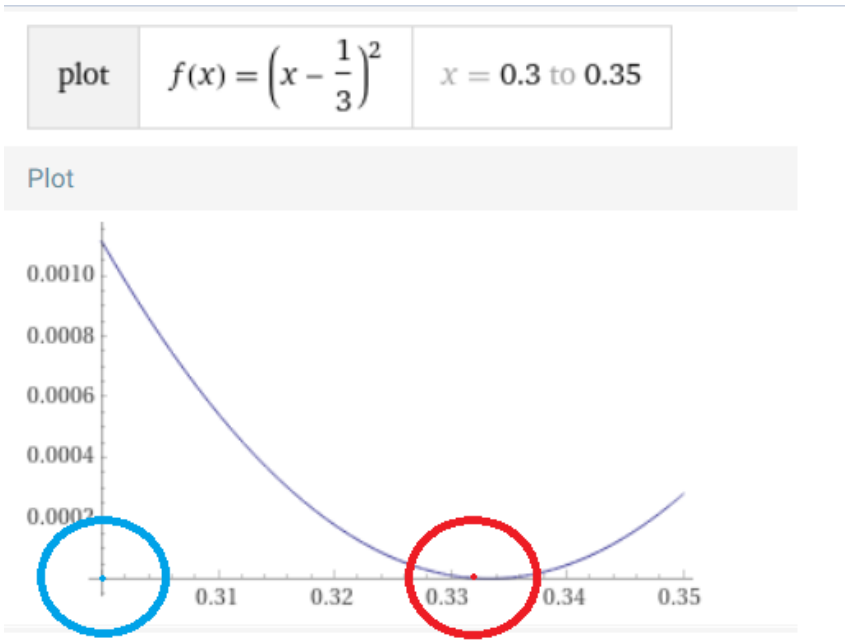
where b_i and b_j are the i-th and j-th elements of $\mathcal{B}$ respectively, and $(b_i \cdot b_j)(M_1, M_2, \ldots, M_n)$ is the matrix obtained by evaluating the polynomial $b_i \cdot b_j$ in the matrices $M_1, M_2, \ldots, M_n$
then return Fail.
Else we certified $H_1 = H_1(\mathcal{I})$.

7: **Return** H_1 and $H_g \leftarrow H_1 \cdot g(M_1, \ldots, M_n)$.

How to choose g?

If we choose $g(x) = 1$, then $\sigma(H_1(\mathcal{I})) = \#\{x \in V_{\mathbb{R}}(\mathcal{I})\}$.

What happens if we choose $g(x) = |x - z|^2 - \varepsilon^2$?



$z = 0$ $z = 0.33$

Hermite Certification Theorem

Corollary (A. and Szanto, 2023)

Let $f = (f_1, \ldots, f_m) \in \mathbb{Q}[x_1, \ldots, x_n]^m$ *for all* $i = 1, \ldots m$, *and* $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ *is a zero dimensional radical ideal. Given* $z^* \in \mathbb{Q}^n$ *and* $\varepsilon \in \mathbb{Q}_+$, *define* $g(x) := \|x - z^*\|_2^2 - \varepsilon^2 \in \mathbb{Q}[x_1, \ldots, x_n]$. *Then*

$$\sigma(H_1(\mathcal{I})) = \sigma(H_g(\mathcal{I}))$$

if and only if there is no real root within the closed ball in $\mathbb{R}^n$ *of radius* ε *around* z^*.

Algorithm 3: Real Root Certification

Input: $f = (f_1, \ldots, f_m) \in \mathbb{Q}[x_1, \ldots, x_n]^m$; $z^* \in \mathbb{Q}[i]^n$; $\varepsilon^2 \in \mathbb{Q}_+$;
$\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ connected to 1 with $|\mathcal{B}^+| = l$ for some $k, l \in \mathbb{N}$
$E, M \in \mathbb{R}_+$ and $z_1, \ldots, z_k \in \mathbb{C}^n$ such that $\|z_i\|_\infty \leq M + E$ for $i = 1, \ldots, k$ and the accuracy of z_i is at least E.

Output: True: $\exists z \in V_{\mathbb{R}}(\mathcal{I})$ such that z is in the closed ball of radius ε around z^*
False: No real root of $\mathcal{I}$ within the closed ball of radius ε around z^*
or Fail.

Algorithm 3: Real Root Certification (cont'd)

1: Define $g(x) := \|x - z^*\|_2^2 - \varepsilon^2 \in \mathbb{Q}[x_1, \ldots, x_n]$

2: $H_1^+ := H_1^{\mathcal{B}^+}(z_1, \ldots, z_k) \leftarrow$
HERMITE MATRIX COMPUTATION $(\mathcal{B}, \mathcal{B}^+, E, M, \{z_1, \ldots, z_k\})$
using the second definition.

3: For $I := \langle f_1, \ldots, f_m \rangle$ call
HERMITE MATRIX CERTIFICATION$(f, g(x), B, H_1^+)$ to obtain certified $H_1(I)$ and $H_g(I)$, that algorithm can also return Fail.

4: Compute $\sigma(H_1(\mathcal{I}))$ and $\sigma(H_g(\mathcal{I}))$.

5: **If** $\sigma(H_1(\mathcal{I})) = \sigma(H_g(\mathcal{I}))$ **then** return False
else return True.

A Simple Example

Consider $f(x) = 16x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$, with $g(x) = 1$.
The exact roots: $1/\sqrt{2}, -1/\sqrt{2}, 1/2\sqrt{2}, -1/2\sqrt{2}$.
Approximate solutions (homotopy method on Maple):
$z_1 = 0.7071067810, z_2 = -0.7071067810, z_3 = 0.3535533905, z_4 = -0.3535533905$.
This solution has error bound $E := 10^{-8}$.

Compute the approximate extended Hankel matrix $\tilde{H}_1^+$ from z_1, z_2, z_3, z_4:

$$\tilde{H}_1^+ = \begin{bmatrix} 4.0 & -0.0000000007 & 1.2500000052 & -0.00000000026 & 0 \\ -0.0000000007 & 1.2500000053 & -0.0000000002 & 0.5312500055 & -5.336 \\ 1.2500000052999999 & -0.0000000002 & 0.5312500055 & -5.4597088135 \times 10^{-11} & 0 \\ -0.0000000002 & 0.5312500055 & -5.4597088135 \times 10^{-11} & 0.2539062542 & -9.365 \\ 0.5312500055 & -5.3363907043 \times 10^{-11} & 0.2539062541 & -9.3658008865 \times 10^{-12} & 0 \end{bmatrix}$$

Example (cont'd)

Rationalize H_1^+, using $M = 0.8$ and $E = 10^{-8}$ and the denominator bound defined in the Algorithm 1. This gives $B \cong 2700$ as upper bound for the denominators of each entry of the Hankel matrix H_1^+.

$$H_1^+ = \begin{bmatrix} 4 & 0 & \frac{5}{4} & 0 & \frac{17}{32} \\ 0 & \frac{5}{4} & 0 & \frac{17}{32} & 0 \\ \frac{5}{4} & 0 & \frac{17}{32} & 0 & \frac{65}{256} \\ 0 & \frac{17}{32} & 0 & \frac{65}{256} & 0 \\ \frac{17}{32} & 0 & \frac{65}{256} & 0 & \frac{257}{2048} \end{bmatrix}$$

Let H_1 be the first k rows and the first k columns of H_1^+, and H_1^k be the first k rows and the last k columns of H_1^+.

H_1^+ has Hankel structure and $\mathrm{rank}(H_1^+) = \mathrm{rank}(H_1) = 4$. Then

$$C = H_1^{-1} \cdot H_1^4 = \begin{bmatrix} 0 & 0 & 0 & -\frac{1}{16} \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & \frac{5}{8} \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

C has a companion matrix shape and $f(C) = 0$, then $p(x) := x^4 - \frac{5}{8}x^2 + \frac{1}{16}$ with $\gcd(p, p') = 1$ (square free).
We Newton–Girard formulas with the elementary symmetric functions:
$e_0 = 1, e_1 = 0, e_2 = -\frac{5}{8}, e_3 = 0, e_4 = \frac{1}{16}$, which yields

$$\sum_{i=1}^{4} \xi_i^0 = 4, \sum_{i=1}^{4} \xi_i^2 = \frac{5}{4}, \sum_{i=1}^{4} \xi_i^4 = \frac{17}{32}, \sum_{i=1}^{4} \xi_i^6 = \frac{65}{256},$$

and all odd power sums are zero. Each sum matches the corresponding entry, thus we certified H_1.
Since $g(x) = 1$, Return H_1.

Further Research

Extra sections in the paper:

- Extension to the Non-Radical Case
- Another interesting application of Hermite Matrices: Non-positivity over $V(f) \cap \mathbb{R}^n$

Other research interests:

- Real Eigenvalue certification
- Positivity Certificates
- Fast Polynomial Multiplication
- Applications of Polyhedral Omega (joint work with Zefeirakis Zafeirakopoulos)

Thank You!