Certified Hermite Matrices from Approximate Roots - Univariate Case

Tulay Ayyildiz Akoglu[1⋆] and Agnes Szanto[2⋆⋆]

[1] Karadeniz Technical University, Trabzon, Turkey
[2] North Carolina State University, Raleigh, NC, USA
tulayaa@ktu.edu.tr
aszanto@ncsu.edu

Abstract. Let $f_1, \ldots, f_m$ be univariate polynomials with rational coefficients and $\mathcal{I} := \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x]$ be the ideal they generate. Assume that we are given approximations $\{z_1, \ldots, z_k\} \subset \mathbb{Q}[i]$ for the common roots $\{\xi_1, \ldots, \xi_k\} = V(\mathcal{I}) \subseteq \mathbb{C}$. In this study, we describe a symbolic-numeric algorithm to construct a rational matrix, called *Hermite matrix*, from the approximate roots $\{z_1, \ldots, z_k\}$ and certify that this matrix is the true Hermite matrix corresponding to the roots $V(\mathcal{I})$. Applications of Hermite matrices include counting and locating real roots of the polynomials and certifying their existence.

Keywords: Symbolic–Numeric computation · Approximate roots · Hermite Matrices.

1 Introduction

The development of numerical and symbolic techniques to solve systems of polynomial equations resulted in an explosion of applicability, both in term of the size of the systems efficiently solvable and the reliability of the output. Nonetheless, many of the results produced by numerical methods are not certified. In this paper, we show how to compute exact Hermite matrices from approximate roots of polynomials, and how to certify that these Hermite matrices are correct.

Hermite matrices and Hermite bilinear forms were introduced by Hermite in 1850 [7], and have many applications, including counting real roots [8, 9, 3] and locating them [2]. Assume that we are given the ideal $\mathcal{I} := \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x]$ generated by rational polynomials, and assume that $\dim_{\mathbb{Q}} \mathbb{Q}[x]/\mathcal{I} = k$. Hermite matrices have two kinds of definitions (see the precise formulation in Section 2.1):

1. The first definition of Hermite matrices uses the traces of k^2 multiplication matrices, each of them of size $k \times k$. The advantage of this definition is that it can be computed exactly, working with rational numbers only. The disadvantage is that it requires the computation of the traces of k^2 matrices.

⋆ T. Ayyildiz Akoglu was partially supported by TUBITAK grant 119F211.
⋆⋆ A. Szanto was partially supported by NSF grants CCF-1813340 and CCF-1217557.

2. The second definition uses symmetric functions of the k common roots of $\mathcal{I}$, counted with multiplicity. The advantage of this definition is that it gives a very efficient way to evaluate the entries of the Hermite matrix, assuming that we know the common roots of $\mathcal{I}$ exactly. The disadvantage is that we need to compute the common roots exactly, which may involve working in field extensions of $\mathbb{Q}$.

In this paper we propose to use the second definition to compute Hermite matrices, but instead of using exact roots, we use approximate roots that can be computed with numerical methods efficiently [6]. Once we obtain an approximate Hermite matrix, we use rational number reconstruction (RNR) to construct a matrix with rational entries of bounded denominators. Finally, we give a symbolic method which certifies that the rational Hermite matrix we computed is in fact the correct one, corresponding to the exact roots of $\mathcal{I}$.

Using RNR techniques on rational polynomial systems is not a new concept. A common approach is to use p-adic lifting or iterative refinement to build an approximate solution, then apply rational number reconstruction [13–15]. Peryl and Parrilo [11] used the approximate solutions as starting points for the computation of exact rational sum of squares decomposition of rational polynomials. RNR is also used to solve systems of linear equations and inequalities over the rational numbers [12]. Moreover, RNR can be used to construct the coefficients of the rational univariate representation of rational polynomial systems [1].

The novelty of this note and the difficulty of this problem is to certify the correctness of the Hermite matrix that we computed with the above heuristic approach. This part of the algorithm is purely symbolic. The main idea is to use the fact that companion matrices act like roots of the polynomials, so we can certify them, and then we use the famous Newton-Girard formulas [16] to connect the entries of the companion matrix with the entries of the Hermite matrix.

A natural question arises about the advantage of this hybrid symbolic–numeric approach over purely symbolic methods, for example by taking the gcd of the input polynomials and computing the symbolic Hermite matrix of the gcd using the definition with traces. In many cases, the input polynomials have much higher degree D than the number of common roots, so the bottleneck of the computation is computing the common roots or the gcd of the polynomials. Our approach computes numerically the roots of one polynomial with integer coefficients of size at most h, substitutes them into the other $m-1$ polynomials to find the common roots, which can be done using $O((D^3+hD^2)+hmD)$ binary operations up to logarithmic factors (c.f. [4, 10]). On the other hand, computing the gcd of m degree D polynomials with integer coefficients of overall size $H \leq mh$ takes $O(mD^3)$ arithmetic operation with integers of size $O(D^4H)$. (c.f. [5]).

2 Preliminaries

2.1 Hermite Matrices

Let $f_1, \ldots, f_m \in \mathbb{Q}[x]$, $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x]$ and $k := \dim_{\mathbb{Q}} \mathbb{Q}[x]/\mathcal{I}$. Assume that (the residue classes of the polynomials in) $\mathcal{B} = \{1, x, \ldots, x^{k-1}\}$ form a basis for $\mathbb{Q}[x]/\mathcal{I}$. Note that all definitions in this section are valid for polynomials over $\mathbb{R}$ or $\mathbb{C}$, but in this note we only consider polynomials with rational coefficients.

In [3, Section 4.3.2] it is shown that the following two definitions of Hermite matrices are equivalent:

Definition 1. *Let $\xi_1, \xi_2, \ldots, \xi_k \in \mathbb{C}$ be the common roots of $\mathcal{I}$ (here each root is listed as many times as their multiplicity) and $g \in \mathbb{Q}[x]$. Then the* **Hermite matrix** *of $\mathcal{I}$ with respect to g is*

$$H_g := V_B^T G V_B \tag{1}$$

where $V_B = [\xi_i^{j-1}]_{i,j=1,\ldots,k}$ is the Vandermonde matrix of the roots with respect to the basis $\mathcal{B}$ and G is an $k \times k$ diagonal matrix with $[G]_{ii} = g(\xi_i)$ for $i = 1, \ldots, k$. We will also need the **extended Hermite matrix** *of $\mathcal{I}$ with respect to g*

$$H_g^+ := V_{B^+}^T G V_{B^+} \in \mathbb{Q}^{(k+1)\times(k+1)} \tag{2}$$

where $V_{B^+} = [\xi_i^{j-1}]_{i=1,\ldots,k,j=1,\ldots,k+1} \in \mathbb{C}^{k\times(k+1)}$ is the Vandermonde matrix corresponding to $\mathcal{B}^+ := \{1, x, x^2, \ldots, x^k\}$.

Definition 1 gives the following formula for $g = 1$

$$H_1 = \left[\sum_{l=1}^{k} \xi_l^{i+j-2}\right]_{i,j=1,\ldots,k}. \tag{3}$$

The right hand side of (3) is the $(i+j-2)$-th power sum of the roots, which is an elementary symmetric function of the roots.

The second definition implies that the Hermite matrix has a Hankel structure and its entries are rational numbers.

Definition 2. *Let $\mathcal{I}$ as above and $g \in \mathbb{Q}[x]$. The* Hermite matrix *of $\mathcal{I}$ with respect of g is*

$$H_g := \left[\mathrm{Tr}(M_{gx^{i+j-2}})\right]_{i,j=1}^{k},$$

where M_f denotes the matrix of the multiplication map $\mu_f : \mathbb{Q}[x]/\mathcal{I} \to \mathbb{Q}[x]/\mathcal{I}$, $\mu_f(p) := p \cdot f + \mathcal{I}$ in the basis $\mathcal{B}$.

2.2 Rational Number Reconstruction

Continued fractions are widely used for rational approximation purposes. Let z be a real number, one can compute the sequence of repeated quotients using continued fractions, yielding rational approximations for z. If the denominator is bounded, the following theorem guarantees the uniqueness of the rational approximation in case of existence.

Theorem 1. *[12] There exists a polynomial time algorithm which, for a given rational number z and a natural number B tests if there exists a pair of integers (p, q) with $1 \leq q \leq B$ and*

$$\left| z - \frac{p}{q} \right| < \frac{1}{2B^2}$$

if so, finds this unique pair of integers.

If we have a bound E for the absolute approximation error of z, then the denominator bound can be defined as $B := \lceil (2E)^{-1/2} \rceil$ to guarantee the uniqueness of a rational number within distance E from z with denominator at most B.

3 Construction and Certification of Hermite Matrices

In the following algorithm we assume that $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ is radical, i.e. if $k = \dim \mathbb{Q}[x]/\mathcal{I}$ then $V(\mathcal{I})$ has cardinality k. Our algorithm to construct and certify Hermite matrices from approximate roots is as follows.

Algorithm: Certified Univariate Hermite Matrix

- **Input:** $f_1, \ldots, f_m, g \in \mathbb{Q}[x]$; $k = \dim \mathbb{Q}[x]/\mathcal{I}$; $\{z_1, \ldots, z_k\} \subset \mathbb{Q}[i]$ approximate roots; a bound E on the absolute error of these approximate roots.
- **Output:** $H_g \in \mathbb{Q}^{k \times k}$ or Fail.

1: Compute the approximate extended Hermite matrix

$$\tilde{H}_1^+ := \left[\sum_{l=1}^{k} z_l^{i+j-2} \right]_{i,j=1,\ldots,k+1} \in \mathbb{Q}[i]^{(k+1)\times(k+1)}.$$

2: Use Rational Number Reconstruction for the real part of each entry $\tilde{H}_1^+$, using Theorem 1 with denominator bound for the (i, j)-th entry

$$B_{i,j} := \left\lceil (2k(i+j-2)EA^{i+j-3})^{-1/2} \right\rceil. \tag{4}$$

Here A is an upper bound for the coordinates of the approximate roots. The resulting matrix is denoted by $H_1^+ \in \mathbb{Q}^{(k+1)\times(k+1)}$.

3: $H_1 \leftarrow$ the first k rows and the first k columns of H_1^+
$H_1^k \leftarrow$ the first k rows and the last k columns of H_1^+.

4: **If** H_1^+ has Hankel structure and $\operatorname{rank}(H_1) = \operatorname{rank}(H_1^+) = k$, **then**

$$M_x \leftarrow H_1^{-1} \cdot H_1^k$$

else return Fail.

5: **If** M_x has a companion matrix shape and $f_i(M_x) = 0$ for $i = 1, \ldots, m$ **then** $p(x) \leftarrow$ charpol(M_x) **else** return Fail;
If p is not square-free **then** return Fail. Otherwise M_x is the certified multiplication matrix by x in $\mathbb{Q}[x]/\mathcal{I}$.

6: Use the Newton–Girard formulas [16] with the coefficients of p to yield the d-th power sums of the roots of p for $d = 0, \ldots, 2k-2$, as in (3). **If** each one matches to the corresponding entry of H_1, **then** it certifies H_1, **else** return Fail.

7: Once H_1 and M_x are certified, **return**

$$H_g \leftarrow H_1 \cdot g(M_x),$$

which is correct by $H_1 \cdot g(M_x) = (V^T V) \cdot (V^{-1} G V) = V^T G V = H_g$.

Note that if we do not give $k = \dim_{\mathbb{Q}} \mathbb{Q}[x]/\mathcal{I}$ as part of the input, the above algorithm only certifies that the output matrix H_g corresponds to a rational subvariety of $V(\mathcal{I})$, i.e. possibly a proper subset of $V(\mathcal{I})$ that is defined by rational polynomials.

We finish this note by describing a modification of the above algorithm for the case when $\mathcal{I}$ is not radical. In this case we return a certified Hermite matrix H_g corresponding to a rational component of the *radical* of $\mathcal{I}$, i.e. each common roots of $\mathcal{I}$ is counted with multiplicity one or zero. We still start with the same input, but $z_1, \ldots, z_k$ may have repetitions (or form clusters). In Step 4, instead of requiring H_1 to have rank k, we compute the companion matrix M_x using a maximal non-singular submatrix of H_1^+, which may have size smaller than k. In Step 6, we use the Newton–Girard formulas to define H_1, and return H_g defined as in Step 7, which may also have size smaller than k.

In future work, we plan to extend these results to multivariate and overdetermined polynomial systems.

4 Example

We demonstrate our algorithm on a simple example. Consider $f(x) = 16x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$, with $g(x) = 1$. The exact roots of f are $1/\sqrt{2}, -1/\sqrt{2}, 1/2\sqrt{2}, -1/2\sqrt{2}$. We get the following approximate solutions using homotopy method in Maple: $z_1 = 0.7071067810, z_2 = -0.7071067810, z_3 = 0.3535533905, z_4 = -0.3535533905$. This solution has error bound $E := 10^{-8}$.

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

$$\tilde{H}_1^+ = \begin{bmatrix} 4.0 & -0.0000000007 & 1.2500000052 & -0.00000000026 & 0.5312500055 \\ -0.0000000007 & 1.2500000053 & -0.0000000002 & 0.5312500055 & -5.3363907043 \times 10^{-11} \\ 1.2500000052999999 & -0.0000000002 & 0.5312500055 & -5.4597088135 \times 10^{-11} & 0.2539062541 \\ -0.0000000002 & 0.5312500055 & -5.4597088135 \times 10^{-11} & 0.2539062542 & -9.3658008865 \times 10^{-12} \\ 0.5312500055 & -5.3363907043 \times 10^{-11} & 0.2539062541 & -9.3658008865 \times 10^{-12} & 0.1254882840 \end{bmatrix}.$$

2: Rationalize H_1^+, using $A = 0.8$ and $E = 10^{-8}$ and (4). This gives $B \cong 2700$ as upper bound for the denominators of each entry of the Hankel matrix H_1^+.

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

3: 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^+.
4: H_1^+ has Hankel structure and $\text{rank}(H_1^+) = \text{rank}(H_1) = 4$. Then

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

5: M_x has a companion matrix shape and $f(M_x) = 0$, then $p(x) := x^4 - \frac{5}{8}x^2 + \frac{1}{16}$ with $\gcd(p, p') = 1$ (square free). Thus we certified that M_x is the multiplication matrix by x in $\mathbb{Q}[x]/\langle f \rangle$.
6: 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

$$\sum_{i=1}^{4} \xi_i^0 = 4, \sum_{i=1}^{4} \xi_i^2 = \frac{5}{4}, \sum_{i=1}^{4} \xi_i^4 = \frac{17}{32}, \sum_{i=1}^{4} \xi_i^6 = \frac{65}{256}, \sum_{i=1}^{4} \xi_i^8 = \frac{257}{2048},$$

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

References

1. Ayyildiz Akoglu, T., Hauenstein, J.D., Szanto, A. : Certifying solutions to overdetermined and singular polynomial systems over Q. Journal of Symbolic Computation, **84**, 147–171 (2018)
2. Ayyildiz Akoglu, T. : Certifying solutions to polynomial systems over Q. PhD thesis, North Carolina State University (2016)
3. Basu, S., Pollack, R., Roy, M.-F. : Algorithms in real algebraic geometry. Springer-Verlag, Berlin Heidelberg (2006)
4. Becker, R., Sagraloff, M., Sharma, V. and Yap, C.: A near-optimal subdivision algorithm for complex root isolation based on the pellet test and newton iteration. Journal of Symbolic Computation, 86, pp.51-96 (2018)

5. Gonzlez-Vega, L., 1995, April. On the complexity of computing the greatest common divisor of several univariate polynomials. In Latin American Symposium on Theoretical Informatics (pp. 332-345). Springer, Berlin, Heidelberg.
6. Bates, D.J., Hauenstein, J.D., Sommese, A.J., Wampler, C.W. : Numerically solving polynomial systems with Bertini (Vol. 25). SIAM, (2013)
7. Hermite, C.: Sur le nombre des racines d'une équation algébrique comprise entre des limites données, J. Reine Angew. Math. 52 (1850), 39-51; also in Oeuvres completes, Vol. 1, pp. 397-414.
8. Hermite, C. : Remarques sur le théorème de Sturm. CR Acad. Sci. Paris, 36(52-54), 171 (1853)
9. Hermite, C. : Extrait d'une lettre de Mr. Ch. Hermite de Paris à Mr. Borchardt de Berlin sur le nombre des racines d'une équation algébrique comprises entre des limites données. Journal für die reine und angewandte Mathematik **52** 39–51 (1856)
10. Pan, V. Y.: Nearly Optimal Polynomial Root-finders: the State of the Art and New Progress, arXiv:1805.12042v10 [cs.NA] (2019)
11. Peyrl, H., Parrilo, P. A. : Computing Sum of Squares Decompositions with Rational Coefficients. Theor. Comput. Sci., **409**(2), 269-281 (2008)
12. Schrijver, A. : Theory of linear and integer programming. JohnWiley & Sons, New York (1998)
13. Steffy, D. E.: Exact solutions to linear systems of equations using output sensitive lifting. ACM Communications in Computer Algebra, **44**(3/4), 160182 (2011)
14. Wan, Z.: An algorithm to solve integer linear systems exactly using numerical methods. Journal of Symbolic Computation, 41:621632, (2006)
15. Wang X., Pan V. Y. : Acceleration of Euclidean algorithm and rational number reconstruction. SIAM J. Comput., **32**(2), 548–556 (2003)
16. Weisstein, E. W. "Newton-Girard Formulas." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/Newton-GirardFormulas.html