Certified Hermite matrices from approximate roots

Tulay Ayyildiz Akoglu [a,1], Agnes Szanto [b,2]

[a] *Karadeniz Technical University, Trabzon, Turkey*
[b] *North Carolina State University, Raleigh, NC, USA*

A B S T R A C T

Let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$ be a zero dimensional radical ideal defined by polynomials given with exact rational coefficients. Assume that we are given approximations $\{z_1, \ldots, z_k\} \subset \mathbb{C}^n$ for the common roots $\{\xi_1, \ldots, \xi_k\} = V(\mathcal{I}) \subseteq \mathbb{C}^n$. In this paper we show how to construct and certify the rational entries of Hermite matrices for $\mathcal{I}$ from the approximate roots $\{z_1, \ldots, z_k\}$. When $\mathcal{I}$ is non-radical, we give methods to construct and certify Hermite matrices for $\sqrt{\mathcal{I}}$ from the approximate roots. Furthermore, we use signatures of these Hermite matrices to give rational certificates of non-negativity of a given polynomial over a (possibly positive dimensional) real variety, as well as certificates that there is a real root within an ε distance from a given point $z \in \mathbb{Q}^n$.

© 2022 Elsevier Ltd. All rights reserved.

1. Introduction

The development of numerical and symbolic techniques to solve systems of polynomial equations resulted in an explosion of applicability, both in terms 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. When we want to certify the output, we always have to do some symbolic computations.

Either we use purely symbolic algorithms, or we perform symbolic-numeric hybrid computations with enough precision so that we are able to identify zero.

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 (1850) for univariate polynomials and were extended to the multivariate zero-dimensional setting in Basu et al. (2006); Stickelberger (1890). Hermite matrices have many applications, including counting real roots Basu et al. (2006); Hermite (1853, 1856) and locating them Ayyildiz Akoglu (2016). Assume that we are given the ideal $\mathcal{I} := \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$ generated by rational polynomials and assume that $\dim_{\mathbb{Q}} \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I} = k < \infty$. Hermite matrices have two kinds of definitions (see the precise formulation in Section 2.1):

1. The first definition uses symmetric functions of the k common roots of $\mathcal{I}$, counted with multiplicity (see Definition 2.1). 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 $\mathbb{Q}$.
2. The second definition of Hermite matrices uses the traces of k^2 multiplication matrices (see Definition 2.3), 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 multiplication matrices.

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 Bates et al. (2013). Once we obtain an approximate Hermite matrix, we use rational number reconstruction 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 $\mathcal{I}$.

The novelty of this work 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 that we use the relationship between multiplication matrices and Hermite matrices to compute a system of multiplication matrices using Hermite matrices and vice versa. As multiplication matrices, which are also rational matrices, act as roots of the polynomial system, we can certify their correctness, which in turn gives us a method to certify Hermite matrices.

Note that both of the above definitions of Hermite matrices are continuous (entry-wise maps are continuous) in the presence of root multiplicities. However our use of approximate roots and multiplication matrices necessitate that we first consider the case where $\mathcal{I}$ is radical. To handle the non-radical case, we use the fact that the maximal non-singular submatrix of the Hermite matrix of $\mathcal{I}$ gives the Hermite matrix of $\sqrt{\mathcal{I}}$, so this is what we compute and certify. In both the radical and non-radical cases we were able to give sufficient conditions in terms of the quality of the root approximations and the size of the rational numbers in the Hermite matrices that guarantee that our Hermite matrix construction and certification algorithms do not fail.

Another contribution of this paper is the presentation of two novel applications using the signature of the certified Hermite matrices:

The first application is to give a rational certificate that a polynomial $g \in \mathbb{Q}[x_1, \ldots, x_n]$ is non-negative over a smooth real variety $V(f_1, \ldots, f_s) \cap \mathbb{R}^n$ where $f_1, \ldots, f_s \in \mathbb{Q}[x_1, \ldots, x_n]$. This application was inspired by Cifuentes and Parrilo (2017) where the authors give a method to compute a degree d sum of squares (SOS) decomposition (if one exists) for a non-negative polynomial over a real algebraic set using a finite set of sample points from the (complex) algebraic set. While the SOS decomposition constructed in Cifuentes and Parrilo (2017) is approximate, the construction we give here is exact, using Hermite matrices with rational entries.

The second application is to give a rational certificate that for a given point $z \in \mathbb{Q}^n$, $\varepsilon \in \mathbb{Q}_+$ and $\mathcal{I} := \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$ zero dimensional, there exists $\xi \in V(f_1, \ldots, f_m) \cap \mathbb{R}^n$ such that

$$\|z - \xi\|_2^2 \leq \varepsilon.$$

A natural question arises about the advantage of this hybrid symbolic–numeric approach over purely symbolic methods to compute Hermite matrices. The answer to this question is not black and white, it depends on the situation. For example, one could use a purely symbolic method computing a Gröbner bases, and then computing a system of multiplication matrices of the input polynomials and then the traces of certain multiplication matrices give the entries of Hermite matrices symbolically (just as in the first definition above). Instead, in this study, we use a symbolic-numeric approach. We assume that we have an efficient and parallelizable numerical method that can compute high precision approximations to all common complex roots for *square subsystems* of f, i.e. for n random linear combinations of $f_1, \ldots, f_m$. From these approximate roots we select in a certified manner a subset $z_1, \ldots, z_k \in \mathbb{C}^n$ (given with floating point numbers as coordinates) that are approximations of the solutions of $f \in \mathbb{Q}[x_1, \ldots, x_n]^m$. The worst case bit complexity for both the purely symbolic and the hybrid methods are similar Hashemi and Lazard (2005) (asymptotically bounded by D^n where D is the maximum of the degrees of the input polynomials). In Bardet et al. (2004, 2005) the authors give some evidence that Gröbner basis techniques for highly overdetermined systems ($m >> n$) can be highly efficient. The underlying idea behind this is that if one is given many polynomials already, there is only a little more work needed to generate a Gröbner basis. On the other hand, for systems that are square or close to square, the limited accuracy and parallelizability of the numerical approach allows us to handle larger polynomial systems in practice than with purely symbolic approaches. In Bates et al. (2014) they compare the two different approaches to compute and represent the solutions of polynomial systems: numerical homotopy continuation and symbolic computation.[3]

This paper is a generalization of our paper Ayyildiz Akoglu and Szanto (2020), where we considered only the univariate radical case.

The paper is organized as follows. In the next section we introduce some preliminaries with fundamental definitions such as the Hermite matrices, rational number reconstruction and numerical computation of roots of overdetermined polynomial systems. In Section 3, we explain how one can construct the exact Hermite matrix using the approximate solutions of the given polynomial system. In Section 4 we give an algorithm to certify that the obtained Hermite matrix is the exact one corresponding to our input polynomials. So far we assume that the ideal $\mathcal{I}$ is radical. In Section 5 we generalize the Hermite matrix computation and certification algorithm to the case when $\mathcal{I}$ is not radical. In Section 6 we present the application of Hermite matrices to give a rational certificate that a given rational polynomial is non-negative over a real algebraic variety defined by rational polynomials. Finally, in Section 7 we give another application that is a rational certificate for the existence of an exact common root of a zero-dimensional ideal within ε distance from a given point in $\mathbb{Q}^n$.

2. Preliminaries

2.1. Hermite matrices

In this section we give two definitions for the Hermite matrix of a zero-dimensional ideal. The first one defines the matrix from the common roots of the ideal, and in fact can be used to define Hermite matrices from any set of points. The second definition uses the traces of multiplication matrices of the factor ring of the ideal, and thus it gives a definition where the entries of the Hermite matrices are rational functions of the coefficients of the polynomial system.

Everything in this section is valid for polynomials over $\mathbb{R}$, so while in the rest of the paper we assume that our input polynomials are rational, in this section we present the preliminaries over $\mathbb{R}$. We use the following notation. Let $f = (f_1, \ldots, f_m) \in \mathbb{R}[x_1, \ldots, x_n]^m$ with $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subset \mathbb{R}[x_1, \ldots, x_n]$ a zero-dimensional ideal and $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ be a monomial basis for $\mathbb{R}[x_1, \ldots, x_n]/\mathcal{I}$.

---

[3] We thank Jonathan Hauenstein for pointing out to us the subtleties of using symbolic vs. numeric methods for solving polynomial systems.

Let $\xi_1, \xi_2, \ldots, \xi_k \in \mathbb{C}^n$ be the common roots of $\mathcal{I}$, here each root listed as many times as their multiplicity. If $\mathcal{I}$ is radical (which we assume in most of the later sections), each root is distinct. We denote by $z_1, \ldots, z_k \in \mathbb{C}^n$ approximations to the exact roots $\xi_1, \xi_2, \ldots, \xi_k$.

The first definition of Hermite matrices is given for any multiset of points in $\mathbb{C}^n$ as follows:

Definition 2.1. 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

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

where

$$V := V_{\mathcal{B}}(z_1, z_2, \ldots, z_k) = [z_i^{\alpha_j}]_{i,j=1,\ldots,k}$$

is the multivariate 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 a $k \times k$ diagonal matrix with $[G]_{i,i} = g(z_i)$ for $i = 1, \ldots, k$. We may omit $\mathcal{B}$ from the notation if it is clear from the context.

Example 2.2. When $\mathcal{B} = \{1, x_1, \ldots, x_1^{k-1}\}$ and $g = g(x_1)$ are also univariate, then the Hermite matrices are the same as the univariate Hermite matrices Ayyildiz Akoglu and Szanto (2020). If $z_l = (z_{l,1}, \ldots, z_{l,n}) \in \mathbb{C}^n$ for $l = 1, \ldots, k$ then the entries of the $k \times k$ univariate Hermite matrices are defined by

$$[H_g^{\mathcal{B}}(z_1, \ldots, z_k)]_{i,j} = \sum_{l=1}^{k} g(z_{l,1}) z_{l,1}^{i+j-2}.$$

In particular, for $g(x) = 1$, if $z_{1,1}, \ldots, z_{k,1}$ all distinct, the entries of the Hermite matrix are the power sum elementary symmetric functions of the first coordinates:

$$[H_1^{\mathcal{B}}(z_1, \ldots, z_k)]_{i,j} = \sum_{l=1}^{k} z_{l,1}^{i+j-2}. \tag{2}$$

The second definition of Hermite matrices implies that the entries of the Hermite matrix are rational functions of the coefficients of the defining polynomials of $\mathcal{I}$.

Definition 2.3. 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

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

where $\mathrm{Tr}(\cdot)$ denotes both the trace of a linear transformation and the trace of a matrix (note that the trace of a linear transformation is the trace of its matrix in *any* basis). We may omit $\mathcal{B}$ from the notation when it is clear from the context.

The next theorem asserts that the two definitions give the same matrix if we take the exact common roots of a zero dimensional polynomial system.

Theorem 2.4 *(Basu et al. (2006)). Let $\mathcal{I} \subset \mathbb{R}[x_1, \ldots, x_n]$ be a zero dimensional ideal and $g \in \mathbb{R}[x_1, \ldots, x_n]$. Let $k := \dim \mathbb{R}[x_1, \ldots, x_n]/\mathcal{I}$ and $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ be a monomial basis for $\mathbb{R}[x_1, \ldots, x_n]/\mathcal{I}$. Let $\xi_1, \ldots, \xi_k \in \mathbb{C}^n$ be the roots of $\mathcal{I}$, each root listed as many times as their multiplicity. Then*

$$H_g^{\mathcal{B}}(\xi_1, \ldots, \xi_k) = H_g^{\mathcal{B}}(\mathcal{I}).$$

Remark 2.5. Note that if $f_1, \ldots, f_m, g \in \mathbb{Q}[x_1, \ldots, x_n]$ then for $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ we have $H_g(\mathcal{I}) \in \mathbb{Q}^{k \times k}$, thus $H_g(\xi_1, \ldots, \xi_k) \in \mathbb{Q}^{k \times k}$, even if the roots are not rational.

Next we present the classical Hermite theorem that uses the *signature* of Hermite matrices to count real roots of a real polynomial system. First we define the signature of a matrix.

Definition 2.6. Let A be a real and symmetric matrix. Then the **signature** of A is

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

Definition 2.3 implies that Hermite Matrices of real polynomial ideals are real and symmetric. The classical univariate Hermite Theorem Hermite (1856) was generalized to the multivariate case by Pedersen, Roy and Szpirglas Pedersen et al. (1993), and was also proved in Basu et al. (2006) and Cox et al. (2006):

Theorem 2.7 *(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*

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

Remark 2.8. There are several ways to obtain the signature of a $k \times k$ real and symmetric matrix M without computing the eigenvalues explicitly. We will describe two of these methods here. Note that if M is a rational symmetric matrix, then both of these methods can be computed with exact arithmetic over the rationals.

1. *Using Descartes rule of signs:* Let $p(x)$ be the characteristic polynomial of the given $k \times k$ real and symmetric matrix. Since all eigenvalues of real symmetric matrices are real their characteristic polynomials have only real roots. Then the Descartes Rule of Signs provides that $\sigma(M)$ is the difference between the number of sign variation of the coefficients of $p(x)$ and the number of sign variations of the coefficients of $p(-x)$ (see Proposition 8.4 in Basu et al. (2006)).
2. *Using LU decomposition:* The LU decomposition of real symmetric matrices can be written as LDL^T where L is a special lower triangular matrix with 1's on the diagonal entries and D is a diagonal matrix with the entries $\{u_{11}, \ldots, u_{kk}\}$. These entries are the diagonal entries of the upper triangular matrix U obtained from the LU decomposition. By Sylvester Law of inertia, the signature of M is the difference between $\#\{u_{ii} : u_{ii} > 0\}$ and $\#\{u_{ii} : u_{ii} < 0\}$. The cost of this computation only comes from the LU decomposition which can be found via Gaussian Elimination.

We close this subsection with some definitions that will be used later in this paper. First, in our certification algorithm we need the following property of $\mathcal{B}$ (see Mourrain (1999)):

Definition 2.9. Let $\mathcal{B} \subset \mathbb{R}[x_1, \ldots, x_n]$. We say that $\mathcal{B}$ (or $\mathrm{span}_{\mathbb{R}}(\mathcal{B})$) is *connected to 1* if for all $b \in \mathrm{span}_{\mathbb{R}}(\mathcal{B})$ there exists $b_1, \ldots, b_n \in \mathcal{B}$ such that

$$b = \sum_{i=1}^{n} x_i b_i$$

and $\deg(b_i) < \deg(b)$ for $i = 1, \ldots, n$.

Definition 2.10. $\mathcal{B} \subset \mathbb{R}[x_1, \ldots, x_n]$ be a finite set of monomials. The *extension* of $\mathcal{B}$ is defined by

$$\mathcal{B}^+ := \mathcal{B} \cup \bigcup_{i=1}^{n} x_i \mathcal{B} = \{b, x_1 b, \ldots, x_n b \mid b \in \mathcal{B}\}. \tag{3}$$

Definition 2.11. Let $\mathcal{B}$ be a finite set of monomials 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

$$H_g^+ := H_g^{\mathcal{B}^+}(z_1, \ldots, z_k) := (V^+)^T G V^+ \in \mathbb{C}^{l \times l} \tag{4}$$

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

Remark 2.12. Let $\mathcal{I} \subset \mathbb{R}[x_1, \ldots, x_n]$ be zero dimensional and $\mathcal{B}$ be a monomial basis of $\mathbb{R}[x_1, \ldots, x_n]/\mathcal{I}$ with $\dim \mathbb{R}[x_1, \ldots, x_n]/\mathcal{I} = k$. The computation of $\mathcal{B}$ does not require using Grobner Basis since we work on zero dimensional ideals. One may use the set of the standard monomials, i.e., the monomials "under the staircase" (see Section 11 in Basu et al. (2006)). If one assumes that all of the i-th coordinates of the solutions are distinct, then $\mathcal{B} = \{1, x_i, \ldots, x_i^{k-1}\}$ can be also used (see Section 4.4 in Basu et al. (2006)). Example 2.2 and Remark 4.3 illustrate some important advantages and reasons of using this choice.

Even though we use the same notation as the monomial basis, Hermite matrices can be defined on any monomial set $\mathcal{B}$ using the Definition 2.1. However, in the second definition and most of this study (indicated otherwise) we assume that $\mathcal{B}$ is a monomial basis.

2.2. Rational number reconstruction

The continued fraction method for a real number $\alpha > 0$ can be described as the computation of

$$\alpha = \gamma_1 = \lfloor \gamma_1 \rfloor + \frac{1}{\gamma_2} = \lfloor \gamma_1 \rfloor + \frac{1}{\lfloor \gamma_2 \rfloor + \frac{1}{\gamma_3}} = \cdots$$

where $\gamma_1 = \alpha$ and $\gamma_{i+1} = \frac{1}{\gamma_i - \lfloor \gamma_i \rfloor}$. We call the rational numbers

$$\lfloor \gamma_1 \rfloor, \lfloor \gamma_1 \rfloor + \frac{1}{\lfloor \gamma_2 \rfloor}, \lfloor \gamma_1 \rfloor + \frac{1}{\lfloor \gamma_2 \rfloor + \frac{1}{\lfloor \gamma_3 \rfloor}}, \ldots$$

the *convergents* for α. The following theorem (cf. (Schrijver, 1998, Corollary 6.3a)) gives bounds on the distance from α that guarantees uniqueness of a rational number with bounded denominator, and shows that if such rational number exists, it is a convergent for α.

Theorem 2.13. *Schrijver (1998) There exists a polynomial time algorithm which, for a given rational number α and a natural number B tests if there exists a pair of integers (p, q) with $1 \leq q \leq B$ and*

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

and if so, finds this unique rational number $\frac{p}{q}$ as a convergent for α.

Approximate solutions are floating point numbers which are obtained from numerical computations. Using an absolute error bound $E > 0$ on numerical computations, we can set a denominator bound B such that Theorem 2.13 provides the unique rational approximation of α as follows:

Corollary 2.14. *Given $\alpha \in \mathbb{R}$ and $E > 0$ in $\mathbb{R}$ there is at most one rational number with its denominator bounded by $B := \lceil (2E)^{-1/2} \rceil$ within the distance E from α.*

2.3. Numerical certification of non-roots of overdetermined systems

In this subsection, we summarize some numerical methods from the literature to compute approximations of a superset of the common roots of an overdetermined polynomial systems. Let $f = (f_1, \ldots, f_m) \in \mathbb{Q}[x_1, \ldots, x_n]^m$ where $m > n$, we describe a method to certify that a given point z is *not* an approximate root of f. Assume that $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ is radical and zero dimensional, the difficulty lies in the fact that numerical methods, such as the homotopy continuation method Bates et al. (2013), are designed to compute the common roots of square, well-conditioned polynomial systems. Here we describe the approach presented in Hauenstein and Sottile (2012) to handle overdetermined systems.

The main idea is the following. Even though the consistency of an overdetermined system is a non-continuous property, the converse, inconsistency of an overdetermined system is a continuous property that can be certified with numerical methods. Similarly, while certifying that a point is approximating an exact root of an overdetermined system with exact rational coefficients cannot be certified with purely numerical methods, certifying that a point is *not* an approximate root can be done numerically. This allows us to eliminate roots of a square subsystem of f that are not roots of all f_i's for $i = 1, \ldots, m$, and to give a certified upper bound k on the number of common roots of f. With this upper bound, we can guarantee that our certification algorithm of Hermite matrices in Section 4 is correct when it gives a certification (although it may also return "fail").

More precisely, Hauenstein and Sottile (2012) suggests to consider two square subsystems which are random linear combinations of the polynomials $f_1, \ldots, f_m$. If $R_1, R_2 : \mathbb{C}^m \to \mathbb{C}^n$ are two linear maps (represented by two random matrices), then for $R_1(f) := R_1 \circ f$ and $R_2(f) := R_2 \circ f$, we can assume that

$$V(f) = V(R_1(f)) \cap V(R_2(f)).$$

This property is satisfied unless R_1 and R_2 are from Zariski closed subsets of all linear transformations. Similarly, for $i = 1, 2$, we can assume that the roots of $V(R_i(f))$ are finite and all distinct, this property is also satisfied unless R_i is from a Zariski closed subset of all linear transformations (cf. (Hauenstein and Sottile, 2012, Section 3)). Using numerical homotopy continuation methods and α-theory, one can compute and certify all approximate roots of both $R_1(f)$ and $R_2(f)$, see details on this part of the algorithm in (Hauenstein and Sottile, 2012, Section 2).

The following idea is a slight modification of (Hauenstein and Sottile, 2012, Section 3) which allows us to discard approximate roots of $R_1(f)$ and $R_2(f)$ that do not approximate the exact roots in $V(f)$. First note that for any approximate root z approximating an exact root $\xi \in V(R_i(f))$ for $i = 1, 2$, we can give upper bounds for $\|z - \xi\|$. This bound is defined to be two times the β function in α-theory (cf. (Blum et al., 1998, Ch 8, Theorem 2)), even without knowing the exact root. Let $\tilde{V}(R_i(f))$ (for $i = 1, 2$) denote the set of pairs $(z, \varepsilon) \in \mathbb{C}^n \times \mathbb{R}_+$, where z is one of the approximate roots computed for $R_i(f)$ and ε is an upper bound of the distance of z from the exact root it approximates. Fix $(z, \varepsilon) \in \tilde{V}(R_1(f))$ and define

$$S_{(z, \varepsilon)} := \left\{ (z', \varepsilon') \in \tilde{V}(R_2(f)) \: : \: \|z - z'\| \leq \varepsilon + \varepsilon' \right\}.$$

If $|S_{(z,\varepsilon)}| > 1$ then we need to refine z and all z' such that $(z', \varepsilon') \in S_{(z,\varepsilon)}$ using Newton's method w.r.t $R_1(f)$ and $R_2(f)$ respectively, until one gets $S_{(z,\varepsilon)} = \emptyset$ or $|S_{(z,\varepsilon)}| = 1$. If $S_z = \emptyset$ then we can discard (z, ε) since it cannot approximate an exact root in $V(f) = V(R_1(f)) \cap V(R_2(f))$. If S_z has one element (z', ε'), suppose z approximates an exact root $\xi \in V(R_1(f))$, z' approximates an exact root $\xi' \in V(R_2(f))$ but $\xi \neq \xi'$. Then we can compute refinements z_k and z'_k using k iterations of Newton's method starting from z and z' w.r.t $R_1(f)$ and $R_2(f)$ respectively, such that

$$\|z_k - z'_k\| > \varepsilon_k + \varepsilon'_k, \tag{5}$$

where $\varepsilon_k \leq \frac{1}{2^{2^k-1}} \varepsilon$ is a bound on $\|z_k - \xi\|$, and ε'_k is a bound for $\|z'_k - \xi'\|$. If we find a k such that the inequality (5) is satisfied then we discard (z, ε), otherwise we keep it. We repeat the above procedure for all elements in $\tilde{V}(R_1(f)) \cup \tilde{V}(R_2(f))$.

Note that the above method never eliminates points that are approximating roots in $V(f)$, but may leave in points that are not near $V(f)$. Thus, as a consequence, we can always guarantee that the input $z_1, \ldots, z_k$ for Algorithm 3.1 below, to compute an approximate Hermite matrix, is a *superset* of an approximation of $V(f)$, and in particular the above method gives a certification that $k \geq \dim \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I}$. On the other hand, our main symbolic-numeric certification Algorithm 4.1 for Hermite matrices will always fail when there are superfluous points among the input. Thus, using the assumption $k \geq \dim \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I}$, the Hermite matrices that we certify successfully will correspond to all roots of $V(f)$ (see Theorem 4.2).

In the rest of the paper we assume that we already computed a set $\{z_1, \ldots, z_k\} \subset \mathbb{C}^n$ that contains an approximate root for each root in $V(f)$, i.e. if $V(f) = \{\xi_1, \ldots, \xi_{k'}\}$ then $k' \leq k$ and for $i = 1, \ldots, k'$ there exists $j_i \in \{1, \ldots, k\}$ such that the Newton iteration starting from z_{j_i} quadratically converges to ξ_i. Moreover, using the β function from α-theory as above, we assume that we have a certified bound $E \in \mathbb{R}_+$ that we call *accuracy*, such that

$$\left\| \xi_i - z_{j_i} \right\|_2 \leq E \quad i = 1, \ldots, k'. \tag{6}$$

3. Constructing rational Hermite matrices

In this section we construct a rational matrix $H_1^+ \in \mathbb{Q}^{l \times l}$ from points $z_1, \ldots, z_k$ given with limited precision, using the definition of Hermite matrices in Definition 2.11 and rational number reconstruction.

Let $z_1, \ldots, z_k \in \mathbb{C}^n$ with $z_i = (z_{i,1}, \ldots, z_{i,n})$ for $i = 1, \ldots, k$. Let $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ be basis for $\mathbb{R}[x_1, \ldots, x_n]/\mathcal{I}(z_1, \ldots, z_k)$, and we use $\mathcal{B}^+$ as described in (3). Algorithm 3.1 below computes the matrix H_1^+ from the Hermite matrix $H_1^{\mathcal{B}^+}(z_1, z_2, \ldots, z_k)$ with respect to $\mathcal{B}^+$ by applying rational number reconstruction.

As part of the input of Algorithm 3.1, we also use quantities $E, M \in \mathbb{R}_+$, where E is an upper bound for the accuracy of each z_i for $i = 1, \ldots, k$ and M is an upper bound for the absolute values of the coordinates of the exact common roots of $\mathcal{I}$. We assume that E is computed as part of the numerical method computing $z_1, \ldots, z_k$, as described in Section 2.3. In this section we use E and M to estimate the denominator in the rational number reconstruction for each entry of H_1^+ using Proposition 3.2 below. Moreover, note that $\|z_i\|_\infty \leq M + E$ for $i = 1, \ldots, k$ since the coordinates of the exact roots are bounded by M and each z_i cannot be larger than $M + E$.

Algorithm 3.1 *(Hermite Matrix Computation).*

Input: $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ and $\mathcal{B}^+$ as in (3) 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 is as in (6).

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 2.11 with respect to the auxiliary function $g = 1$ and the monomials in $\mathcal{B}^+$.

   2: Rationalize each entry of the approximate Hermite matrix $H_1^{\mathcal{B}^+}(z_1, z_2, \ldots, z_k)$ using rational number reconstruction as explained in Subsection 2.2. 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:

$$B_{ij} := \left\lceil \left(2Eknd_{i,j} M^{d_{i,j}-1} \right)^{-1/2} \right\rceil, \tag{7}$$

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 $1 \leq i, j \leq l$. (See Proposition 3.2 below for obtaining this bound.) Return the resulting rational matrix.

We need the following proposition to get the bounds in (7) for the denominators of the entries of the Hermite matrix.

Proposition 3.2. *Assume $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$ is a zero dimensional radical ideal with $V(\mathcal{I}) = \{\xi_1, \ldots, \xi_k\} \subset \mathbb{C}^n$. Suppose $E > 0$ and $z_1, \ldots, z_k \in \mathbb{C}^n$ are such that*

$$\|\xi_i - z_i\|_2 < E.$$

Let $M > 0$ such that for all $i = 1, \ldots, k$ and $y \in \text{Ball}(z_i, E) = \{x \in \mathbb{C}^n : \|x - z_i\|_2 < E\}$

$$\|y\|_\infty \leq M.$$

Let $\alpha \in \mathbb{N}^n$ with $d := |\alpha|$. Then we have

$$\left| \sum_{i=1}^{k} \xi_i^\alpha - \sum_{i=1}^{k} z_i^\alpha \right| \leq EkndM^{d-1}. \tag{8}$$

Furthermore, there is at most one rational number within $EkndM^{d-1}$ distance from $\sum_{i=1}^{k} z_i^\alpha$ with denominator bounded by

$$B := \left\lceil (2EkndM^{d-1})^{-1/2} \right\rceil.$$

Proof. Fix $\alpha \in \mathbb{N}^n$ with $d := |\alpha|$. First note that $\sum_{i=1}^{k} z_i^\alpha$ is a polynomial in the nk coordinates of $z_1, \ldots, z_k$ of degree d. Using a multivariate version of Taylor's Theorem Apostol (1969), there exist $R_{i,j}(z_1, \ldots, z_k)$ for $i = 1, \ldots, k$ and $j = 1, \ldots, n$ such that

$$\sum_{i=1}^{k} z_i^\alpha - \sum_{i=1}^{k} \xi_i^\alpha = \sum_{i=1}^{k} \sum_{j=1}^{n} R_{i,j}(z_1, \ldots, z_k)(z_{i,j} - \xi_{i,j}).$$

Moreover,

$$|R_{i,j}(z_1, \ldots, z_k)| \leq \max_{s,t} \max_{y_s \in \text{Ball}(z_s, E)} \left| \frac{\partial z_s^\alpha}{\partial z_{s,t}}(y_s) \right| \leq dM^{d-1}.$$

Thus we get

$$\left| \sum_{i=1}^{k} z_i^\alpha - \sum_{i=1}^{k} \xi_i^\alpha \right| \leq \sum_{j=1}^{n} \sum_{i=1}^{k} dM^{d-1} |z_{i,j} - \xi_{i,j}| \leq kndM^{d-1}E.$$

The second claim is straightforward from Corollary 2.14 using $E' = EkndM^{d-1}$. □

The next theorem gives sufficient conditions for Algorithm 3.1 to correctly compute the exact Hermite matrices H_1^+ for $\mathcal{I}$ from the approximate points $z_1, \ldots, z_k$.

Theorem 3.3. *Let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$ be a zero dimensional radical ideal with $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ a basis for $\mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I}$. Denote $V_\mathbb{C}(\mathcal{I}) = \{\xi_1, \ldots, \xi_k\} \subset \mathbb{C}^n$. Let $E > 0$ and $z_1, \ldots, z_k \in \mathbb{C}^n$ such that for each $i \in \{1, \ldots, k\}$ there exists a unique j_i such that*

$$\|z_{j_i} - \xi_i\|_2 < E.$$

Assume further that $\|z_i\|_\infty \leq M + E$ for all $i = 1, \ldots, k$. Finally, assume that for $x^\alpha = x_i x_j x^{\alpha_t} x^{\alpha_s}$ for $i, j = 1, \ldots n$ and $t, s = 1, \ldots, k$, the denominator of $\sum_{j=1}^{k} \xi_i^\alpha \in \mathbb{Q}$ is at most $\lceil (2Ekn|\alpha||M^{|\alpha|-1})^{-1/2} \rceil$. Then Algorithm 3.1 computes the exact Hermite matrices $H_1^{\mathcal{B}^+}(\mathcal{I})$.

Proof. Since $\|z_i - \xi_{j_i}\|_2 < E$ and $\|z_i\|_\infty \le M + E$, we have that $\|\xi_i\|_\infty \le M$, thus the assumptions of Proposition 3.2 are satisfied. Therefore, for all $\alpha \in \mathbb{N}^n$ as in the claim, we have that there is at most one rational number within $Ekn|\alpha|M^{|\alpha|-1}$ distance from $\sum_{i=1}^k z_i^\alpha$ with denominators bounded by $\lceil (2Ek|\alpha|M^{|\alpha|-1})^{-1/2} \rceil$. By Proposition 3.2 we can see that $\sum_{i=1}^k \xi_i^\alpha$ is within that distance from $\sum_{i=1}^k z_i^\alpha$, and using our assumption on the denominator of $\sum_{i=1}^k \xi_i^\alpha \in \mathbb{Q}$, by Theorem 2.13 the rational number reconstruction algorithm finds $\sum_{i=1}^k \xi_i^\alpha$. Thus, the entries of H_1^+ computed by Algorithm 3.1 are the same as the entries of $H_1^{\mathcal{B}^+}(\mathcal{I})$ as claimed. $\quad\square$

Remark 3.4. The assumption of Theorem 3.3 that the denominator of $\sum_{j=1}^k \xi_i^\alpha \in \mathbb{Q}$ is at most $\lceil (2Ekn|\alpha|M^{|\alpha|-1})^{-1/2} \rceil$ can be achieved by improving the accuracy E of the approximate roots $z_1, \ldots, z_k$. If we assume that $z_1, \ldots, z_k$ are all approximate roots for a square subsystem of f, we can use Newton iterations to quadratically converge to the exact roots, thus decrease E. Meanwhile, the other quantities in this bound $(k, n, |\alpha|, M)$ are fixed, so with enough iterations we increase $\lceil (2Ekn|\alpha|M^{|\alpha|-1})^{-1/2} \rceil$ to satisfy the condition of the Theorem. One could in theory study the separation bounds for how small E has to be to satisfy this condition, (for similar analysis see Emiris et al. (2020) and Ayyildiz Akoglu et al. (2018)), but in this paper we let our Hermite matrix certification algorithm reject cases when the accuracy of the root approximation is not sufficiently good.

4. Certification of the exact Hermite matrix

Let $f = (f_1, \ldots, f_m) \in \mathbb{Q}[x_1, \ldots, x_n]^m$ be a polynomial system with zero dimensional radical ideal $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$. In the previous section we computed a matrix H_1^+ with rows and columns corresponding to $\mathcal{B}^+$, where $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$. In this section we certify if this matrix is the extended Hermite matrix of $\mathcal{I}$ and $H_g(\mathcal{I})$ for any polynomial $g \in \mathbb{Q}[x_1, \ldots, x_n]$, as long as $k \ge \dim \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I}$. Here we assume that $\mathcal{B}$ is connected to 1 as in Definition 2.9. The following algorithm is purely symbolic:

Algorithm 4.1 *(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;
$\quad g \in \mathbb{Q}[x_1, \ldots, x_n]$,
$\quad \mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ connected to 1 with $|\mathcal{B}^+| = l$ for some $k, l \in \mathbb{N}$
$\quad H_1^+ \in \mathbb{Q}^{l \times l}$ 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.
$\quad$**1:** $H_1 \leftarrow k \times k$ submatrix of H_1^+ with rows and columns corresponding to $\mathcal{B}$.
$\qquad H_1^{x_s} \leftarrow k \times k$ submatrix of H_1^+ with rows corresponding to $\mathcal{B}$ and columns corresponding to $x_s \mathcal{B}$ for $s = 1, \ldots, n$.
$\quad$**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.
$\quad$**3:** **For** $s = 1, \ldots, n$, $i, j = 1, \ldots, k$
$\qquad$ **if** $x_s x^{\alpha_i} = x^{\alpha_j}$ **and** $[M_s]_{i,*} \neq \mathbf{e}_j^T$ **then return** Fail.
$\quad$**4:** Let $c_1, \ldots, c_n$ be either new parameters or generic elements of $\mathbb{Q}$.
$\qquad p(\lambda) \leftarrow$ characteristic polynomial to $\sum_{i=1}^n c_i M_i$.
$\qquad$ **if** $\gcd(p(\lambda), p'(\lambda)) \neq 1$ **return** Fail.
$\quad$**5:** **If**

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

$\qquad$ and

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

$\qquad$ **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 $i = 1, \ldots, n$.
$\qquad$ **Else return** Fail.

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 $H_g \leftarrow H_1 \cdot g(M_1, \ldots, M_n)$.

We have the following result on the correctness of Algorithm 4.1.

Theorem 4.2. *Let* $f = (f_1, \ldots, f_m) \in \mathbb{Q}[x_1, \ldots, x_n]$ *with* $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$, $g \in \mathbb{Q}[x_1, \ldots, x_n]$, $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ *connected to 1 with* $|\mathcal{B}^+| = l$ *for some* $k, l \in \mathbb{N}$. *Let* $H_1^+ \in \mathbb{Q}^{l \times l}$ *be a matrix with rows and columns indexed by the elements of* $\mathcal{B}^+$. *If* $k \geq \dim \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I}$ *and Algorithm 4.1 does not return Fail then* $\mathcal{I}$ *is radical,* $\mathcal{B}$ *is a basis for* $\mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I}$ *and the output satisfies*

$$H_1 = H_1^{\mathcal{B}}(\mathcal{I}) \quad \text{and} \quad H_g = H_g^{\mathcal{B}}(\mathcal{I}).$$

Proof. Assume Algorithm 4.1 did not fail, and let $M_1, \ldots, M_n$ be the matrices computed in Step 2. Define the set of polynomials $\mathcal{F}$ from the columns of $M_1, \ldots, M_n$ as follows

$$\mathcal{F} := \left\{ x_j x^{\alpha_t} - \sum_{i=1}^k [M_j]_{i,t} \, x^{\alpha_i} \; : \; j = 1, \ldots, n, t = 1, \ldots, k \right\}.$$

Let $J := \langle \mathcal{F} \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$. In (Mourrain, 1999, Theorem 3.1) it is proved that $\mathcal{B}$ forms a basis for $\mathbb{Q}[x_1, \ldots, x_n]/J$ and $\mathcal{F}$ is a border basis for J if the following three conditions are satisfied:

1. the map $N : \mathrm{span}(\mathcal{B}^+) \to \mathrm{span}(\mathcal{B})$ defined as $N(x_j x^{\alpha_t}) := \sum_{i=1}^k [M_j]_{i,t} x^{\alpha_i}$ satisfy $N|_{\mathcal{B}} = \mathrm{Id}$;
2. the space spanned by $\mathcal{B}$ is connected to 1;
3. $\{M_1, \ldots, M_n\}$ is a set of pairwise commuting matrices.

The first condition is certified in Step 3, the second is an assumption, and the third is certified in Step 5. Also by Step 5 we have

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

thus $\mathcal{I} \subset J$. Since $\dim \mathbb{Q}[x_1, \ldots, x_n]/J = k$ and $\dim \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I} \leq k$ by assumption, we must have that $\mathcal{I} = J$ and for $s = 1, \ldots, n$, M_s is the transpose of the matrix of the multiplication map

$$\mu_{x_s} : \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I} \to \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I}, \quad [p] \mapsto [x_s p],$$

with respect to the basis $\mathcal{B}$. Step 6 certifies that the entries of H_1^+ are correct using Definition 2.3. Let p be the characteristic polynomial as in Step 4. Since $\gcd(p(\lambda), p'(\lambda)) \neq 1$ we have that p has k distinct roots, so $M_1, \ldots, M_n$ are simultaneously diagonalizable, and we have for $g \in \mathbb{Q}[x_1, \ldots, x_n]$

$$g(M_1, \ldots, M_n) = V^{-1} G V$$

where $V = V_{\mathcal{B}}(\xi_1, \ldots, \xi_k)$ is the Vandermonde matrix of the exact roots of $V(\mathcal{I}) = \{\xi_1, \ldots, \xi_k\}$ with respect to $\mathcal{B}$ and G is the diagonal matrix $\mathrm{diag}(g(\xi_1), \ldots, g(\xi_k))$. This gives

$$H_1 \cdot g(M_1, \ldots, M_n) = (V^T V) \cdot (V^{-1} G V) = V^T G V = H_g.$$

Thus, once H_1 and $M_1, \ldots, M_n$ are certified, we have computed the certified matrix $H_g(\mathcal{I})$. $\quad \square$

Remark 4.3. For $\mathcal{B} = \{1, x_1, \ldots, x_1^{k-1}\}$ we can guarantee that

$$\mathrm{rank}(H_1) = \mathrm{rank}(H_1^+) = k,$$

by checking that the difference between the first coordinates of z_i and z_j is at least $2E$ for all $1 \le i < j \le n$. In this case, since we assume that $\|z_i - \xi_{j_i}\|_2 < E$, then we must have that the first coordinates of $\xi_1, \ldots, \xi_k$ are all distinct. Since $H_1(\mathcal{I}) = V^T V$ where V is the usual univariate Vandermonde matrix of these first coordinates of $\xi_1, \ldots, \xi_k$, we get that $H_1(\mathcal{I})$ is invertible. Since $H_1^+(\mathcal{I}) = V_{\mathcal{B}^+}^T V_{\mathcal{B}^+}$, and $\mathrm{rank}(V_{\mathcal{B}^+}) = k$, we have that $\mathrm{rank}(H_1) = \mathrm{rank}(H_1^+) = k$. For general $\mathcal{B}$ there are no such simple conditions, but the SVD of the Vandermonde matrix of $z_1, \ldots, z_k$ with respect to $\mathcal{B}$ gives a good indication that $\mathcal{B}$ is a basis for both $\mathbb{C}[x_1, \ldots, x_n]/I(z_1, \ldots, z_k)$ and $\mathbb{C}[x_1, \ldots, x_n]/I(\xi_1, \ldots, \xi_k)$. Also for $\mathcal{B} = \{1, x_1, \ldots, x_1^{k-1}\}$, Step 3 is simply checking if M_1 has a companion matrix structure. In this case, in Step 6 we can certify H_1^+ using the Newton-Girard formulae (cf. Macdonald (1979)), computing the power sum elementary symmetric functions for degrees $1, \ldots, 2k$ from the coefficients of $p(x_1)$, and constructing the matrix H_1^+ according to (2).

5. Extension to the non-radical case

So far in this paper we assumed that the ideal $\mathcal{I}$ is radical and zero-dimensional. In this section, we describe what we can certify when we drop the assumption of radicality. However for sake of simplicity, we continue the radical case assumption after this section.

First note that Definition 2.1 for the Hermite matrix in terms of roots is well defined and continuous (the computation of the entries is only use continuous maps) even if some of the roots are repeated. This is no longer true when we try to define the multiplication matrices from the roots. Using a notation similar to the previous section, for $\mathcal{B}$ a basis for $\mathbb{R}[x_1, \ldots, x_n]/\mathcal{I}$ and $g \in \mathbb{Q}[x_1, \ldots, x_n]$, denote by $M_g^{\mathcal{B}}$ the transpose of the matrix of multiplication $\mu_g : \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I} \to \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I}$, $[p] \mapsto [gp]$ in the basis $\mathcal{B}$. While in the case when $\mathcal{I}$ is radical we have

$$M_g^{\mathcal{B}} = V_{\mathcal{B}} \, G \, V_{\mathcal{B}}^{-1},$$

with $V_{\mathcal{B}} = [b(\xi)]_{\xi \in V(\mathcal{I}), b \in \mathcal{B}}$ and $G = \mathrm{diag}(g(\xi) : \xi \in V(\mathcal{I}))$, $M_g^{\mathcal{B}}$ is not diagonalizable when $\mathcal{I}$ is not radical. In particular, $V_{\mathcal{B}}(\mathcal{I})$ and $H_1^{\mathcal{B}}(I)$ are not invertible, so we cannot use them to compute multiplication matrices in the certification algorithm as above.

To overcome this difficulty, we notice that while in the non-radical case $H_1^{\mathcal{B}}(\mathcal{I})$ is not invertible, its maximal non-singular submatrix is the Hermite matrix $H_1^{\bar{\mathcal{B}}}(\sqrt{\mathcal{I}})$ of the radical of $\mathcal{I}$, with respect to a subset $\bar{\mathcal{B}} \subset \mathcal{B}$ that is a basis for $\mathbb{R}[x_1, \ldots, x_n]/\sqrt{\mathcal{I}}$ (cf. Janovitz-Freireich et al. (2007)). Denote by $\bar{H}_1$ this maximal non-singular submatrix of $H_1^{\mathcal{B}}(\mathcal{I})$, with rows and columns corresponding to $\bar{\mathcal{B}} \subset \mathcal{B}$ and by $\bar{H}_1^{x_i}$ the submatrix of $H_1^{\mathcal{B}+}(\mathcal{I})$ corresponding to rows indexed by $\bar{\mathcal{B}}$ and columns indexed by $x_i \cdot \bar{\mathcal{B}}$. Then we get the transpose of the matrix of multiplication by x_i in $\mathbb{Q}[x_1, \ldots, x_n]/\sqrt{\mathcal{I}}$ w.r.t. the basis $\bar{\mathcal{B}}$ by

$$\bar{M}_i := M_{x_i}^{\bar{\mathcal{B}}} = \bar{H}_1^{-1} \cdot \bar{H}_1^{x_i} \quad i = 1, \ldots, n.$$

Thus we can use $\bar{H}_1^{\bar{\mathcal{B}}+}$ to compute the multiplication matrices of the radical $\sqrt{\mathcal{I}}$ and certify them.

We modify Algorithm 3.1 to output the maximal non-singular submatrix $\bar{H}_1$ of H_1 with rows and columns corresponding to $\bar{\mathcal{B}} \subset \mathcal{B}$, and its extension $\bar{H}_1^+$ to the basis $\bar{\mathcal{B}}^+$.

Algorithm 5.1 *(Hermite Matrix Computation - Non Radical Case).*

Input: $k \in \mathbb{N}$, $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ connected to 1, $E, M \in \mathbb{R}_+$ and $z_1, \ldots, z_k \in \mathbb{C}^n$ such that E is a bound on the accuracy of z_i and $\|z_i\|_\infty \le M + E$ for $i = 1, \ldots, k$.

Output: Fail or $\bar{k} \le k \in \mathbb{N}$, $\bar{\mathcal{B}} \subset \mathcal{B}$ connected to 1, and $\bar{H}_1^+ \in \mathbb{Q}^{\bar{l} \times \bar{l}}$ with rows and columns indexed by the elements of $\bar{\mathcal{B}}^+$ such that

$$\text{rank } \bar{H}_1 = \text{rank } \bar{H}_1^+ = \bar{k},$$

where $\bar{H}_1$ is the submatrix of $\bar{H}_1^+$ with rows and columns corresponding to $\bar{\mathcal{B}}$.

1: $H_1^{\mathcal{B}^+}(z_1, z_2, \ldots, z_k) \leftarrow$ Hermite Matrix Computation $\left(\mathcal{B}, \mathcal{B}^+, E, M, \{z_1, \ldots, z_k\}\right)$
(see Algorithm 3.1). Denote the resulting matrix by H_1^+ and its submatrix corresponding to rows and columns of $\mathcal{B}$ by H_1.

2: Find $\bar{k}$ maximal and $\bar{\mathcal{B}} \subset \mathcal{B}$ connected to 1 with $|\bar{\mathcal{B}}| = \bar{k}$ such that the submatrix $\bar{H}_1$ of H_1, corresponding to rows and columns in $\bar{\mathcal{B}}$, have the same rank as H_1.

3: If $\text{rank}(H_1^+) > \bar{k}$ return Fail. Else return $\bar{H}_1^+$, the submatrix of H_1^+ with rows and columns corresponding to $\bar{\mathcal{B}}^+$.

Theorem 5.2. *Let* $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$, $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$ *be a zero dimensional ideal* $V_{\mathbb{C}}(\mathcal{I}) = \{\xi_1, \ldots, \xi_{\bar{k}}\} \subset \mathbb{C}^n$ *for some* $\bar{k} \in \mathbb{N}$ *with the multiplicity of* ξ_i *denoted by* k_i, *where* $k := \sum_{i=1}^{\bar{k}} k_i = \dim \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I}$. *Let* $E > 0$ *and* $z_1, \ldots, z_k \in \mathbb{C}^n$, *not necessarily all distinct. Assume that for each* $i \in \{1, \ldots, \bar{k}\}$ *there exists a multi-subset* Z_i *of the multiset* $\{z_1, \ldots, z_k\}$ *such that for* $z \in Z_i$

$$\|z - \xi_i\|_2 < E.$$

Furthermore, assume that the multiset Z_i *has* k_i *elements, counted with multiplicity,* $Z_i \cap Z_j = \emptyset$ *for* $1 \le i < j \le \bar{k}$ *and* $k = \sum_{i=1}^{\bar{k}} k_i$. *Assume further that* $\|z_i\|_{\infty} \le M + E$ *for all* $i = 1, \ldots, k$. *Finally, assume that for* $x^{\alpha} = x_i x_j x^{\alpha_t} x^{\alpha_s}$ *for* $i, j = 1, \ldots n$ *and* $t, s = 1, \ldots, k$, *the denominator of* $\sum_{j=1}^{\bar{k}} k_i \xi_i^{\alpha} \in \mathbb{Q}$ *is at most* $\lceil (2Ekn|\alpha|M^{|\alpha|-1})^{-1/2} \rceil$. *Then Step 1 computes the exact Hermite matrices* $H_1^+ = H_1^{\mathcal{B}^+}(\mathcal{I})$. *Moreover, if* $\bar{\mathcal{B}}$ *defined in Step 2 forms a basis of* $\mathbb{Q}[x_1, \ldots, x_n]/\sqrt{\mathcal{I}}$ *then* $\text{rank}(H_1^+) = \text{rank}(\bar{H}_1) = \bar{k}$ *and* $\bar{H}_1^+ = H_1^{\bar{\mathcal{B}}^+}(\sqrt{\mathcal{I}})$.

Proof. Since $\|z_i - \xi_i\|_2 < E$ and $\|z_i\|_{\infty} \le M + E$, we have that $\|\xi_i\|_{\infty} \le M$, thus the assumptions of Proposition 3.2 are satisfied. Therefore, for all $\alpha \in \mathbb{N}^n$ as in the claim, we have that there is at most one rational number within $Ekn|\alpha|M^{|\alpha|-1}$ distance from $\sum_{i=1}^{k} z_i^{\alpha}$ with denominators bounded by $\lceil (2Ek|\alpha|M^{|\alpha|-1})^{-1/2} \rceil$. We can take a limit argument from k distinct points to the multiset $\{(\xi_1, k_1), \ldots, (\xi_{\bar{k}}, k_{\bar{k}})\}$ and apply Proposition 3.2 to this multiset and get that $\sum_{i=1}^{\bar{k}} k_i \xi_i^{\alpha}$ is within that distance from $\sum_{i=1}^{k} z_i^{\alpha}$. Using our assumption on the denominator of $\sum_{i=1}^{k} \xi_i^{\alpha} \in \mathbb{Q}$, by Theorem 2.13 the rational number reconstruction algorithm finds $\sum_{i=1}^{\bar{k}} k_i \xi_i^{\alpha}$. Thus, the entries of H_1^+ computed by Algorithm 3.1 are the same as the entries of $H_1^+(\mathcal{I})$ as claimed.

To prove the last claim, if $\bar{\mathcal{B}}$ forms a basis for $\mathbb{Q}[x_1, \ldots, x_n]/\sqrt{\mathcal{I}}$ then $V_{\bar{\mathcal{B}}} = [b(\xi_i)]_{i=1,\ldots,\bar{k}, b \in \bar{\mathcal{B}}}$ is a square submatrix of maximal rank of $V_{\mathcal{B}^+}(I) = [b(\xi)]_{\xi \in V(\mathcal{I}), b \in \mathcal{B}^+}$ with each roots in $V(\mathcal{I})$ listed as many times as their multiplicity. Since $H_1^+ = H_1^{\mathcal{B}^+}(\mathcal{I}) = V_{\mathcal{B}^+}(I)^T V_{\mathcal{B}^+}(I)$, and $\bar{H}_1 = V_{\bar{\mathcal{B}}}^T V_{\bar{\mathcal{B}}}$ which proves $\text{rank}(H_1^+) = \text{rank}(\bar{H}_1) = \bar{k}$ and $\bar{H}_1^+ = H_1^{\bar{\mathcal{B}}^+}(\sqrt{\mathcal{I}})$. □

We can use Algorithm 4.1 unchanged with input f, g, $\bar{\mathcal{B}}$, and $\bar{H}_1^+$ to compute certified Hermite matrices H_1 and H_g for $\sqrt{\mathcal{I}}$. We have the following theorem.

Theorem 5.3. *Let* $f = (f_1, \ldots, f_m) \in \mathbb{Q}[x_1, \ldots, x_n]^m$, $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$ *a zero dimensional ideal,* $g \in \mathbb{Q}[x_1, \ldots, x_n]$. *Let* $\mathcal{B}$ *connected to 1 with* $|\mathcal{B}| = k$ *and* $|\mathcal{B}^+| = l$ *for some* $k, l \in \mathbb{N}$. *Suppose Algorithm 5.1 returns* $\bar{k} \le k$, $\bar{\mathcal{B}}$ *connected to 1 with* $|\bar{\mathcal{B}}| = \bar{k}$ *and* $\bar{H}_1^+$ *with rows and columns indexed by the elements of* $\bar{\mathcal{B}}^+$. *If* $\bar{k} \ge \dim \mathbb{Q}[x_1, \ldots, x_n]/\sqrt{\mathcal{I}}$ *and Algorithm 4.1 with inputs* f, g, $\bar{\mathcal{B}}$, *and* $\bar{H}_1^+$ *returns* H_1 *and* H_g *then* $\bar{\mathcal{B}}$ *is a basis for* $\mathbb{Q}[x_1, \ldots, x_n]/\sqrt{\mathcal{I}}$ *and*

$$H_1 = H_1^{\bar{\mathcal{B}}}(\sqrt{\mathcal{I}}) \text{ and } H_g = H_g^{\bar{\mathcal{B}}}(\sqrt{\mathcal{I}}).$$

Proof. Assume Algorithm 5.1 did not fail, and returns $\bar{k} \leq k$, $\bar{\mathcal{B}}$ connected to 1 with $|\bar{\mathcal{B}}| = \bar{k}$ and $\bar{H}_1^+$. Then by Step 3 of Algorithm 5.1 we have $\mathrm{rank}(H_1^+) = \mathrm{rank}(\bar{H}_1^+) = \mathrm{rank}(\bar{H}_1) = \bar{k}$ so we can define the $\bar{k} \times \bar{k}$ matrices $M_1, \ldots, M_n$ in Step 2 of Algorithm 4.1. The same argument as in the proof of Theorem 4.2 shows that $M_1, \ldots, M_n$ forms a system of (transpose) multiplication matrices for an ideal J such that $\dim \mathbb{Q}[x_1, \ldots, x_n]/J = \bar{k}$, and $M_1, \ldots, M_n$ are simultaneously diagonalizable and their eigenvalues are the coordinates of the $\bar{k}$ distinct roots of J. Since $f_i(M_1, \ldots, M_n) = 0$ for all $i = 1, \ldots m$ we have that these $\bar{k}$ distinct roots are also common roots of $\mathcal{I}$. By assumption, $\bar{k} \geq \dim \mathbb{Q}[x_1, \ldots, x_n]/\sqrt{\mathcal{I}}$, so $\mathcal{I}$ has at most $\bar{k}$ distinct roots, so we must have $\bar{k} = \dim \mathbb{Q}[x_1, \ldots, x_n]/\sqrt{\mathcal{I}}$ and $\bar{B}$ forms a basis $\mathbb{Q}[x_1, \ldots, x_n]/\sqrt{\mathcal{I}}$. Thus $J = \sqrt{\mathcal{I}}$. The rest of the proof is the same as the proof of Theorem 4.2 with $\sqrt{\mathcal{I}}$ replacing $\mathcal{I}$. □

6. Application: rational certificate of non-negativity over real varieties

As mentioned in the Introduction, the following application was inspired by Cifuentes and Parrilo (2017) where the authors give a method to compute a degree d sum of squares (SOS) decomposition (if one exists) for a non-negative polynomial over a real algebraic set using a finite set of sample points from the (complex) algebraic set. In Cifuentes and Parrilo (2017) they also give bounds on the number of sample points needed to decide whether a degree d SOS decomposition exists. Their method uses semidefinite programming.

The application we present below also gives a certificate for the non-negativity of a polynomial over a real algebraic set, and also uses sample points of the complex algebraic set. However, it does not give an SOS decomposition, instead it uses Hermite matrices reconstructed and certified from the sample points. While the SOS decomposition constructed in Cifuentes and Parrilo (2017) is approximate, the construction we give here is exact, using rational numbers.

Consider the following problem:

Problem 6.1. *Given $f = (f_1, \ldots, f_s) \in \mathbb{Q}[x]^s$ and $g \in \mathbb{Q}[x]$ for $x = (x_1, \ldots, x_n)$. Decide if $g(z) \geq 0$ for all $z \in V(f) \cap \mathbb{R}^n$ and give a rational certificate.*

We use the following notion of critical points of g in $V(f) \subset \mathbb{C}^n$:

Definition 6.2. *Let $f = (f_1, \ldots, f_s) \in \mathbb{Q}[x]^s$ and $g \in \mathbb{Q}[x]$, and assume that $\mathcal{I} := \langle f_1, \ldots, f_s \rangle$ is a radical ideal. $z \in \mathbb{C}^n$ is a critical point of g in $V(f)$ if $z \in V(f)$, z is non-singular in $V(f)$, i.e. the Jacobian matrix $Jf(z)$ of f has rank $c := n - \dim V(f)$, and the Jacobian matrix $Jf(z)$ augmented with the row vector $\nabla g(z)$ has also rank c.*

We can solve Problem 6.1 using the following assumptions on $f = (f_1, \ldots, f_s)$ and g:

Assumption 6.3. *Let $f = (f_1, \ldots, f_s) \in \mathbb{Q}[x]^s$ and $g \in \mathbb{Q}[x]$ for $x = (x_1, \ldots, x_n)$. We assume*

1. *For all $z \in V(f)$, the Jacobian matrix $Jf(z)$ of f has rank $s \leq n$, i.e., f is a regular sequence and $V(f)$ is smooth.*
2. *$V(f) \cap \mathbb{R}^n$ is bounded,*
3. *g has finitely many critical points on $V(f)$.*

We need the following lemma:

Lemma 6.4. *Let $f \in \mathbb{Q}[x]^s$ and $g \in \mathbb{Q}[x]$ satisfying Assumption 6.3. Then, the set of polynomials in $\mathbb{Q}[x_1, \ldots, x_n, \lambda_1, \ldots, \lambda_s]$*

$$
L(x, \lambda) = \{f_1, \ldots, f_s\} \cup \left\{ \frac{\partial g}{\partial x_i} + \sum_{j=1}^{s} \lambda_j \frac{\partial f_j}{\partial x_i} : i = 1, \ldots, n \right\}
$$

has finitely many roots in $\mathbb{C}^{n+s}$, and their projections to the x coordinates contain all real points where g attains its extreme values on each connected component of $(V(f) \setminus V(g)) \cap \mathbb{R}^n$.

Proof. First we prove that the projection $V(L) \subset \mathbb{C}^{n+s}$ onto the x-coordinates are the critical points of g in $V(f)$. Let $(x, \lambda) \in V(L) \subset \mathbb{C}^{n+s}$. Then clearly $x \in V(f)$, and because of our first assumption and that $s \geq c = n - \dim V(f)$ we have that $s = c$ and x is non-singular in $V(f)$. By $(x, \lambda) \in V(L)$ we also have that $Jf(x)$ augmented with $\nabla g(x)$ has rank at most c, thus x is a critical point. Conversely, let x be a critical point of g on $V(f)$. Then $f_1, \ldots, f_s$ vanishes at x, and since both $Jf(x)$ and the augmented matrix $Jf(x)$ by $\nabla g(x)$ has rank s, $\nabla g(x)$ is in the row space of $Jf(x)$, thus there exists $\lambda \in \mathbb{C}^s$ such that $(x, \lambda) \in V(L)$.

Next we prove that $V(L) \subset \mathbb{C}^{n+s}$ is finite. By assumption, g has finitely many critical points in $V(f)$, thus the projection of $V(L)$ onto the x coordinates is finite. Since $Jf(x)$ has full row rank for every $x \in V(f)$, for every critical point x there is a unique $\lambda \in \mathbb{C}^s$ such that $(x, \lambda) \in V(L)$. Thus $V(L)$ is finite.

To prove the second claim, assume that $(V(f) \setminus V(g)) \cap \mathbb{R}^n \neq \emptyset$ and let C be a connected component of the set $(V(f) \setminus V(g)) \cap \mathbb{R}^n$. Since $V(f) \cap \mathbb{R}^n$ is bounded, C is bounded as well. Since $C \not\subset V(g)$, there exists $x \in C$ with $g(x) \neq 0$. Let $\overline{C}$ be the Euclidean closure of C so that $\overline{C} \subset V \cap \mathbb{R}^n$ is closed and bounded, and g vanishes identically on $\overline{C} \setminus C$. By the extreme value theorem, g attains both a minimum and a maximum on $\overline{C}$. Since g is not identically zero on $\overline{C}$, either the minimum or the maximum value of g on $\overline{C}$ must be nonzero, so g attains a non-zero extreme value on C. By the Lagrange multiplier theorem, using our assumptions, the points in C where g attains its extreme values are critical points of g in $V(f)$, which proves the claim. □

Now we are ready to prove the main result of the section:

Theorem 6.5. *Let $f \in \mathbb{Q}[x]^s$, $g \in \mathbb{Q}[x]$ and $L \subset \mathbb{Q}[x, \lambda]$ as in Lemma 6.4. Let J be the ideal generated by L in $\mathbb{Q}[x, \lambda]$, and $\mathcal{B} \subset \mathbb{Q}[x, \lambda]$ be any finite monomial basis for $\mathbb{Q}[x, \lambda]/J$. Then*[4]

$$\sigma(H_g^{\mathcal{B}}) = \sigma(H_{g^2}^{\mathcal{B}}) \text{ if and only if } g(x) \geq 0 \text{ for all } x \in V(f) \cap \mathbb{R}^n.$$

Proof. For the given polynomials $f \in \mathbb{Q}[x]^s$ and $g \in \mathbb{Q}[x]$, let

$$g(x, \lambda) \in \left\{ \frac{\partial g}{\partial x_i} + \sum_{j=1}^{s} \lambda_j \frac{\partial f_j}{\partial x_i} : i = 1, \ldots, n \right\} \subset L(x, \lambda).$$

First we prove that $g(x) \geq 0$ for all $x \in V(f) \cap \mathbb{R}^n$ if and only if $g(x, \lambda) \geq 0$ for all $(x, \lambda) \in V(L) \cap \mathbb{R}^{n+s}$. Assume that $g(x) \geq 0$ for all $x \in V(f) \cap \mathbb{R}^n$. Let $(x, \lambda) \in V(L) \cap \mathbb{R}^{n+s}$. Then $x \in V(f) \cap \mathbb{R}^n$ and since $g \in \mathbb{Q}[x]$, $g(x, \lambda) = g(x) \geq 0$. Conversely, assume $g(x, \lambda) \geq 0$ for all $(x, \lambda) \in V(L) \cap \mathbb{R}^{n+s}$. Suppose there exists $x \in V(f) \cap \mathbb{R}^n$ such that $g(x) < 0$. Let C be the bounded connected component of $(V(f) \setminus V(g)) \cap \mathbb{R}^n$ that contains x and $\overline{C}$ its Euclidean closure. Let $x^* \in \overline{C}$ where g attains its minimum on $\overline{C}$. Then $g(x^*) \leq g(x) < 0$, so $x^* \in C$ and x^* is a critical point of g in $V(f)$. Thus there exists a unique $\lambda \in \mathbb{R}^s$, the solution of a linear system, such that $(x^*, \lambda) \in V(L) \cap \mathbb{R}^{n+s}$. But then $g(x^*, \lambda) = g(x^*) \geq 0$, a contradiction.

By Lemma 6.4 we have $V(L)$ is finite, so $\mathcal{B}$ is finite. Since L has real (rational) coefficients, by Hermite's theorem

$$\sigma(H_g^{\mathcal{B}}) = \#\{(x, \lambda) \in V(L) \cap \mathbb{R}^{n+s} : g(x) > 0\} - \#\{(x, \lambda) \in V(L) \cap \mathbb{R}^{n+s} : g(x) < 0\}$$

$$\sigma(H_{g^2}^{\mathcal{B}}) = \#\{(x, \lambda) \in V(L) \cap \mathbb{R}^{n+s} : g(x) > 0\}.$$

---

[4] We thank to Bernard Mourrain for pointing out this simple fact.

Thus, $\sigma(H_g^{\mathcal{B}}) = \sigma(H_{g^2}^{\mathcal{B}})$ if and only if $\#\{(x,\lambda) \in V(L) \cap \mathbb{R}^{n+s} : g(x) < 0\} = 0$, i.e. for all $(x,\lambda) \in V(L) \cap \mathbb{R}^{n+s}$ we have $g(x) \geq 0$. This proves the theorem. $\square$

Corollary 6.6. *Let $f \in \mathbb{Q}[x]^s$, $g \in \mathbb{Q}[x]$ and $L \subset \mathbb{Q}[x,\lambda]$ as in Lemma 6.4 and $\mathcal{B} \subset \mathbb{Q}[x,\lambda]$ as in Theorem 6.5. Then $H_g^{\mathcal{B}}$ and $H_{g^2}^{\mathcal{B}}$ have rational entries, and can be computed and certified from approximate roots for the system L. Moreover, $\sigma(H_g^{\mathcal{B}}) = \sigma(H_{g^2}^{\mathcal{B}})$ can be also certified exactly over the rationals, giving a rational certificate for $g(x) \geq 0$ for all $x \in V(f) \cap \mathbb{R}^n$.*

Proof. Since L and g has rational coefficients, the matrices $H_g^{\mathcal{B}}$ and $H_{g^2}^{\mathcal{B}}$ have rational entries. One can find their signature by computing their LU-decomposition for example, again resulting in rational matrices. These give a rational certificate for $\sigma(H_g^{\mathcal{B}}) = \sigma(H_{g^2}^{\mathcal{B}})$ and by the previous theorem for $g(x) \geq 0$ for all $x \in V(f) \cap \mathbb{R}^n$. $\square$

Remark 6.7. The size k of the matrices $H_g^{\mathcal{B}}$ and $H_{g^2}^{\mathcal{B}}$ is equal to the number of critical points of g in $V(f)$. A rough estimate is given by $|V(L)| \leq d^{n+s}$ with $d = \max\{\deg(g), \deg(f_1), \ldots, \deg(f_s)\}$, using the Bezout bound for the polynomial system L.

The following proposition is needed in the algorithm below.

Proposition 6.8. *Let $\{z_1, \ldots, z_k\}, \{\xi_1, \ldots, \xi_k\} \subset \mathbb{C}^n$ be such that for some $E, M > 0$*

$$\|\xi_i - z_i\|_2 < E \text{ and } \|z_i\|_2 \leq M + E \quad i = 1, \ldots, k.$$

Let $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\} \subset \mathbb{Q}[x_1, \ldots, x_n]$ be a set of monomials such that $\deg(x^{\alpha_i}) \leq d$ for some $d > 0$. Then the Frobenious distance of the Vandermonde matrices is bounded by

$$\|V_{\mathcal{B}}(\xi_1, \ldots, \xi_k) - V_{\mathcal{B}}(z_1, \ldots, z_k)\|_F \leq knd M^{d-1} E.$$

Proof. As in the proof of Proposition 3.2 we can see that for $\alpha \in \mathbb{N}^n$, $|\alpha| \leq d$ we have

$$\left| \xi_i^{\alpha} - z_i^{\alpha} \right| \leq nd M^{d-1} E.$$

Taking the Frobenius norm of the difference of the Vandermonde matrices gives

$$\|V_{\mathcal{B}}(\xi_1, \ldots, \xi_k) - V_{\mathcal{B}}(z_1, \ldots, z_k)\|_F \leq \sqrt{k^2 (nd M^{d-1} E)^2} = knd M^{d-1} E.   \square$$

Algorithm 6.9. (Certification that g is non-negative over $V(f) \cap \mathbb{R}^n$)

Input: $n \in \mathbb{N}$, $f \in \mathbb{Q}[x]^s$, $g \in \mathbb{Q}[x]$ for $x = (x_1, \ldots, x_n)$ satisfying Assumption 6.3.
Output: True: $g(z) \geq 0$ for all $z \in V(f) \cap \mathbb{R}^n$
    False: $g(z)$ is not ≥ 0 for all $z \in V(f) \cap \mathbb{R}^n$
    or Fail
  1: Construct $L(x,\lambda)$ as defined in Lemma 6.4.
  2: Compute $\{(z_1, \mu_1) \ldots, (z_k, \mu_k)\} \subset \mathbb{C}^{n+s}$, finitely many approximate roots of the real polynomial system $L(x,\lambda)$ as defined in Lemma 6.4, together with their precision E and a bound M such that $\|z_i\| \leq M + E$ for $i = 1, \ldots, k$. Return Fail if $L(x,\lambda)$ has infinitely many roots or $z_i = z_j$ for some $1 \leq i < j \leq k$.
  3: Compute $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_k}\}$ connected to 1, such that the Vandermonde matrix $V_{\mathcal{B}}(z_1, \ldots, z_k)$ has smallest singular value is greater than $knd M^{d-1} E$, where d is the maximal degree of the monomials in $\mathcal{B}$ (see Proposition 6.8). Let $\mathcal{B}^+ := \bigcup_i x_i \mathcal{B} \cup \bigcup_j \lambda_j \mathcal{B}$.
  4: $H_1^+ \leftarrow$ Hermite Matrix Computation$\left(\mathcal{B}, \mathcal{B}^+, E, M, \{(z_1, \mu_1), \ldots, (z_k, \mu_k)\}\right)$ (see Algorithm 3.1)

5: For $J := \langle L(x, \lambda) \rangle$ compute $H_g(J)$ and $H_{g^2}(J)$ by calling HERMITE MATRIX CERTIFICATION with input $L(x, \lambda), g, \mathcal{B}, \mathcal{B}^+, H_1^+$ and $L(x, \lambda), g^2, \mathcal{B}, \mathcal{B}^+, H_1^+$ respectively, which algorithm can also return Fail (see Algorithm 4.1)

6: Calculate the signatures $\sigma(H_g(J))$ and $\sigma(H_{g^2}(J))$ (see Remark 2.8)

7: if $\sigma(H_g(J)) = \sigma(H_{g^2}(J))$, then return True
else return False

7. Application: real root certification with Hermite matrices

Let $f = (f_1, \ldots, f_m) \in \mathbb{Q}[x_1, \ldots, x_n]^m$ such that $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ is a zero dimensional radical ideal. The certification problem is the following: We are given $z^* \in \mathbb{Q}^n$, $\varepsilon \in \mathbb{Q}_+$ and we would like to know if there is a root of f within the ε ball of z^* in $\mathbb{R}^n$. In this section, we present how one can use the signature of Hermite matrices to answer this certification problem as an application of Hermite matrices.

Now we introduce the certification theorem as a corollary of the Multivariate Hermite Theorem 2.7.

Corollary 7.1. *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^*.

Proof. By Theorem 2.7, $\sigma(H_g(\mathcal{I})) = \#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) > 0\} - \#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) < 0\}$. Since 1 is greater than 0, the signature of $H_1(\mathcal{I})$ gives the number of all real roots of $\mathcal{I}$. Thus, it can be written as

$$\sigma(H_1(\mathcal{I})) = \#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) > 0\} + \#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) < 0\} + \#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) = 0\} \quad (9)$$

for any $g(x) \in \mathbb{R}[x_1, \ldots, x_n]$. Now, let $g(x) = \|x - z^*\|_2^2 - \varepsilon^2 \in \mathbb{R}[x_1, \ldots, x_n]$.
Assume that $\sigma(H_1(\mathcal{I})) = \sigma(H_g(\mathcal{I}))$. Using the definitions above and canceling the terms $\#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) > 0\}$ from both sides, we have $2\#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) < 0\} = -\#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) = 0\}$. The only solution to this equation is

$$\#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) < 0\} = 0 \text{ and } \#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) = 0\} = 0,$$

since these terms are nonnegative integers by definition. This implies that there is no real solution to $\mathcal{I}$, when $g(x) < 0$ and $g(x) = 0$. By the definition of $g(x) = \|x - z^*\|_2^2 - \varepsilon^2$, there is no $x \in \mathbb{R}^n$ such that $\|x - z^*\|_2^2 \leq \varepsilon^2$. Thus we conclude that there is no real root within the closed ball of radius ε.
Assume that there is no real root to $\mathcal{I}$ within the closed ball in $\mathbb{R}^n$ of radius ε around z^*. It implies that any $x \in V_\mathbb{R}(\mathcal{I})$ satisfies the inequality $\|x - z^*\|_2^2 > \varepsilon^2$. Then $g(x) = \|x - z^*\|_2^2 - \varepsilon^2$ is always positive, and $\#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) \leq 0\} = 0$. By Theorem 2.7 and (9), we have

$$\sigma(H_1(\mathcal{I})) = \sigma(H_g(\mathcal{I})) = \#\{x \in V_\mathbb{R}(\mathcal{I}) \mid g(x) > 0\}. \quad \square$$

Algorithm 7.2 *(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.

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 $\left(\mathcal{B}, \mathcal{B}^+, E, M, \{z_1, \ldots, z_k\}\right)$
(see Algorithm 3.1)

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 (see Algorithm 4.1)

4: Compute $\sigma(H_1(\mathcal{I}))$ and $\sigma(H_g(\mathcal{I}))$. See Remark 2.8 for computational details.

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

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

Apostol, T.M., 1969. Calculus, Volume II: Multi-Variable Calculus and Linear Algebra, with Applications to Differential Equations and Probability. John Wiley & Sons.

Ayyildiz Akoglu, T., Szanto, A., 2020. Certified Hermite matrices from approximate roots-univariate case. In: MACIS 2019. In: Lecture Notes in Computer Science Book Series, vol. 11989, pp. 3–9.

Ayyildiz Akoglu, T., Hauenstein, J.D., Szanto, A., 2018. Certifying solutions to overdetermined and singular polynomial systems over $\mathbb{Q}$. J. Symb. Comput. 84, 147–171.

Ayyildiz Akoglu, T., 2016. Certifying solutions to polynomial systems over $\mathbb{Q}$. PhD thesis. North Carolina State University.

Bardet, M., Faugère, J.C., Salvy, B., 2004. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proceedings of the International Conference on Polynomial System Solving, ICPSS'04, pp. 71–75.

Bardet, M., Faugère, J.C., Salvy, B., Yang, B.Y., 2005. Asymptotic behavior of the degree of regularity of semi-regular polynomial systems. In: MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry. 15 p.

Basu, S., Pollack, R., Roy, M.-F., 2006. Algorithms in Real Algebraic Geometry. Springer-Verlag, Berlin Heidelberg.

Bates, D.J., Decker, W., Hauenstein, J.D., Peterson, C., Pfister, G., Schreyer, F.O., Sommese, A.J., Wampler, C.W., 2014. Comparison of probabilistic algorithms for analyzing the components of an affine algebraic variety. Appl. Math. Comput. 231, 619–633.

Blum, L., Cucker, F., Shub, M., Smale, S., 1998. Complexity and Real Computation. With a foreword by Richard M. Karp Springer-Verlag, New York.

Cifuentes, D., Parrilo, P., 2017. Sampling algebraic varieties for sum of squares programs. SIAM J. Optim. 27 (4), 2381–2404.

Cox, D.A., Little, J., O'shea, D., 2006. Using Algebraic Geometry (vol. 185). Springer Science & Business Media.

Bates, D.J., Hauenstein, J.D., Sommese, A.J., Wampler, C.W., 2013. Numerically Solving Polynomial Systems with Bertini, vol. 25. SIAM.

Emiris, I., Mourrain, B., Tsigaridas, E., 2020. Separation bounds for polynomial systems. J. Symb. Comput. 101, 128–151.

Hauenstein, J.D., Sottile, F., 2012. Algorithm 921: alphaCertified: certifying solutions to polynomial systems. ACM Trans. Math. Softw. 38 (4), 28.

Hashemi, A., Lazard, D., 2005. Complexity of Zero-dimensional Gröbner Bases. [Research Report] RR-5660, INRIA. p. 29. ffinria-00070348f.

Hermite, C., 1850. Sur le nombre des racines d'une équation algébrique comprise entre des limites données. J. Reine Angew. Math. 52, 39–51. also in Oeuvres completes, vol. 1, pp. 397-414.

Hermite, C., 1853. Remarques sur le théorème de Sturm. C. R. Math. Acad. Sci. Paris 36 (52–54), 171.

Hermite, C., 1856. 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. J. Reine Angew. Math. 52, 39–51.

Janovitz-Freireich, I., Rónyai, L., Szántó, A., 2007. Approximate radical for clusters: a global approach using Gaussian elimination or SVD. Math. Comput. Sci. 1, 393.

Macdonald, I.G., 1979. Symmetric Functions and Hall Polynomials. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, Oxford.

Mourrain, B., 1999. A new criterion for normal form algorithms. In: Fossorier, M., Imai, H., Lin, Shu, Poli, A. (Eds.), Proc. AAECC. In: LNCS, vol. 1719. Springer, Berlin, pp. 430–443.

Pedersen, P., Roy, M.F., Szpirglas, A., 1993. Counting real zeros in the multivariate case. In: Computational Algebraic Geometry. Birkhäuser, Boston, MA, pp. 203–224.

Schrijver, A., 1998. Theory of Linear and Integer Programming. JohnWiley & Sons, New York.

Stickelberger, L., 1890. Ueber eine Verallgemeinerung der Kreistheilung. Math. Ann. 37, 312–367.