Solving parametric systems of polynomial equations over the reals through Hermite matrices

Huu Phuoc Le, Mohab Safey El Din[1]

Sorbonne Université, CNRS, LIP6, F-75005, Paris, France

Abstract

We design a new algorithm for solving parametric systems of equations having finitely many complex solutions for generic values of the parameters. More precisely, let $\boldsymbol{f} = (f_1, \ldots, f_m) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ with $\boldsymbol{y} = (y_1, \ldots, y_t)$ and $\boldsymbol{x} = (x_1, \ldots, x_n)$, $\mathcal{V} \subset \mathbb{C}^t \times \mathbb{C}^n$ be the algebraic set defined by the simultaneous vanishing of the f_i's and π be the projection $(\boldsymbol{y}, \boldsymbol{x}) \to \boldsymbol{y}$. Under the assumptions that $\boldsymbol{f}$ admits finitely many complex solutions when specializing $\boldsymbol{y}$ to generic values and that the ideal generated by $\boldsymbol{f}$ is radical, we solve the following algorithmic problem. On input $\boldsymbol{f}$, we compute semi-algebraic formulas defining open semi-algebraic sets $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ in the parameters' space $\mathbb{R}^t$ such that $\cup_{i=1}^{\ell} \mathcal{S}_i$ is dense in $\mathbb{R}^t$ and, for $1 \leq i \leq \ell$, the number of real points in $\mathcal{V} \cap \pi^{-1}(\eta)$ is invariant when η ranges over $\mathcal{S}_i$.

This algorithm exploits special properties of some well chosen monomial bases in the quotient algebra $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/I$ where $I \subset \mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ is the ideal generated by $\boldsymbol{f}$ in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ as well as the specialization property of the so-called Hermite matrices which represent Hermite's quadratic forms. This allows us to obtain "compact" representations of the semi-algebraic sets $\mathcal{S}_i$ by means of semi-algebraic formulas encoding the signature of a given symmetric matrix.

When $\boldsymbol{f}$ satisfies extra genericity assumptions (such as regularity), we use the theory of Gröbner bases to derive complexity bounds both on the number of arithmetic operations in $\mathbb{Q}$ and the degree of the output polynomials. More precisely, letting d be the maximal degrees of the f_i's and $\mathfrak{D} = n(d-1)d^n$, we prove that, on a generic input $\boldsymbol{f} = (f_1, \ldots, f_n)$, one can compute those semi-algebraic formulas using $O^{\sim}\left(\binom{t+\mathfrak{D}}{t}\, 2^{3t}\, n^{2t+1} d^{3nt+2(n+t)+1}\right)$ arithmetic operations in $\mathbb{Q}$ and that the polynomials involved in these formulas have degree bounded by $\mathfrak{D}$.

We report on practical experiments which illustrate the efficiency of this algorithm, both on generic parametric systems and parametric systems coming from applications since it allows us to solve systems which were out of reach on the current state-of-the-art.

Keywords: Real algebraic geometry; Polynomial system solving; Real root classification; Hermite quadratic forms; Gröbner bases

Email addresses: huu-phuoc.le@lip6.fr (Huu Phuoc Le), mohab.safey@lip6.fr (Mohab Safey El Din)

[1]Mohab Safey El Din and Huu Phuoc Le are supported by the ANR grants ANR-18-CE33-0011

1. Introduction

1.1. Problem statement and motivations

In the whole paper, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote respectively the fields of rational, real and complex numbers.

Let $\boldsymbol{f} = (f_1, \ldots, f_m)$ be a polynomial sequence in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ where the indeterminates $\boldsymbol{y} = (y_1, \ldots, y_t)$ are considered as parameters and $\boldsymbol{x} = (x_1, \ldots, x_n)$ are considered as variables. We denote by $\mathcal{V} \subset \mathbb{C}^t \times \mathbb{C}^n$ the (complex) algebraic set defined by $f_1 = \cdots = f_m = 0$ and by $\mathcal{V}_{\mathbb{R}}$ its real trace $\mathcal{V} \cap \mathbb{R}^{t+n}$. We consider also the projection on the parameter space $\boldsymbol{y}$

$$\pi : \begin{array}{cl} \mathbb{C}^t \times \mathbb{C}^n & \to \mathbb{C}^t, \\ (\boldsymbol{y}, \boldsymbol{x}) & \mapsto \boldsymbol{y}. \end{array}$$

Further, we say that $\boldsymbol{f}$ satisfies Assumption (A) when the following holds.

Assumption A. There exists a non-empty Zariski open subset $\mathcal{O} \subset \mathbb{C}^t$ such that $\pi^{-1}(\eta) \cap \mathcal{V}$ is non-empty and finite for any $\eta \in \mathcal{O}$.

In other words, assuming (A) ensures that, for a generic value η of the parameters, the sequence $\boldsymbol{f}(\eta, \cdot)$ defines a finite algebraic set and hence finitely many real points. Note that, it is easy to prove that one can choose $\mathcal{O}$ in a way that the number of complex solutions to the entries of $\boldsymbol{f}(\eta, \cdot)$ is invariant when η ranges over $\mathcal{O}$ (e.g. using the theory of Gröbner basis). This is no more the case when considering real solutions whose number may vary when η ranges over $\mathcal{O}$.

By Hardt's triviality theorem [27], there exists a real algebraic proper subset $\mathcal{R}$ of $\mathbb{R}^t$ such that, for any non-empty connected open set $\mathcal{U}$ of $\mathbb{R}^t \setminus \mathcal{R}$ and $\eta \in \mathcal{U}$, $\pi^{-1}(\eta) \times \mathcal{U}$ is homeomorphic with $\pi^{-1}(\mathcal{U})$.

This leads us to consider the following real root classification problem.

Problem 1 (Real root classification). On input $\boldsymbol{f}$ satisfying Assumption (A), compute semi-algebraic formulas (i.e. finitely many disjunctions of conjunctions of polynomial inequalities) defining semi-algebraic sets $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ such that

(i) The number of real points in $\mathcal{V} \cap \pi^{-1}(\eta)$ is invariant when η ranges over $\mathcal{S}_i$, for $1 \leq i \leq \ell$;

(ii) The union of the $\mathcal{S}_i$'s is dense in $\mathbb{R}^t$;

as well as at least one sample point η_i in each $\mathcal{S}_i$ and the corresponding number of real points in $\mathcal{V} \cap \pi^{-1}(\eta_i)$.

A collection of semi-algebraic formulas sets is said to solve Problem (1) for the input $\boldsymbol{f}$ if it defines a collection of semi-algebraic sets $\mathcal{S}_i$ satisfies the above properties (i) and (ii).

Our output will have the form $\{(\Phi_i, \eta_i, r_i) \mid 1 \leq i \leq \ell\}$ where Φ_i is a semi-algebraic formula defining the set $\mathcal{S}_i$, $\eta_i \in \mathbb{Q}^t$ is a sample point of $\mathcal{S}_i$ and r_i is the corresponding number of real roots.

Sesame, and ANR-19-CE40-0018 De Rerum Natura, the joint ANR-FWF ANR-19-CE48-0015 ECARP project, the PGMO grant CAMiSAdo, the European Union's Horizon 2020 research and innovative training network program under the Marie Skłodowska-Curie grant agreement N° 813211 (POEMA) and the Grant FA8665-20-1-7029 of the EOARD-AFOSR.

A weak version of Problem (1) would be to compute only a set $\{\eta_1, \ldots, \eta_\ell\}$ of sample points for a collection of semi-algebraic sets $\mathcal{S}_i$ solving Problem (1) and their corresponding numbers of real points in $\mathcal{V} \cap \pi^{-1}(\eta_j)$.

Problem (1) appears in many areas of engineering sciences such as robotics or medical imagery (see, e.g., [50, 10, 51, 19, 6]).

In this paper, we design a new algorithm whose arithmetic complexity improves the previously known bounds and reports on practical experiments showing that its practical behaviour outperforms the current software state-of-the-art.

Before going further with a description of the prior works and our contributions, we introduce the complexity model which we use. We measure only the arithmetic complexity of algorithms, i.e., the number of arithmetic operations $+, -, \times, \div$, in the base field $\mathbb{Q}$, hence, without taking into account the cost of real root isolation. We use the Landau notation:

- Let $f : \mathbb{R}_+^\ell \mapsto \mathbb{R}_+$ be a positive function. We let $O(f)$ denote the class of functions $g : \mathbb{R}_+^\ell \to \mathbb{R}_+$ such that there exist $C, K \in \mathbb{R}_+$ such that for all $\|x\| \geq K$, $g(x) \leq Cf(x)$, where $\|\cdot\|$ is a norm of $\mathbb{R}^\ell$.
- The notation $O^{\sim}$ denotes the class of functions $g : \mathbb{R}_+^\ell \to \mathbb{R}_+$ such that $g \in O(f \log^\kappa(f))$ for some $\kappa > 0$.

Further, the notation ω always stands for the exponent constant of the matrix multiplication, i.e., the smallest positive number such that the product of two matrices in $\mathbb{Q}^{N \times N}$ can be done using $O(N^\omega)$ arithmetic operations in $\mathbb{Q}$. The value of ω can be bounded from above by 2.37286, which is established in [1].

1.2. Prior works

A first approach to Problem (1) would be to compute a cylindrical algebraic decomposition (CAD) of $\mathbb{R}^t \times \mathbb{R}^n$ adapted to $\boldsymbol{f}$ using e.g. Collins' algorithm (and its more recent improvements) ; see [9]. While, up to our knowledge, there is no clear reference for this fact, the cylindrical structure of the cells of the CAD will imply that their projection on the parameters' space $\mathbb{R}^t$ define semi-algebraic sets enjoying the properties needed to solve Problem (1). However, the doubly exponential complexity of CAD both in terms of runtime and output size [14, 7] makes it difficult to use in practice.

A more popular approach consists in computing polynomials $h_1, \ldots, h_r$ in $\mathbb{Q}[\boldsymbol{y}]$ such that $\cup_{i=1}^r V(h_i) \cap \mathbb{R}^t$ contains the boundaries of semi-algebraic sets $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ enjoying the properties required to solve Problem (1). Next, one needs to compute semi-algebraic descriptions of the connected components of $\mathbb{R}^t \setminus \cup_{i=1}^r V(h_i)$ as well as sample points in these connected components. This is basically the approach followed by [49] (the h_i's are called border polynomials) and [35] (the set $\cup_{i=1}^r V(h_i)$ is called discriminant variety) under the assumption that $\langle \boldsymbol{f} \rangle$ is a radical ideal. Note that both [49] and [35] provide algorithms that can handle variants of Problem (1) allowing inequalities. In this paper, we focus on the situation where we only have equations in our input parametric system.

When $\langle \boldsymbol{f} \rangle$ is radical and the restriction of π to $\mathcal{V} \cap \mathbb{R}^t \times \mathbb{R}^n$ is proper, one can easily prove using a semi-algebraic version of Thom's isotopy lemma [11] that one can choose $\cup_{i=1}^r V(h_i)$ to be the set of critical values of the restriction of π to $\mathcal{V}$ (see e.g. [6]). If $\boldsymbol{f}$ is a regular sequence (hence $m = n$), the critical set of the restriction of π to $\mathcal{V}$ is defined as the intersection of $\mathcal{V}$ with the hypersurface defined by the vanishing of the determinant of the Jacobian matrix of $\boldsymbol{f}$ with respect to the variables $\boldsymbol{x}$. When d dominates the degrees of the entries of $\boldsymbol{f}$, Bézout's theorem allows us to state that the degree of this set is bounded above by $n(d-1)d^n$.

It is worth noticing that, usually, this approach is used only to solve the aforementioned weak version of Problem (1) as getting a semi-algebraic description of the connected components of $\mathbb{R}^t \setminus \cup_{i=1}^r V(h_i)$ through CAD is too expensive when $t \geq 4$ (still, because of the doubly exponential complexity of CAD). Under the above assumptions and notation, the output degree of the polynomials in such formulas would be bounded by $(n(d-1)d^n)^{2^{O(t)}}$.

An alternative would be to use parametric roadmap algorithms to do such computations using e.g. [4, Chap. 16] to compute semi-algebraic representations of the connected components of $\mathbb{R}^t \setminus \cup_{i=1}^r V(h_i)$. Under the above extra assumptions, this would result in output formulas involving polynomials of degree bounded by $(n(d-1)d^n)^{O(t^3)}$ using $(n(d-1)d^n)^{O(t^4)}$ arithmetic operations (see [4, Theorem 16.13]). Note that the output degrees are by several orders of magnitude larger than $n(d-1)d^n$ which bounds the degree of the set of critical values of the restriction of π to $\mathcal{V}$.

Hence, one topical algorithmic issue is to design an efficient algorithm for solving Problem (1) which would output semi-algebraic formulas of degree bounded by $n(d-1)d^n$ (using a number of arithmetic operations polynomial in this quantity). At this stage of our exposition, this is not clear that it is doable. Actually, admittedly "folklore" algorithms in symbolic computation already allow one to achieve such a result.

Using the (probabilistic) algorithm of [44], one can compute a rational parametrization of $\mathcal{V} = V(\boldsymbol{f})$ with respect to the $\boldsymbol{x}$-variables, i.e. a sequence of polynomials $(w, v_1, \dots, v_n)$ in $\mathbb{Q}(\boldsymbol{y})[u]$ where u is a new variable, such that the constructible set $\mathcal{Z} \subset \mathbb{C}^t \times \mathbb{C}^n$ of every point

$$\left(\eta, \frac{v_1}{\partial w/\partial u}(\eta, \vartheta), \dots, \frac{v_n}{\partial w/\partial u}(\eta, \vartheta)\right),$$

where $(\eta, \vartheta) \in \mathbb{C}^t \times \mathbb{C}$ such that $w(\eta, \vartheta) = 0$ and η does not cancel $\partial w/\partial u$ and any denominator of $(w, v_1, \dots, v_n)$, is Zariski dense in $\mathcal{V}$, i.e., the Zariski closure of $\mathcal{Z}$ coincides with $\mathcal{V}$.

The bi-rational equivalence between $\mathcal{Z}$ and its projection on the $(u, \boldsymbol{y})$-space implies that semi-algebraic formulas solving Problem (1) can be obtained through the computation of the subresultant sequence associated to $\left(w, \frac{\partial w}{\partial u}\right)$ (see e.g. [4, Chap. 4]). Combining the complexity results of [44] to compute a rational parametrization of $\mathcal{V}$ with those of [4, Chap. 4] for computing subresultants we obtain that this algorithm uses

$$O^{\sim}\left(\binom{t+2d^{2n}}{t} 2^{5t} \, d^{5nt+3n}\right)$$

arithmetic operations in $\mathbb{Q}$, and that the semi-algebraic formulas computed by this algorithm involve polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree bounded by $2d^{2n}$. Recall that the degree of the critical locus of the restriction of π to $\mathcal{V}$ is bounded by $n(d-1)d^n$. Hence, computing semi-algebraic formulas solving Problem (1) involving polynomials of degrees in $O(d^n)$ through an efficient algorithm reflecting this complexity gain is still an open problem.

1.3. Main results

Basically, our main result is to provide a new algorithm solving Problem (1) when $\langle \boldsymbol{f} \rangle$ is radical and assumption (A) holds. Under some genericity assumptions, we prove that it outputs formulas involing polynomials of degree in $O(d^n)$ with a better arithmetic complexity than what was previously known.

Theorem I. Let $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_d$ be the set of polynomials in $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]$ having total degree bounded by d and set $\mathfrak{D} = n(d-1)d^n$.

There exists a non-empty Zariski open set $\mathscr{F} \subset \mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_d^n$ such that for $\boldsymbol{f} = (f_1, \ldots, f_n) \in \mathscr{F} \cap \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]^n$, the following holds:

i) There exists an algorithm that computes a solution for the weak-version of Problem (1) within
$$O^{\sim}\left(\binom{t+\mathfrak{D}}{t} 2^{3t}\ n^{2t+1} d^{2nt+n+2t+1}\right).$$
arithmetic operations in $\mathbb{Q}$.

ii) There exists a probabilistic algorithm that returns the formulas of a collection of semi-algebraic sets solving Problem (1) within
$$O^{\sim}\left(\binom{t+\mathfrak{D}}{t} 2^{3t}\ n^{2t+1} d^{3nt+2(n+t)+1}\right)$$
arithmetic operations in $\mathbb{Q}$ in case of success.

iii) The semi-algebraic descriptions output by the above algorithm involves polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree bounded by $\mathfrak{D}$.

We note that the binomial coefficient $\binom{t+\mathfrak{D}}{t}$ is bounded from above by $\mathfrak{D}^t \simeq n^t d^{nt+t}$. Therefore, the complexities given in the items i) and ii) of Theorem I can be bounded by $O^{\sim}\left(2^{3t}\ n^{3t} d^{3nt}\right)$ and $O^{\sim}\left(2^{3t}\ n^{3t} d^{4nt}\right)$ respectively.

We also implemented this algorithm to illustrate its practical behaviour and compare it with the state-of-the-art software within the Maple packages RootFinding[Parametric] and RegularChains[ParametricSystemTools]. We report on experiments showing that our implementation outperforms these packages, which is justified by our complexity result.

The key ingredient on which one relies to obtain these results is a set of well-known properties of Hermite quadratic forms to count the real roots of zero-dimensional ideals. The use of such quadratic forms for counting the number of real solutions was introduced in [30] and then later on generalized by [38] and used in [39]. We refer to [4, Theorem 4.102] for the explicit relation between the number of real roots of a zero-dimensional algebraic set and the signature of these quadratic forms and to [4, Algo. 8.43] for an algorithm computing these signatures.

We first slightly extend the definition of Hermite's quadratic forms and Hermite's matrices to the context of parametric systems; we call them parametric Hermite quadratic forms and parametric Hermite matrices. This is easily done since the ideal of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ generated by $\boldsymbol{f}$, considering $\mathbb{Q}(\boldsymbol{y})$ as the base field, has dimension zero. We also establish natural specialization properties for these parametric Hermite matrices.

Hence, a parametric Hermite matrix, similar to its zero-dimensional counterpart, allows one to count respectively the number of distinct real and complex roots at any parameters outside a strict algebraic sets of $\mathbb{R}^t$ by evaluating the signature and rank of its specialization.

Based on this specialization property, we design two algorithms for solving Problem (1) and also its weak version for the input system $\boldsymbol{f}$ which satisfies Assumption (A) and generates a radical ideal.

Our algorithm for the weak version of Problem (1) reduces to the following main steps.

(a) Compute a parametric Hermite matrix $\mathcal{H}$ associated to $\boldsymbol{f} \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$.

(b) Compute a set of sample points $\{\eta_1, \ldots, \eta_\ell\}$ in the connected components of the semi-algebraic set of $\mathbb{R}^t$ defined by $\boldsymbol{w} \neq 0$ where $\boldsymbol{w}$ is derived from $\mathcal{H}$.

This is done through the so-called critical point method (see e.g. [4, Chap. 12] and references therein) which are adapted to obtain practically fast algorithms following [41]. We will explain in detail this step in Section 3.

This algorithm takes as input s polynomials of degree D involving t variables and computes sample points per connected components in the semi-algebraic set defined by the non-vanishing of these polynomials using

$$O\tilde{~}\left(\binom{D+t}{t} s^{t+1} 2^{3t} D^{2t+1}\right).$$

(c) Compute the number r_i of real points in $\mathcal{V} \cap \pi^{-1}(\eta_i)$ for $1 \leq i \leq \ell$.

This is done by simply evaluating the signature of the specialization of $\mathcal{H}$ at each η_i.

It is worth noting that, in the algorithm above, we obtain through parametric Hermite matrices a polynomial $\boldsymbol{w}$ that plays the same role as the discriminant varieties of [35] or the border polynomials of [48]. We will see in the section reporting experiments that our approach outperforms the other two on every example we consider.

To return semi-algebraic formulas, our routine is basically the same except instead of computing sample points in the set $\{w \neq 0\}$, one needs to consider all principal minors of the matrix $\mathcal{H}$ and compute sample points outside the union of the vanishing sets of all these polynomials.

Another contribution of this paper is to make clear how to perform the step (a). For this, we rely on the theory of Gröbner bases. More precisely, we use specialization properties of Gröbner bases, similar to those already proven in [32]. This leaves some freedom when running the algorithm: since we rely on Gröbner bases, one may choose monomial orderings which are more convenient for practical computations. In particular, the monomial basis of the quotient ring $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/I$ where I is the ideal generated by $\boldsymbol{f}$ in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ depends on the choice of the monomial ordering used for Gröbner bases computations. We describe the behavior of our algorithm when choosing the graded reverse lexicographical ordering whose interest for practical computations is explained in [5]. Further, we denote by $\mathsf{grevlex}(\boldsymbol{x})$ the graded reverse lexicographical ordering applied to the sequence of the variables $\boldsymbol{x} = (x_1, \dots, x_n)$ (with $x_1 \succ \cdots \succ x_n$). Further, we also denote by $\succ_{lex}$ the lexicographical ordering.

We report, at the end of the paper, on the practical behavior of this algorithm. We compare with two Maple packages RootFinding[Parametric] and RegularChains[ParametricSystemTools] which respectively implement the algorithms of [35] and [49]. In particular, our algorithm allows us to solve instances of Problem (1) which were not tractable by the state-of-the-art as well as the actual degrees of the polynomials in the output formula which are bounded by $n(d-1)d^n$.

We actually prove such a statement under some generic assumptions. Our main complexity result is stated below. Its proof is given in Subsection 6.2, where the generic assumptions in use are given explicitly.

Organization of the paper. Section 2 reviews fundamental notions of algebraic geometry and the theory of Gröbner bases that we use further. Next, we present a dedicated algorithm for computing at least one point per connected component of a semi-algebraic defined by a list of inequations in Section 3. Section 4 lies the definition and some useful properties of parametric Hermite matrices. In Section 5, we describe our algorithm for solving the real root classification problem using this parametric Hermite matrix. The complexity analysis of the algorithms mentioned above is given in Section 6. Finally, in Section 7, we report on the practical behavior of our algorithms and illustrate its practical capabilities.

2. Preliminaries

In the first paragraph, we fix some notations on ideals and algebraic sets and recall the definition of critical points associated to a given polynomial map. Next, we give the definitions of regular sequences, Hilbert series, Noether position and proper maps, which are used later in Subsection 6.1. The fourth paragraph recalls some basic properties of Gröbner bases and quotient algebras of zero-dimensional ideals. We refer to [12] for an introductory study on the algorithmic theory of Gröbner bases. In the last paragraphs, we recall respectively the definitions of zero-dimensional parametrizations and rational parametrizations which go back to [33] and is widely used in computer algebra (see e.g. [24, 26, 25]) to represent finite algebraic sets.

Algebraic sets and critical points. We consider a sub-field $\mathbb{F}$ of $\mathbb{C}$. Let I be a polynomial ideal of $\mathbb{F}[x_1, \dots, x_n]$, the algebraic subset of $\mathbb{C}^n$ at which the elements of I vanish is denoted by $V(I)$. Conversely, for an algebraic set $\mathcal{V} \subset \mathbb{C}^n$, we denote by $I(\mathcal{V}) \subset \mathbb{C}[x_1, \dots, x_n]$ the radical ideal associated to $\mathcal{V}$. Given any subset $\mathcal{A}$ of $\mathbb{C}^n$, we denote by $\overline{\mathcal{A}}$ the Zariski closure of $\mathcal{A}$, i.e., the smallest algebraic set containing $\mathcal{A}$.

A map φ between two algebraic sets $\mathcal{V} \subset \mathbb{C}^n$ and $\mathcal{W} \subset \mathbb{C}^s$ is a polynomial map if there exist $\varphi_1, \dots, \varphi_t \in \mathbb{C}[x_1, \dots, x_n]$ such that the $\varphi(\eta) = (\varphi_1(\eta), \dots, \varphi_s(\eta))$ for $\eta \in \mathcal{V}$.

An algebraic set $\mathcal{V}$ is equi-dimensional of dimension t if it is the union of irreducible algebraic sets of dimension t. Let φ be a polynomial map from $\mathcal{V}$ to another algebraic set $\mathcal{W}$. The morphism φ is dominant if and only if the image of every irreducible component $\mathcal{V}'$ of $\mathcal{V}$ by φ is Zariski dense in $\mathcal{W}$, i.e. $\overline{\varphi(\mathcal{V}')} = \mathcal{W}$.

Let $\phi \in \mathbb{C}[x_1, \ldots, x_n]$ which defines the polynomial function

$$\phi : \begin{array}{rl} \mathbb{C}^n & \to \mathbb{C}, \\ (x_1, \ldots, x_n) & \mapsto \phi(x_1, \ldots, x_n) \end{array}$$

and $\mathcal{V} \subset \mathbb{C}^n$ be a smooth equi-dimensional algebraic set. We denote by $\mathsf{crit}(\phi, \mathcal{V})$ the set of critical points of the restriction of ϕ to $\mathcal{V}$. If c is the codimension of $\mathcal{V}$ and $(f_1, \ldots, f_m)$ generates the vanishing ideal associated to $\mathcal{V}$, then $\mathsf{crit}(\phi, \mathcal{V})$ is the subset of $\mathcal{V}$ at which the Jacobian matrix associated to $(f_1, \ldots, f_m, \phi)$ has rank less than or equal to c (see, e.g., [42, Subsection 3.1]).

Regular sequences & Hilbert series. Let $\mathbb{F}$ be a field and $(f_1, \ldots, f_m) \subset \mathbb{F}[\boldsymbol{x}]$ where $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $m \leq n$ be a homogeneous polynomial sequence. We say that $(f_1, \ldots, f_m) \subset \mathbb{F}[\boldsymbol{x}]$ is a regular sequence if for any $i \in \{1, \ldots, m\}$, f_i is not a zero-divisor in $\mathbb{F}[\boldsymbol{x}]/\langle f_1, \ldots, f_{i-1}\rangle$.

The notion of regular sequences is the algebraic analogue of complete intersection. In this paper, we focus particularly on the Hilbert series of homogeneous regular sequences, which are recalled below.

Let $I \subset \mathbb{F}[\boldsymbol{x}]$ be a homogeneous ideal. We denote by $\mathbb{F}[\boldsymbol{x}]_r$ the set of every homogeneous polynomial whose degree is equal to r. Then $\mathbb{F}[\boldsymbol{x}]_r$ and $I \cap \mathbb{F}[\boldsymbol{x}]_r$ are two $\mathbb{F}$-vector spaces of dimensions $\dim_{\mathbb{F}}(\mathbb{F}[\boldsymbol{x}]_r)$ and $\dim_{\mathbb{F}}(I \cap \mathbb{F}[\boldsymbol{x}]_r)$ respectively. The Hilbert series of I is defined as

$$\mathrm{HS}_I(z) = \sum_{r=0}^{\infty} (\dim_{\mathbb{F}}(\mathbb{F}[\boldsymbol{x}]_r) - \dim_{\mathbb{F}}(I \cap \mathbb{F}[\boldsymbol{x}]_r)) \cdot z^r.$$

We now consider the affine polynomial sequences. Note that one can define affine regular sequences by simply removing the homogeneity assumption of $(f_1, \ldots, f_m)$ from the above definition. However, as explained in [2, Sec 1.7], many important properties that hold for homogeneous regular sequences are no longer valid for the affine ones. Therefore, in this paper, we use [2, Definition 1.7.2] of affine regular sequences, which is more restrictive but allows us to preserve similar results as the homogeneous case. We recall that definition below.

For $p \in \mathbb{F}[x_1, \ldots, x_n]$, we denote by ${}^H p$ the homogeneous component of largest degree of p. A polynomial sequence $(f_1, \ldots, f_m) \subset \mathbb{F}[x_1, \ldots, x_n]$, not necessarily homogeneous, is called a regular sequence if and only if $({}^H f_1, \ldots, {}^H f_m)$ is a homogeneous regular sequence.

Noether position & Properness. Let $\mathbb{F}$ be a field and $\boldsymbol{f} = (f_1, \ldots, f_n) \subset \mathbb{F}[x_1, \ldots, x_{n+t}]$. The variables $(x_1, \ldots, x_n)$ are in Noether position with respect to the ideal $\langle \boldsymbol{f} \rangle$ if their canonical images in the quotient algebra $\mathbb{F}[x_1, \ldots, x_{n+t}]/\langle \boldsymbol{f} \rangle$ are algebraic integers over $\mathbb{F}[x_{n+1}, \ldots, x_{n+t}]$ and, moreover, $\mathbb{F}[x_{n+1}, \ldots, x_{n+t}] \cap \langle \boldsymbol{f} \rangle = \langle 0 \rangle$.

From a geometric point of view, Noether position is strongly related to the notion of proper map below (see [3]).

Let $\mathcal{V}$ be the algebraic set defined by $\boldsymbol{f} \in \mathbb{R}[y_1, \ldots, y_t, x_1, \ldots, x_n]$. The restriction of the projection $\pi : (\boldsymbol{y}, \boldsymbol{x}) \mapsto \boldsymbol{y}$ to $\mathcal{V} \cap \mathbb{R}^{t+n}$ is said to be proper if the inverse image of every compact subset of $\pi(\mathcal{V} \cap \mathbb{R}^{t+n})$ is compact. If the variables $\boldsymbol{x} = (x_1, \ldots, x_n)$ is in Noether position with respect to $\langle \boldsymbol{f} \rangle$, then the projection $\pi : \mathcal{V} \cap \mathbb{R}^{t+n} \to \mathbb{R}^t$, $(\boldsymbol{y}, \boldsymbol{x}) \mapsto \boldsymbol{y}$ is proper.

A point $\eta \in \mathbb{R}^t$ is a non-proper point of the restriction of π to $\mathcal{V}$ if and only $\pi^{-1}(\mathcal{U}) \cap \mathcal{V} \cap \mathbb{R}^{t+n}$ is not compact for any compact neighborhood $\mathcal{U}$ of η in $\mathbb{R}^t$.

Gröbner bases and zero-dimensional ideals. Let $\mathbb{F}$ be a field and $\overline{\mathbb{F}}$ be its algebraic closure. We denote by $\mathbb{F}[\boldsymbol{x}]$ the polynomial algebra in the variables $\boldsymbol{x} = (x_1, \ldots, x_n)$. We fix an admissible monomial ordering $\succ$ (see Section 2.2, [12]) over $\mathbb{F}[\boldsymbol{x}]$. For a polynomial $p \in \mathbb{F}[\boldsymbol{x}]$, the leading monomial of p with respect to $\succ$ is denoted by $\mathrm{lm}_{\succ}(p)$.

Given an ideal $I \subset \mathbb{F}[\boldsymbol{x}]$, the initial ideal of I with respect to the ordering $\succ$ is the ideal $\langle \mathrm{lm}_{\succ}(p) \mid p \in I \rangle$. A Gröbner basis G of I with respect to the ordering $\succ$ is a generating set of I such that the set of leading monomials $\{\mathrm{lm}_{\succ}(g) \mid g \in G\}$ generates the initial ideal $\langle \mathrm{lm}_{\succ}(p) \mid p \in I \rangle$.

For any polynomial $p \in \mathbb{F}[\boldsymbol{x}]$, the remainder of the division of p by G using the monomial ordering $\succ$ is uniquely defined. It is called the normal form of p with respect to G and is denoted by $\mathrm{NF}_G(p)$. A polynomial p is reduced by G if p coincides with its normal form in G. A Gröbner basis G is said to be reduced if, for any $g \in G$, all terms of g are reduced modulo the leading terms of G.

An ideal I is said to be zero-dimensional if the algebraic set $V(I) \subset \overline{\mathbb{F}}^n$ is finite and non-empty. By [12, Sec. 5.3, Theorem 6], the quotient ring $\mathbb{F}[\boldsymbol{x}]/I$ is a $\mathbb{F}$-vector space of finite dimension. The dimension of this vector space is also called the algebraic degree of I; it coincides with the number of points of $V(I)$ counted with multiplicities [4, Sec. 4.5]. For any Gröbner basis of I, the set of monomials in $\mathbb{F}[\boldsymbol{x}]$ which are irreducible by G forms a monomial basis, which we call B, of this vector space. For any $p \in \mathbb{F}[\boldsymbol{x}]$, the normal form of p by G can be interpreted as the image of p in $\mathbb{F}[\boldsymbol{x}]/I$ and is a linear combination of elements of B (with coefficients in $\mathbb{F}$). Therefore, the operations in the quotient algebra $\mathbb{F}[\boldsymbol{x}]/I$ such as vector additions or scalar multiplications can be computed explicitly using the normal form reduction.

In this article, while working with polynomial systems depending on parameters in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$, we frequently take $\mathbb{F}$ to be the rational function field $\mathbb{Q}(\boldsymbol{y})$ and treat polynomials in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ as elements of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$.

Zero-dimensional parametrizations. A zero-dimensional parametrization $\mathscr{R}$ of coefficients in $\mathbb{Q}$ consists of $(a_1, \ldots, a_n) \in \mathbb{Q}^n$ and a sequence of polynomials $(w, v_1, \ldots, v_n) \in (\mathbb{Q}[u])^{n+1}$ where $u = \sum_{i=1}^n a_i x_i$ such that w is square-free. The solution set of $\mathscr{R}$, defined as

$$Z(\mathscr{R}) = \left\{ \left(\frac{v_1(\vartheta)}{w'(\vartheta)}, \ldots, \frac{v_n(\vartheta)}{w'(\vartheta)} \right) \in \mathbb{C}^n \mid \vartheta \in \mathbb{C} \text{ such that } w(\vartheta) = 0 \right\},$$

is finite.

A finite algebraic set $\mathcal{V} \in \mathbb{C}^n$ is said to be represented by a zero-dimensional parametrization $\mathscr{R}$ if and only if $\mathcal{V}$ coincides with $Z(\mathscr{R})$. Note that the cardinality of $\mathcal{V}$ is the same as the degree of w ; we also call it the degree of the zero-dimensional parametrization.

Note that it is possible to retrieve a polynomial parametrization by inverting the derivative w' modulo w. Still, this rational parametrization whose denominator is the derivative of w is known to be better for practical computations as it usually involves coefficients with smaller bit size (see [13]).

3. Computing sample points in semi-algebraic sets defined by the non-vanishing of polynomials

In this section, we study the following algorithmic problem. Given $(g_1, \ldots, g_s)$ in $\mathbb{Q}[y_1, \ldots, y_t]$, compute at least one sample point per connected component of the semi-algebraic set $\mathcal{S} \subset \mathbb{R}^t$ defined by

$$g_1 \neq 0, \ldots, g_s \neq 0.$$

Such sample points will be encoded with zero-dimensional parametrizations which we described in Section 2.

The main result of this section which will be used in the sequel of this paper is the following.

Theorem II. Let $(g_1, \ldots, g_s)$ in $\mathbb{Q}[y_1, \ldots, y_t]$ with $D \geq \max_{1 \leq i \leq s} \deg(g_i)$ and $\mathcal{S} \subset \mathbb{R}^t$ be the semi-algebraic set defined by

$$g_1 \neq 0, \ldots, g_s \neq 0.$$

There exists a probabilistic algorithm which on input $(g_1, \ldots, g_s)$ outputs a finite family of zero-dimensional parametrizations $\mathscr{R}_1, \ldots, \mathscr{R}_k$, all of them of degree bounded by $(2D)^t$, which encode at most $(2sD)^t$ points such that $\cup_{i=1}^k Z(\mathscr{R}_i)$ meets every connected component of $\mathcal{S}$ using

$$O^{\sim}\left(\binom{D+t}{t} s^{t+1} 2^{3t} D^{2t+1}\right).$$

arithmetic operations in $\mathbb{Q}$.

The rest of this section is devoted to the proof of this theorem.

Proof. By [19, Lemma 1], there exists a non-empty Zariski open set $\mathscr{A} \times \mathscr{E} \subset \mathbb{C}^s \times \mathbb{C}$ such that for $(\boldsymbol{a} = (a_1, \ldots, a_s), e) \in \mathscr{A} \times \mathscr{E} \cap \mathbb{R}^s \times \mathbb{R}$, the following holds. For $\mathcal{I} = \{i_1, \ldots, i_\ell\} \subset \{1, \ldots, s\}$ and $\sigma = (\sigma_1, \ldots, \sigma_s) \in \{-1, 1\}^s$, the algebraic sets $V_{\boldsymbol{a},e}^{\mathcal{I},\sigma} \subset \mathbb{C}^t$ defined by

$$g_{i_1} + \sigma_{i_1} a_{i_1} e = \cdots = g_{i_\ell} + \sigma_{i_\ell} a_{i_\ell} e = 0$$

are, either empty, or $(t-\ell)$-equidimensional and smooth, and the ideal generated by their defining equations is radical.

Note that by the transfer principle, one can choose instead of a scalar e an infinitesimal ε so that the algebraic sets $V_{\boldsymbol{a},\varepsilon}^{\mathcal{I},\sigma}$ and their defining set of equations satisfy the above properties. When, in the above equations, one leaves ε as a variable, one obtains equations defining an algebraic set in $\mathbb{C}^{t+1}$. We denote by $\mathfrak{V}_{\boldsymbol{a},\varepsilon}^{\mathcal{I},\sigma}$ the union of the $(t+1-\ell)$-equidimensional components of this algebraic set.

Further we also assume that the a_i's are chosen positive.

Denote by $\mathcal{S}^{(\varepsilon)}$ the extension of the semi-algebraic set $\mathcal{S}$ to $\mathbb{R}\langle\varepsilon\rangle^t$; similarly, the extension of any connected component C of $\mathcal{S}$ to $\mathbb{R}\langle\varepsilon\rangle^t$ is denoted by $C^{(\varepsilon)}$.

Now, remark that any connected component $C^{(\varepsilon)}$ of $\mathcal{S}^{(\varepsilon)}$ contains a connected component of the semi-algebraic set $\mathcal{S}_{\boldsymbol{a}}^{(\varepsilon)}$ defined by:

$$(-a_1\varepsilon \geq g_1 \vee g_1 \geq a_1\varepsilon) \wedge \cdots \wedge (-a_s\varepsilon \geq g_s \vee g_s \geq a_s\varepsilon)$$

Hence, we are led to compute sample points per connected component of $\mathcal{S}_{\boldsymbol{a}}^{(\varepsilon)}$. These will be encoded with zero-dimensional parametrizations with coefficients in $\mathbb{Q}[\varepsilon]$.

By [4, Proposition 13.1], in order to compute sample points per connected component in $\mathcal{S}_{\boldsymbol{a}}^{(\varepsilon)}$, it suffices to compute sample points in the real algebraic sets $V_{\boldsymbol{a},\varepsilon}^{\mathcal{I},\sigma} \cap \mathbb{R}^t$. To do that, since the algebraic sets $V_{\boldsymbol{a},\varepsilon}^{\mathcal{I},\sigma}$ satisfy the above regularity properties, we can use the algorithm and geometric results of [41]. To state these results, one needs to introduce some notation.

Let $\mathfrak{Q}$ be a real field, $\mathfrak{R}$ be a real closure of $\mathfrak{Q}$ and $\mathfrak{C}$ be an algebraic closure of $\mathfrak{R}$. For an algebraic set $V \subset \mathfrak{C}^t$ defined by $h_1 = \cdots = h_\ell = 0$ ($h_i \in \mathfrak{Q}[\boldsymbol{y}]$ with $\boldsymbol{y} = (y_1, \ldots, y_t)$) and $M \in \mathrm{GL}_t(\mathfrak{R})$, we denote by V^M the set $\{M^{-1} \cdot \boldsymbol{x} \mid \boldsymbol{x} \in V\}$ and, for $1 \leq i \leq \ell$, by ${h_i}^M$ the polynomial $h_i(M \cdot \boldsymbol{y})$ and by π_i the canonical projection $(y_1, \ldots, y_t) \mapsto (y_1, \ldots, y_i)$ (π_0 will simply denote $(y_1, \ldots, y_t) \mapsto \{\bullet\}$). By slightly abusing notation, we will also denote by π_i projections from $\mathfrak{V}^{\mathcal{I},\sigma}_{\boldsymbol{a},\varepsilon}$ to the first i coordinates $(y_1, \ldots, y_i)$.

We will consider the set of critical points of the restriction of π_i to V and will denote this set by $\mathsf{crit}(\pi_i, V)$ for $1 \leq i \leq \ell$. By [41, Theorem 2], for a generic choice of $M \in \mathrm{GL}_t(\mathfrak{R})$, the union of $V^M \cap \pi_{t-\ell}^{-1}(0)$ with the sets $\mathrm{crit}(\pi_i, V^M) \cap \pi_{i-1}^{-1}(0)$ (for $1 \leq i \leq t-\ell$) is finite and meets all connected components of $V^M \cap \mathfrak{R}^t$. Because V satisfies the aforementioned regularity assumptions, $\mathrm{crit}(\pi_i, V^M) \cap \pi_{i-1}^{-1}(0)$ is defined as the projection on the $\boldsymbol{y}$-space of the solution set to the polynomials

$$\boldsymbol{h}^M, \quad (\lambda_1, \ldots, \lambda_\ell).jac(\boldsymbol{h}^M, i), \quad u_1\lambda_1 + \cdots + u_\ell\lambda_\ell = 1, \quad y_1 = \cdots = y_{i-1} = 0,$$

where $\boldsymbol{h} = (h_1, \ldots, h_\ell)$, $\lambda_1, \ldots, \lambda_\ell$ are new variables (called Lagrange multipliers), $jac(\boldsymbol{h}^M, i)$ is the Jacobian matrix associated to $\boldsymbol{h}^M$ truncated by forgetting its first first i columns and the u_i's are generically chosen (see also [42, App. B]).

Assume that D is the maximum degree of the h_j's and let E be the length of a straight-line program evaluating $\boldsymbol{h}$. Observe now that, setting the y_j's to 0 (for $1 \leq j \leq i-1$), and using [43, Theorem 1] combined with the degree estimates in [43, Section 5], we obtain that such systems can be solved using

$$O\left(\left(\binom{t-i}{\ell} D^\ell (D-1)^{t-(i-1)-\ell}\right)^2 (E + (t+\ell)D + (t+\ell)^2)(t+\ell)\right)$$

arithmetic operations in $\mathfrak{Q}$ and have at most

$$\binom{t-i}{\ell} D^\ell (D-1)^{t-(i-1)-\ell}$$

solutions.

Going back to our initial problem, one then needs to solve polynomial systems which encode the set $\mathsf{crit}(\pi_i, V^{\mathcal{I},\sigma}_{\boldsymbol{a},\varepsilon})$ of critical points of the restriction of π_i to $V^{\mathcal{I},\sigma}_{\boldsymbol{a},\varepsilon}$. Note that these systems have coefficients in $\mathbb{Q}[\varepsilon]$. To solve such systems, we rely on [44], which consists in specializing ε to a generic value $v \in \mathbb{Q}$ and compute a zero-dimensional parametrization of the solution set to the obtained system (within the above arithmetic complexity over $\mathbb{Q}$) and next use Hensel lifting and rational reconstruction to deduce from this parametrization a zero-dimensional parametrization with coefficients in $\mathbb{Q}(\varepsilon)$. By [44, Corollary 1] and multi-homogeneous bounds on the degree of the critical points of π_i to $\mathfrak{V}^{\mathcal{I},\sigma}_{\boldsymbol{a},\varepsilon}$ as in [43, Section 5], this lifting step has a cost

$$O^{\sim}\left(((t+\ell)^4 + (t+\ell+1)E)\left(\binom{t-i}{\ell} D^\ell (D-1)^{t-(i-1)-\ell}\right)^2\right).$$

Hence, all in all computing one zero-dimensional parametrization for one critical locus uses

$$O^{\sim}\left(((t+\ell)^4 D + (t+\ell+1)E)\left(\binom{t-i}{\ell} D^\ell (D-1)^{t-(i-1)-\ell}\right)^2\right)$$

arithmetic operations in $\mathbb{Q}$. Note that, following [44], the degrees in ε of the numerators and denominators of the coefficients of these parametrizations are bounded by $\binom{t}{\ell}D^{\ell}(D-1)^{t-\ell}$.

Summing up for all critical loci and using

$$\sum_{i=0}^{t-\ell}\binom{t-i}{\ell}=\binom{t+1}{\ell+1},$$

the computation for a fixed $V_{\boldsymbol{a},\varepsilon}^{\mathcal{I},\sigma}$ uses

$$O^{\sim}\left(((t+\ell)^4 D+(t+\ell+1)E)\binom{t+1}{\ell+1}^2\left(D^{\ell}(D-1)^{t-\ell}\right)^2\right)$$

arithmetic operations in $\mathbb{Q}$. Also, the number of points computed this way is dominated by

$$\binom{t+1}{\ell+1}\left(D^{\ell}(D-1)^{t-\ell}\right).$$

Note that the above quantity is upper bounded by $(2D)^t$ and bounds the degree of the output zero-dimensional parametrizations.

Taking the sum for all possible algebraic sets $V_{\boldsymbol{a},\varepsilon}^{\mathcal{I},\sigma}$ and remarking that

- the sum of number of indices of cardinality ℓ for $0\leq\ell\leq t$ is bounded by s^t;
- the number of sets σ for a given ℓ is bounded by 2^t;
- the sum $\sum_{\ell=0}^{t}\binom{t+1}{\ell+1}^2$ equals $2\binom{2t+1}{t}-1$

one deduces that all these zero-dimensional parametrizations can be computed within

$$O^{\sim}\left(s^t 2^t\binom{2t+1}{t}\left((2t)^4 D+(2t+1)\Gamma\right)\ D^{2t}\right)$$

arithmetic operations in $\mathbb{Q}$ (recall that Γ bounds the length of a straight line program evaluating all the polynomials defining our semi-algebraic set $\mathcal{S}$) which we simplify to

$$O^{\sim}\left(\Gamma\ s^t\ 2^{3t}\ D^{2t+1}\right).$$

Similarly, using the above simplifications, the total number of points encoded by these zero-dimensional parametrizations is bounded above by $(2sD)^t$.

At this stage, we have just obtained zero-dimensional parametrizations with coefficients in $\mathbb{Q}(\varepsilon)$.

The above bound on the number of returned points is done but it remains to show how to specialize ε in order to get sample points per connected components in $\mathcal{S}$. To do that, given a parametrization $\mathscr{R}_\varepsilon=(w,v_1,\ldots,v_t)\subset\mathbb{Q}(\varepsilon)[u]^{t+1}$, we need to find a specialization value e for ε to obtain a parametrization $\mathscr{R}_e$ such that

- the number of real roots of the zero set associated to $\mathscr{R}_e$ is the same as the number of real roots of the zero set associated to $\mathscr{R}_\varepsilon$;

- when η ranges over the interval $]0, e]$ the signs of the g_i's at the zero set associated to η does not vary.

To do that, it suffices to choose e such that it is smaller than the smallest positive root of the resultant associated to $\left(w, \frac{\partial w}{\partial u}\right)$ and the smallest positive roots of the resultant associated to w and $g_i\left(\frac{v_1}{\partial w/\partial u}, \ldots, \frac{v_t}{\partial w/\partial u}\right)$. The algebraic cost (i.e. the resultant computations) are dominated by the complexity estimates of the previous step.

Finally, note that Γ can be bounded by $s\binom{D+t}{t}$ when the g_i's are given in an expanded form in the monomial basis. Therefore, the arithmetic complexity for computing sample points of the semi-algebraic set defined by $g_1 \neq 0, \ldots, g_s \neq 0$ can be bounded by

$$O^{\sim}\left(\binom{D+t}{t} s^{t+1}\ 2^{3t}\ D^{2t+1}\right).$$

$\square$

Remark 2. Observe that since the coefficients of the rational parametrizations with coefficients in $\mathbb{Q}[\varepsilon]$ have bit size depending both on the maximum bit size τ of the coefficients of the input polynomials $g_1, \ldots, g_s$ and the bit size of the generically chosen a_i's.

When substituting ε by a small enough rational number e, one obtains zero-dimensional parametrizations with coefficients in $\mathbb{Q}$ of bit size depending on the one of e also. Admissible values for e depend on the magnitude of the real roots of the univariate resultant we exhibit in the above proof. Because we start with rational parametrizations of degree bounded by $O(D)^t$, assuming that the bit size of the a_i's is bounded by $O(D)^t$ (following reasonings like the one in [15]), one could show using standard quantitative results that the bit size of e may be $\tau\ D^{O(t)}$ (because e is obtained through the isolation of real roots of a univariate polynomial of degree $D^{O(t)}$). However, this is a worst case analysis and most of the time, we observe in practice that one can choose for e values of reasonable bit size.

We end this section with a Corollary which is a consequence of the proof of [4, Theorem 13.18]. Basically, once we have the parametrizations computed by the algorithm on which Theorem II relies, one can compute sample points per connected components of the semi-algebraic set $\mathcal{S}$ within the same arithmetic complexity bounds. The idea is just to evaluate the g_i's at these rational parametrizations and use bounds on the minimal distance between two roots of a univariate polynomial such as [4, Prop. 10.22]. Hence, the proof of the corollary below follows mutatis mutandis the same steps as the one of [4, Theorem 13.18].

Corollary 3. Let $(g_1, \ldots, g_s)$ in $\mathbb{Q}[y_1, \ldots, y_t]$ with $D \geq \max_{1\leq i\leq s} \deg(g_i)$ and $\mathcal{S} \subset \mathbb{R}^t$ be the semi-algebraic set defined by

$$g_1 \neq 0, \ldots, g_s \neq 0.$$

There exists a probabilistic algorithm which on input $(g_1, \ldots, g_s)$ outputs a finite set of points $\mathscr{P}$ in $\mathbb{Q}^t$ of cardinality at most $(2sD)^t$ points such that $\mathscr{P}$ meets every connected component of $\mathcal{S}$ using

$$O^{\sim}\left(\binom{D+t}{t} s^{t+1} 2^{3t} D^{2t+1}\right).$$

arithmetic operations in $\mathbb{Q}$.

Note that the main difference, by contrast with Theorem II, the above Corollary shows how to obtain output points with coordinates in $\mathbb{Q}$.

4. Parametric Hermite matrices

In this section, we adapt the construction encoding Hermite's quadratic forms, also known as Hermite matrices to the context of parametric systems and describe an algorithm for computing those parametric Hermite matrices.

4.1. Definition

Let $\mathbb{K}$ be a field and $I \subset \mathbb{K}[\boldsymbol{x}]$ be a zero-dimensional ideal. Recall that the quotient ring $A_{\mathbb{K}} = \mathbb{K}[\boldsymbol{x}]/I$ is a $\mathbb{K}$-vector space of finite dimension [12, Section 5.3, Theorem 6]. For $p \in \mathbb{K}[\boldsymbol{x}]$, we denote by $\mathcal{L}_p$ the multiplication map $\overline{q} \in A_{\mathbb{K}} \mapsto \overline{p \cdot q}, \in A_{\mathbb{K}}$.

Note that the map $\mathcal{L}_p$ is an endomorphism of $A_{\mathbb{K}}$ as a $\mathbb{K}$-vector space. The Hermite quadratic form associated to I is defined as the bilinear form that sends $(\overline{p}, \overline{q}) \in A_{\mathbb{K}} \times A_{\mathbb{K}}$ to the trace of $\mathcal{L}_{p \cdot q}$ as an endomorphism of $A_{\mathbb{K}}$.

We refer to [4, Chap. 4] for more details about Hermite quadratic forms.

Now, let $\boldsymbol{f} = (f_1, \ldots, f_m)$ be a polynomial sequence in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$. We take the rational function field $\mathbb{Q}(\boldsymbol{y})$ as the base field $\mathbb{K}$ and denote by $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ the ideal generated by $\boldsymbol{f}$ in $\mathbb{K}[\boldsymbol{x}]$. We require that the system $\boldsymbol{f}$ satisfies Assumption (A).

This leads to the following well-known lemma, which is the foundation for the construction of our parametric Hermite matrices.

Lemma 4. Assume that $\boldsymbol{f}$ satisfies Assumption (A). Then the ideal $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ is zero-dimensional.

Proof. Assume that there exists a coordinate x_i for $1 \le i \le n$ such that $\langle \boldsymbol{f} \rangle \cap \mathbb{C}[\boldsymbol{y}, x_i] = \langle 0 \rangle$. We denote respectively by π_i and $\tilde{\pi}_i$ the projections $(\boldsymbol{y}, \boldsymbol{x}) \mapsto (\boldsymbol{y}, x_i)$ and $(\boldsymbol{y}, x_i) \mapsto \boldsymbol{y}$. By the assumption above, $\overline{\pi_i(\mathcal{V})}$ is the whole space $\mathbb{C}^{t+1}$. Then, we have the identity

$$\mathbb{C}^{t+1} = \overline{\left(\tilde{\pi}_i{}^{-1}(O) \cup \tilde{\pi}_i{}^{-1}(\mathbb{C}^t \setminus O)\right) \cap \pi_i(\mathcal{V})},$$

where O be the dense Zariski open subset of $\mathbb{C}^t$ required in Assumption (A).

Since $\tilde{\pi}_i$ is a map from $\mathbb{C}^{t+1}$ to $\mathbb{C}^t$, its fibers are of dimension at most 1. Therefore, we have that $\dim \tilde{\pi}_i{}^{-1}(\mathbb{C}^t \setminus O) \le 1 + \dim(\mathbb{C}^t \setminus O) \le t$. As Assumption (A) holds and $\dim \tilde{\pi}_i^{-1}(\mathbb{C}^t \setminus O) \le t$, we have that $\dim \overline{\tilde{\pi}_i{}^{-1}(O) \cap \pi_i(\mathcal{V})} = t$. This contradicts to the identity above. We conclude that, for $1 \le i \le n$, $\langle \boldsymbol{f} \rangle \cap \mathbb{C}[\boldsymbol{y}, x_i] \neq \langle 0 \rangle$.

On the other hand, by Assumption (A), the Zariski-closure of $\pi(\mathcal{V})$ is the whole parameter space $\mathbb{C}^t$. Thus, we have that $\langle \boldsymbol{f} \rangle \cap \mathbb{C}[\boldsymbol{y}] = \langle 0 \rangle$. Since $\langle \boldsymbol{f} \rangle \cap \mathbb{C}[\boldsymbol{y}] = (\langle \boldsymbol{f} \rangle \cap \mathbb{C}[\boldsymbol{y}, x_i]) \cap \mathbb{C}[\boldsymbol{y}]$ for every $1 \le i \le n$, there exists a polynomial $p_i \in \langle \boldsymbol{f} \rangle \cap \mathbb{C}[\boldsymbol{y}, x_i]$ whose degree with respect to x_i is non-zero. Clearly, p_i is an element of the ideal $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$. Thus, there exists d_i such that $x_i^{d_i}$ is a leading term in $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$. Hence, $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ is a zero-dimensional ideal. ☐

Lemma 4 allows us to apply the construction of Hermite matrices described in [4, Chap. 4] to parametric systems as follows.

Since the ideal $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ is zero-dimensional by Lemma 4, its associated quotient ring $A_{\mathbb{K}} = \mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ is a finite dimensional $\mathbb{K}$-vector space. Let δ denote the dimension of $A_{\mathbb{K}}$ as a $\mathbb{K}$-vector space.

We consider a basis $B = \{b_1, \ldots, b_\delta\}$ of $A_{\mathbb{K}}$, where the b_i's are taken as monomials in the variables $\boldsymbol{x}$. Such a basis can be derived from Gröbner bases as follows. We fix an admissible monomial ordering $\succ$ over the set of monomials in the variables $\boldsymbol{x}$ and compute a Gröbner basis G with respect to the ordering $\succ$ of the ideal $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$. Then, the monomials that are not divisible by any leading monomial of elements of G form a basis of $A_{\mathbb{K}}$.

Recall that, for an element $p \in \mathbb{K}[\boldsymbol{x}]$, we denote by $\overline{p}$ the class of p in the quotient ring $A_{\mathbb{K}}$. A representative of $\overline{p}$ can be derived by computing the normal form of p by the Gröbner basis G, which results in a linear combination of elements of B with coefficients in $\mathbb{Q}(\boldsymbol{y})$.

Assume now the basis B of $A_{\mathbb{K}}$ is fixed. For any $p \in \mathbb{K}[\boldsymbol{x}]$, the multiplication map $\mathcal{L}_p$ is an endomorphism of $A_{\mathbb{K}}$. Therefore, it admits a matrix representation with respect to B, whose entries are elements in $\mathbb{Q}(\boldsymbol{y})$. The trace of $\mathcal{L}_p$ can be computed as the trace of the matrix representing it. Similarly, the Hermite's quadratic form of the ideal $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ can be represented by a matrix with respect to B. This leads to the following definition.

Definition 5. Given a parametric polynomial system $\boldsymbol{f} = (f_1, \ldots, f_m) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ satisfying Assumption (A). We fix a basis $B = \{b_1, \ldots, b_\delta\}$ of the vector space $\mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$. The parametric Hermite matrix associated to $\boldsymbol{f}$ with respect to the basis B is defined as the symmetric matrix $H = (h_{i,j})_{1 \le i,j \le \delta}$ where $h_{i,j} = \mathsf{trace}(\mathcal{L}_{b_i \cdot b_j})$.

It is important to note that the definition of parametric Hermite matrices depends both on the input system $\boldsymbol{f}$ and the choice of the monomial basis B.

4.2. Gröbner bases and parametric Hermite matrices

In the previous subsection, we have defined parametric Hermite matrices assuming one knows a Gröbner basis G with respect to some monomial ordering of the ideal $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ where $\mathbb{K} = \mathbb{Q}(\boldsymbol{y})$ and $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ is the ideal of $\mathbb{K}[\boldsymbol{x}]$ generated by $\boldsymbol{f}$.

Computing such a Gröbner basis may be costly as this would require to perform arithmetic operations over the field $\mathbb{Q}(\boldsymbol{y})$ (or $\mathbb{Z}/p\mathbb{Z}(\boldsymbol{y})$ where p is a prime when tackling this computational task through modular computations). In this paragraph, we show that one can obtain parametric Hermite matrices by considering some Gröbner bases of the ideal $\langle \boldsymbol{f} \rangle \subset \mathbb{Q}[\boldsymbol{y}, \boldsymbol{x}]$ (hence, enabling the use of efficient implementations of Gröbner bases such as the F_4/F_5 algorithms [17, 18]).

Since the graded reverse lexicographical ordering (grevlex for short) is known for yielding Gröbner bases of relatively small degree comparing to other orders, we prefer using this ordering to construct our parametric Hermite matrices. Further, we will use the notation $\mathsf{grevlex}(\boldsymbol{x})$ for the grevlex ordering among the variables $\boldsymbol{x}$ (with $x_1 \succ \cdots \succ x_n$) and $\mathsf{grevlex}(\boldsymbol{x}) \succ \mathsf{grevlex}(\boldsymbol{y})$ (with $y_1 \succ \cdots \succ y_t$) for the elimination ordering. We denote respectively by $\mathsf{lm}_{\boldsymbol{x}}(p)$ and $\mathsf{lc}_{\boldsymbol{x}}(p)$ the leading monomial and the leading coefficient of $p \in \mathbb{K}[\boldsymbol{x}]$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x})$.

Lemma 6. Let $\mathcal{G}$ be the reduced Gröbner basis of $\langle \boldsymbol{f} \rangle$ with respect to the elimination ordering $\mathsf{grevlex}(\boldsymbol{x}) \succ \mathsf{grevlex}(\boldsymbol{y})$. Then $\mathcal{G}$ is also a Gröbner basis of $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x})$.

Proof. Since $\mathcal{G}$ is a Gröbner basis of the ideal $\langle \boldsymbol{f} \rangle$, every polynomial f_i of $\boldsymbol{f}$ can be written as $f_i = \sum_{g \in \mathcal{G}} c_g \cdot g$ where $c_g \in \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$. Therefore, any element of $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ can also be written as a combination of elements of $\mathcal{G}$ with coefficients in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$. In other words, $\mathcal{G}$ is a set of generators of $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$.

Let p be a polynomial in $\mathbb{K}[\boldsymbol{x}]$, p is contained in $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ if and only if there exists a polynomial $q \in \mathbb{Q}[\boldsymbol{y}]$ such that $q \cdot p \in \langle \boldsymbol{f} \rangle$. Thus, the leading monomial of p as an element of $\mathbb{K}[\boldsymbol{x}]$ with respect to the grevlex ordering $\mathsf{grevlex}(\boldsymbol{x})$ is contained in the ideal $\langle \mathrm{lm}_{\boldsymbol{x}}(g) \mid g \in \mathcal{G} \rangle$. Therefore, $\mathcal{G}$ is a Gröbner basis of $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$. □

Hereafter, we denote by $\mathcal{G}$ the reduced Gröbner basis of $\langle \boldsymbol{f} \rangle$ with respect to the elimination ordering $\mathsf{grevlex}(\boldsymbol{x}) \succ \mathsf{grevlex}(\boldsymbol{y})$. Let $\mathcal{B}$ be the set of all monomials in $\boldsymbol{x}$ that are not reducible by $\mathcal{G}$, which is finite by Lemmas 4 and 6. The set $\mathcal{B}$ actually forms a basis of the $\mathbb{K}$-vector space $\mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$. Then, we denote by $\mathcal{H}$ the parametric Hermite matrix associated to $\boldsymbol{f}$ with respect to this basis $\mathcal{B}$.

We consider the following assumption on the input system $\boldsymbol{f}$.

Assumption B. For $g \in \mathcal{G}$, the leading coefficient $\mathrm{lc}_{\boldsymbol{x}}(g)$ does not depend on the parameters $\boldsymbol{y}$.

As the computations in the quotient ring $A_{\mathbb{K}}$ are done through normal form reductions by $\mathcal{G}$, the lemma below is straight-forward.

Lemma 7. Under Assumption (B), the entries of the parametric Hermite matrix $\mathcal{H}$ are elements of $\mathbb{Q}[\boldsymbol{y}]$.

Proof. Since Assumption (B) holds, the leading coefficients $\mathrm{lc}_{\boldsymbol{x}}(g)$ do not depend on parameters $\boldsymbol{y}$ for $g \in \mathcal{G}$. The normal form reduction in $A_{\mathbb{K}}$ of any polynomial in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ returns a polynomial in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$. Thus, each normal form can be written as a linear combination of $\mathcal{B}$ whose coefficients lie in $\mathbb{Q}[\boldsymbol{y}]$. Hence, the multiplication map $\mathcal{L}_{b_i \cdot b_j}$ for $1 \leq i, j \leq \delta$ can be represented by polynomial matrices in $\mathbb{Q}[\boldsymbol{y}]$ with respect to the basis $\mathcal{B}$. As an immediate consequence, the entries of $\mathcal{H}$, as being the traces of those multiplication maps, are polynomials in $\mathbb{Q}[\boldsymbol{y}]$. □

The next proposition states that Assumption (B) is satisfied by a generic system $\boldsymbol{f}$. It implies that the entries of the parametric Hermite matrix of a generic system with respect to the basis $\mathcal{B}$ derived from $\mathcal{G}$ completely lie in $\mathbb{Q}[\boldsymbol{y}]$. We postpone the proof of Proposition 8 to Subsection 6.1 where we prove a more general result (see Proposition 20).

Proposition 8. Let $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_d$ be the set of polynomials in $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]$ having total degree bounded by d. There exists a non-empty Zariski open subset $\mathscr{F}_C$ of $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_d^n$ such that Assumption (B) is satisfied by any $\boldsymbol{f} \in \mathscr{F}_C \cap \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]^n$.

4.3. Specialization property of parametric Hermite matrices

Recall that $\mathcal{G}$ is the reduced Gröbner basis of $\langle \boldsymbol{f} \rangle$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x}) \succ \mathsf{grevlex}(\boldsymbol{y})$ and $\mathcal{B}$ is the basis of $\mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ derived from $\mathcal{G}$ as discussed in the previous subsection. Then, $\mathcal{H}$ is the parametric Hermite matrix associated to $\boldsymbol{f}$ with respect to the basis $\mathcal{B}$.

Let $\eta \in \mathbb{C}^t$ and $\phi_\eta : \mathbb{C}(\boldsymbol{y})[\boldsymbol{x}] \to \mathbb{C}[\boldsymbol{x}]$, $p(\boldsymbol{y}, \boldsymbol{x}) \mapsto p(\eta, \boldsymbol{x})$ be the specialization map that evaluates the parameters $\boldsymbol{y}$ at η. Then $\boldsymbol{f}(\eta, \cdot) = (\phi_\eta(f_1), \dots, \phi_\eta(f_m))$. We denote by $\mathcal{H}(\eta)$ the specialization $(\phi_\eta(h_{i,j}))_{1 \leq i,j \leq \delta}$ of $\mathcal{H}$ at η.

Recall that, for a polynomial $p \in \mathbb{C}(\boldsymbol{y})[\boldsymbol{x}]$, the leading coefficient of p considered as a polynomial in the variables $\boldsymbol{x}$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x})$ is denoted by $\mathsf{lc}_{\boldsymbol{x}}(p)$. In this subsection, for $p \in \mathbb{C}[\boldsymbol{x}]$, we use $\mathsf{lm}(p)$ to denote the leading monomial of p with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x})$.

Let $\mathcal{W}_\infty \subset \mathbb{C}^t$ denote the algebraic set $\cup_{g\in\mathcal{G}} V(\mathsf{lc}_{\boldsymbol{x}}(g))$. In Proposition 10, we prove that, outside $\mathcal{W}_\infty$, the specialization $\mathcal{H}(\eta)$ coincides with the classic Hermite matrix of the zero-dimensional ideal $\boldsymbol{f}(\eta,\cdot) \subset \mathbb{Q}[\boldsymbol{x}]$. This is the main result of this subsection.

Since the operations over the $\mathbb{K}$-vector space $A_{\mathbb{K}}$ rely on normal form reductions by the Gröbner basis $\mathcal{G}$ of $\langle \boldsymbol{f}\rangle_{\mathbb{K}}$, the specialization property of $\mathcal{H}$ depends on the specialization property of $\mathcal{G}$. Lemma 9 below, which is a direct consequence of [32, Theorem 3.1], provides the specialization property of $\mathcal{G}$. We give here a more elementary proof for this lemma than the one in [32].

Lemma 9. Let $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$. Then the specialization $\mathcal{G}(\eta,\cdot) := \{\phi_\eta(g) \mid g \in \mathcal{G}\}$ is a Gröbner basis of the ideal $\langle \boldsymbol{f}(\eta,\cdot)\rangle \subset \mathbb{C}[\boldsymbol{x}]$ generated by $\boldsymbol{f}(\eta,\cdot)$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x})$.

Proof. Since $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$, the leading coefficient $\mathsf{lc}_{\boldsymbol{x}}(g)$ does not vanish at η for every $g \in \mathcal{G}$. Thus, $\mathsf{lm}_{\boldsymbol{x}}(g) = \mathsf{lm}(\phi_\eta(g))$.

We denote by $\mathcal{M}$ the set of all monomials in the variables $\boldsymbol{x}$ and

$$\mathcal{M}_{\mathcal{G}} := \{m \in \mathcal{M} \mid \exists g \in \mathcal{G} \;:\; \mathsf{lm}_{\boldsymbol{x}}(g) \text{ divides } m\} = \{m \in \mathcal{M} \mid \exists g \in \mathcal{G} \;:\; \mathsf{lm}(\phi_\eta(g)) \text{ divides } m\}.$$

For any $p \in \langle \boldsymbol{f}\rangle \subset \mathbb{Q}[\boldsymbol{x},\boldsymbol{y}]$, we prove that $\mathsf{lm}(\phi_\eta(f)) \in \mathcal{M}_G$. If p is identically zero, there is nothing to prove. So, we assume that $p \neq 0$, p is then expanded in the form below:

$$p = \sum_{m\in\mathcal{M}_{\mathcal{G}}} c_m \cdot m + \sum_{m\in\mathcal{M}\setminus\mathcal{M}_{\mathcal{G}}} c_m \cdot m,$$

where the c_m's are elements of $\mathbb{Q}[\boldsymbol{y}]$. Since p is not identically zero, there exists $m \in \mathcal{M}_{\mathcal{G}}$ such that $c_m \neq 0$.

Since $\mathcal{G}$ is a Gröbner basis of $\langle \boldsymbol{f}\rangle_{\mathbb{K}}$, any monomial in $\mathcal{M}_{\mathcal{G}}$ can be reduced by $\mathcal{G}$ to a unique normal form in $\mathbb{K}[\boldsymbol{x}]$. These divisions involve denominators, which are products of some powers of the leading coefficients of $\mathcal{G}$ with respect to the variables $\boldsymbol{x}$. We write

$$\mathrm{NF}_{\mathcal{G}}(p) = \sum_{m\in\mathcal{M}_{\mathcal{G}}} c_m \cdot \mathrm{NF}_{\mathcal{G}}(m) + \sum_{m\in\mathcal{M}\setminus\mathcal{M}_{\mathcal{G}}} c_m \cdot m.$$

As $p \in \langle \boldsymbol{f}\rangle_{\mathbb{K}}$, we have that $\mathrm{NF}_{\mathcal{G}}(p) = 0$, which implies

$$\sum_{m\in\mathcal{M}\setminus\mathcal{M}_{\mathcal{G}}} c_m \cdot m = -\sum_{m\in\mathcal{M}_{\mathcal{G}}} c_m \cdot \mathrm{NF}_{\mathcal{G}}(m).$$

Therefore, we have the identity

$$p = \sum_{m\in\mathcal{M}_{\mathcal{G}}} c_m \cdot (m - \mathrm{NF}_{\mathcal{G}}(m))$$

Since η does not cancel any denominator appearing in $\mathrm{NF}_{\mathcal{G}}(m)$, we can specialize the identity above without any problem:

$$\phi_\eta(p) = \sum_{m\in\mathcal{M}_{\mathcal{G}}} \phi_\eta(c_m) \cdot (m - \phi_\eta(\mathrm{NF}_{\mathcal{G}}(m))).$$

If at least one of the $\phi_\eta(c_m)$ does not vanish, then the leading monomial of $\phi_\eta(f)$ is in $\mathcal{M}_\mathcal{G}$. Otherwise, if all the $\phi_\eta(c_m)$ are canceled, then $\phi_\eta(p)$ is identically zero, and there is not any new leading monomial appearing either. So, the leading monomial of any $p \in \langle \boldsymbol{f}_\eta \rangle$ is contained in $\mathcal{M}_\mathcal{G}$, which means $\mathcal{G}(\eta, \cdot)$ is a Gröbner basis of $\langle \boldsymbol{f}(\eta, \cdot) \rangle$ with respect to $\mathsf{grevlex}(\boldsymbol{x})$. $\square$

Proposition 10. For any $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$, the specialization $\mathcal{H}(\eta)$ coincides with the classic Hermite matrix of the zero-dimensional ideal $\langle \boldsymbol{f}(\eta, \cdot) \rangle \subset \mathbb{C}[\boldsymbol{x}]$.

Proof. As a consequence of Lemma 9, each computation in $A_\mathbb{K}$ derives a corresponding one in $\mathbb{C}[\boldsymbol{x}]/\langle \boldsymbol{f}(\eta, \cdot) \rangle$ by evaluating $\boldsymbol{y}$ at η in every normal form reduction by $\mathcal{G}$. This evaluation is allowed since η does not cancel any denominator appearing during the computation. Therefore, we deduce immediately the specialization property of the Hermite matrix. $\square$

Using Proposition 10 and [4, Theorem 4.102], we obtain immediately the following corollary that allows us to use parametric Hermite matrices to count the root of a specialization of a parametric system.

Corollary 11. Let $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$, then the rank of $H(\eta)$ is the number of distinct complex roots of $\boldsymbol{f}(\eta, \cdot)$. When $\eta \in \mathbb{R}^t \setminus \mathcal{W}_\infty$, the signature of $H(\eta)$ is the number of distinct real roots of $\boldsymbol{f}(\eta, \cdot)$.

Proof. By Proposition 10, $\mathcal{H}(\eta)$ is a Hermite matrix of the zero-dimensional ideal $\langle \boldsymbol{f}(\eta, \cdot) \rangle$. Then, [4, Theorem 4.102] implies that the rank (resp. the signature) of $\mathcal{H}(\eta)$ equals to the number of distinct complex (resp. real) solutions of $\boldsymbol{f}(\eta, \cdot)$. $\square$

We finish this subsection by giving some explanation for what happens above $\mathcal{W}_\infty$, where our parametric Hermite matrix $\mathcal{H}$ does not have good specialization property.

Lemma 12. Let $\mathcal{W}_\infty$ defined as above. Then $\mathcal{W}_\infty$ contains all the following sets:

- The non-proper points of the restriction of π to $\mathcal{V}$ (see Section 2 for this definition).
- The set of points $\eta \in \mathbb{C}^t$ such that the fiber $\pi^{-1}(\eta) \cap \mathcal{V}$ is infinite.
- The image by π of the irreducible components of $\mathcal{V}$ whose dimensions are smaller than t.

Proof. The claim for the set of non-properness of the restriction of π to $\mathcal{V}$ is already proven in [35, Theorem 2]. We focus on the two remaining sets.

Using the Hermite matrix, we know that for $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$, the system $\boldsymbol{f}(\eta, \cdot)$ admits a non-empty finite set of complex solutions. On the other hand, for any $\eta \in \mathbb{C}^t$ such that $\pi^{-1}(\eta) \cap \mathcal{V}$ is infinite, $\boldsymbol{f}(\eta, \cdot)$ has infinitely many complex solutions. Therefore, the set of such points η is contained in $\mathcal{W}_\infty$.

Let $\mathcal{V}_{>t}$ be the union of irreducible components of $\mathcal{V}$ of dimension greater than t. By the fiber dimension theorem [45, Theorem 1.25], the fibers of the restriction of π to $\mathcal{V}_{>t}$ must have dimension at least one. Similarly, the components of dimension t whose images by π are contained in a Zariski closed subset of $\mathbb{C}^t$ also yield infinite fibers. Therefore, as proven above, all of these components are contained in $\pi^{-1}(\mathcal{W}_\infty)$.

We now consider the irreducible components of dimension smaller than t. Let $\mathcal{V}_{\geq t}$ and $\mathcal{V}_{<t}$ be respectively the union of irreducible components of $\mathcal{V}$ of dimension at least t and at most $t-1$. We have that $\mathcal{V} = \mathcal{V}_{\geq t} \cup \mathcal{V}_{<t}$. Let $I \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ denote the ideal generated by $\boldsymbol{f}$. Using the primary decomposition of I (see e.g. [12, Sec. 4.8]), we have that I is the intersection of two ideals $I_{\geq t}$ and $I_{<t}$ such that $V(I_{\geq t}) = \mathcal{V}_{\geq t}$ and $V(I_{<t}) = \mathcal{V}_{<t}$. We write

$$I = I_{\geq t} \cap I_{<t}.$$

We denote by R the polynomial ring $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$. Then, the above identity is transferred into R:

$$I \cdot R = (I_{\geq t} \cdot R) \cap (I_{<t} \cdot R).$$

Since $\mathsf{dim}(\overline{\pi(\mathcal{V}_{<t})}) \leq t-1$, then there exists a non-zero polynomial $p \in I_{<t} \cap \mathbb{Q}[\boldsymbol{y}]$. As p is a unit in $\mathbb{Q}(\boldsymbol{y})$, the ideal $I_{<t} \cdot R$ is exactly R. So,

$$I \cdot R = I_{\geq t} \cdot R.$$

Note that, by Lemma 6, $\mathcal{G}$ is a Gröbner basis of $I \cdot R$, then it is also a Gröbner basis of $I_{\geq t} \cdot R$. Therefore, the Hermite matrices associated to I and $I_{\geq t}$ (with respect to the basis derived from $\mathcal{G}$) coincide. So, for $\eta \notin \mathcal{W}_\infty$, the ranks of those matrices are equal and so are the numbers of complex points in $\pi^{-1}(\eta) \cap \mathcal{V}$ and $\pi^{-1}(\eta) \cap \mathcal{V}_{\geq t}$. As $\pi^{-1}(\eta) \cap \mathcal{V}_{\geq t} \subset \pi^{-1}(\eta) \cap \mathcal{V}$, we have that $\pi^{-1}(\eta) \cap \mathcal{V} = \pi^{-1}(\eta) \cap \mathcal{V}_{\geq t}$. This leads to

$$\pi^{-1}(\mathbb{C}^t \setminus \mathcal{W}_\infty) \cap \mathcal{V}_{\geq t} = \pi^{-1}(\mathbb{C}^t \setminus \mathcal{W}_\infty) \cap \mathcal{V}.$$

Then, $\pi^{-1}(\mathbb{C}^t \setminus \mathcal{W}_\infty) \cap \mathcal{V}_{<t} = \emptyset$ or equivalently, $\mathcal{V}_{<t} \subset \pi^{-1}(\mathcal{W}_\infty)$, which concludes the proof. □

4.4. Computing parametric Hermite matrices

Given $\boldsymbol{f} = (f_1, \ldots, f_m) \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ satisfying Assumption (A). We keep denoting $\mathbb{K} = \mathbb{Q}(\boldsymbol{y})$. Let $\mathcal{G}$ be the reduced Gröbner basis of $\langle \boldsymbol{f} \rangle$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x}) \succ \mathsf{grevlex}(\boldsymbol{y})$ and $\mathcal{B}$ be the set of all monomials in the variables $\boldsymbol{x}$ which are not reducible by $\mathcal{G}$. The set $\mathcal{B}$ then forms a basis of the $\mathbb{K}$-vector space $\mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$.

In this subsection, we focus on the computation of the parametric Hermite matrix associated to $\boldsymbol{f}$ with respect to the basis $\mathcal{B}$.

Note that one can design an algorithm using only the definition of parametric Hermite matrices given in Subsection 4.1. More precisely, for each $b_i \cdot b_j \in \mathcal{B}$ $(1 \leq i, j \leq \delta)$, one computes the matrix representing $\mathcal{L}_{b_i \cdot b_j}$ in the basis $\mathcal{B}$ by computing the normal form of every $b_i \cdot b_j \cdot b_k$ for $1 \leq k \leq \delta$. Therefore, in total, this direct algorithm requires $O(\delta^3)$ normal form reductions of polynomials in $\mathbb{K}[\boldsymbol{x}]$.

In Algorithm 1 below, we present another algorithm for computing $\mathcal{H}$. We call to the following subroutines successively:

- GrobnerBasis that takes as input the system $\boldsymbol{f}$ and computes the reduced Gröbner basis $\mathcal{G}$ of $\langle \boldsymbol{f} \rangle$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x}) \succ \mathsf{grevlex}(\boldsymbol{y})$ and the basis $\mathcal{B} = \{b_1, \ldots, b_\delta\} \subset \mathbb{Q}[\boldsymbol{x}]$ derived from $\mathcal{G}$.

  Such an algorithm can be obtained using any general algorithm for computing Gröbner basis, which we refer to F4/F5 algorithms [17, 18].

- ReduceGB that takes as input the Gröbner basis $\mathcal{G}$ and outputs a subset $\mathcal{G}'$ of $\mathcal{G}$ which is still a Gröbner basis of $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x})$.

  This subroutine aims to remove the elements in $\mathcal{G}$ that we do not need. Even though $\mathcal{G}$ is reduced as a Gröbner basis of $\langle \boldsymbol{f} \rangle$ with respect to $\mathsf{grevlex}(\boldsymbol{x}) \succ \mathsf{grevlex}(\boldsymbol{y})$, it is not necessarily the reduced Gröbner basis of $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ with respect to $\mathsf{grevlex}(\boldsymbol{x})$. Using [12, Lemma 3, Sec. 2.7], we can design ReduceGB to remove all the elements of $\mathcal{G}$ which have duplicate leading monomials (in $\boldsymbol{x}$). We obtain as output a subset $\mathcal{G}'$ of $\mathcal{G}$ which is also a Gröbner basis $\mathcal{G}'$ for $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ with respect to $\mathsf{grevlex}(\boldsymbol{x})$. Note that this tweak reduces not only the cardinal of the Gröbner basis in use but also the size of the set $\mathcal{W}_\infty$ introduced in Subsection 4.3 (as we have less leading coefficients).

- XMatrices that takes as input $(\mathcal{G}', \mathcal{B})$ and computes the matrix representation of the multiplication maps $\mathcal{L}_{x_i}$ $(1 \le i \le n)$ with respect to $\mathcal{B}$.

  This computation is done directly by reducing every $x_i \cdot b_j$ $(1 \le i \le n,\ 1 \le j \le \delta)$ to its normal form in $\mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ using $\mathcal{G}'$.

- BMatrices that takes as input the matrices representing $(\mathcal{L}_{x_1}, \ldots, \mathcal{L}_{x_n})$ and $\mathcal{B}$ and computes the matrices representing the $\mathcal{L}_{b_i}$'s $(1 \le i \le \delta)$ in the basis $\mathcal{B}$.

  We design BMatrices in a way that it constructs the matrices of $\mathcal{L}_{b_i}$'s inductively in the degree of the b_i's as follows.

  At the beginning, we have the multiplication matrices of 1 and the x_i's; those are the matrices of the elements of degree zero and one. Note that, for any element b of $\mathcal{B}$. At the step of computing the matrix of an element $b \in \mathcal{B}$, we remark that there exist a variable x_i and a monomial $b' \in \mathcal{B}$ such that $b = x_i \cdot b'$ and the matrix of b' is already computed (as $\deg(b') < \deg(b)$. Therefore, we simply multiply the matrices of $\mathcal{L}_{x_i}$ and $\mathcal{L}_{b'}$ to obtain the matrix of $\mathcal{L}_b$.

- TraceComputing that takes as input the multiplication matrices $\mathcal{L}_{b_1}, \ldots, \mathcal{L}_{b_\delta}$ and computes the matrix $(\mathrm{trace}(\mathcal{L}_{b_i \cdot b_j}))_{1 \le i \le j \le \delta}$. This matrix is in fact the parametric Hermite matrix $\mathcal{H}$ associated to $\boldsymbol{f}$ with respect to the basis $\mathcal{B}$. To design this subroutine, we use the following remark given in [39].

  Let $p, q \in \mathbb{K}[\boldsymbol{x}]$. The normal form $\overline{p}$ of p by $\mathcal{G}$ can be written as $\overline{p} = \sum_{i=1}^{\delta} c_i \cdot b_i$ where the c_i's lie in $\mathbb{K}$. Then, we have the identity

  $$\mathrm{trace}(\mathcal{L}_{p \cdot q}) = \sum_{i=1}^{\delta} c_i \cdot \mathrm{trace}(\mathcal{L}_{q \cdot b_i}),$$

  Hence, by choosing $p = b_i \cdot b_j$ and $q = 1$, we can compute $h_{i,j}$ using the normal form $\overline{b_i \cdot b_j}$ and $\mathrm{trace}(\mathcal{L}_{b_1}), \ldots, \mathrm{trace}(\mathcal{L}_{b_\delta})$.

  Note that $\mathrm{trace}(\mathcal{L}_{b_i})$ is easily computed from the matrix of the map $\mathcal{L}_{b_i}$. On the other hand, the normal form $\overline{b_i \cdot b_j}$ can be read off from the j-th row of the matrix representing $\mathcal{L}_{b_i}$, which is already computed at this point.

  It is also important to notice that there are many duplicated entries in $\mathcal{H}$. Thus, we should avoid all the unnecessary re-computation. This is done easily be keeping a list for tracking distinct entries of $\mathcal{H}$.

The pseudo-code of Algorithm 1 is presented below. Its correctness follows simply from our definition of parametric Hermite matrices.

Beside the parametric Hermite matrix $\mathcal{H}$, we return a polynomial $\boldsymbol{w}_\infty$ which is the square-free part of $\mathsf{lcm}_{g \in \mathcal{G}}(\mathsf{lc}_{\boldsymbol{x}}(g))$ for further usage. Note that $V(\boldsymbol{w}_\infty) = \mathcal{W}_\infty$.

Algorithm 1: DRL-Matrix

Input: A parametric polynomial system $\boldsymbol{f} = (f_1, \ldots, f_m)$

Output: A parametric Hermite matrix $\mathcal{H}$ associated to $\boldsymbol{f}$ with respect to the basis $\mathcal{B}$

$\mathcal{G}, \mathcal{B} \leftarrow$ GröbnerBasis$(\boldsymbol{f}, \mathsf{grevlex}(\boldsymbol{x}) \succ \mathsf{grevlex}(\boldsymbol{y}))$

$\mathcal{G}' \leftarrow \mathsf{ReduceGB}(\mathcal{G})$

$\boldsymbol{w}_\infty \leftarrow \mathsf{sqfree}(\mathsf{lcm}_{g \in \mathcal{G}}(\mathsf{lc}_{\boldsymbol{x}}(g)))$

$(\mathcal{L}_{x_1}, \ldots, \mathcal{L}_{x_n}) \leftarrow \mathsf{XMatrices}(\mathcal{G}', \mathcal{B})$

$(\mathcal{L}_{b_1}, \ldots, \mathcal{L}_{b_\delta}) \leftarrow \mathsf{BMatrices}((\mathcal{L}_{x_1}, \ldots, \mathcal{L}_{x_n}), \mathcal{B})$

$\mathcal{H} \leftarrow \mathsf{TraceComputing}(\mathcal{L}_{b_1}, \ldots, \mathcal{L}_{b_\delta})$

return $[\mathcal{H}, \boldsymbol{w}_\infty]$

Removing denominators. Note that, through the computation in the quotient ring $A_{\mathbb{K}}$, the entries of our parametric Hermite matrix possibly contains denominators that lie in $\mathbb{Q}[\boldsymbol{y}]$. As the algorithm that we introduce in Section 5 will require us to manipulate the parametric Hermite matrix that we compute, these denominators can be a bottleneck to handle the matrix. Therefore, we introduce an extra subroutine RemoveDenominator that returns a parametric Hermite matrix $\mathcal{H}'$ of $\boldsymbol{f}$ without denominator.

- RemoveDenominator that takes as input the matrix $\mathcal{H}$ computed by DRL-Matrix and outputs a matrix $\mathcal{H}'$ which is the parametric Hermite matrix associated to $\boldsymbol{f}$ with respect to a basis $\mathcal{B}'$ that will be made explicit below.

  As we can freely choose any basis of form $\{c_i \cdot b_i \mid 1 \le i \le \delta\}$ where the c_i's are elements of $\mathbb{Q}[\boldsymbol{y}]$, we should use a basis that leads to a denominator-free matrix. To do this, we choose c_i as the denominator of $\mathsf{trace}(\mathcal{L}_{b_i})$ (which lies in the first row of the matrix $\mathcal{H}$ computed by TraceComputing). Then, for the entry of $\mathcal{H}$ that corresponds to b_i and b_j, we can multiply it with $c_i \cdot c_j$. The output matrix $\mathcal{H}'$ is the parametric Hermite matrix associated to $\boldsymbol{f}$ with respect to the basis $\{c_i \cdot b_i \mid 1 \le i \le \delta\}$.

  We observe in many examples that this subroutine returns either a denominator-free matrix or a matrix with smaller degree denominators. Thus, it facilitates further computations on the output matrix.

Evaluation & interpolation scheme for generic systems. Here we assume that the input system $\boldsymbol{f}$ satisfies Assumption (B). By Lemma 7, the entries of $\mathcal{H}$ are polynomials in $\mathbb{Q}[\boldsymbol{y}]$. Suppose that we know beforehand a value Λ that is larger than the degree of any entry of $\mathcal{H}$, we can compute $\mathcal{H}$ by an evaluation & interpolation scheme as follows.

We start by choosing randomly a set $\mathcal{E}$ of $\binom{t+\Lambda}{t}$ distinct points in $\mathbb{Q}^t$. Then, for each $\eta \in \mathcal{E}$, we use DRL-Matrix (Algorithm 1) on the input $\boldsymbol{f}(\eta, \cdot)$ to compute the classic Hermite matrix associated to $\boldsymbol{f}(\eta, \cdot)$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x})$. These computations involve only polynomials in $\mathbb{Q}[\boldsymbol{x}]$ and not in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$. Finally, we interpolate the parametric Hermite matrix $\mathcal{H}$ from its specialized images $\mathcal{H}(\eta)$ computed previously.

Since Assumption (B) holds, then $\mathcal{W}_\infty$ is empty. By Proposition 10, the Hermite matrix of $\boldsymbol{f}(\eta, \cdot)$ with respect to $\mathsf{grevlex}(\boldsymbol{x})$ is the image $\mathcal{H}(\eta)$ of $\mathcal{H}$. Therefore, the above scheme computes correctly the parametric Hermite matrix $\mathcal{H}$.

We also remark that, in the computation of the specializations $\mathcal{H}(\eta)$, we can replace the subroutine XMatrices in DRL-Matrix by a linear-algebra-based algorithm described in [16]. That algorithm constructs the Macaulay matrix and carries out matrix reductions to obtain simultaneously the normal forms that XMatrices requires.

In Section 6, we will estimate the complexity of this evaluation & interpolation scheme when the input system $\boldsymbol{f}$ satisfies some generic assumptions.

5. Algorithms for real root classification

We present in this section two algorithms targeting the real root classification problem through parametric Hermite matrices. The one described in Subsection 5.1 aims to solve the weak version of Problem (1). The second algorithm, given in Subsection 5.2 outputs the semi-algebraic formulas of the cells $\mathcal{S}_i$ that solves Problem (1). Further, in Section 6, we will see that, for a generic sequence $\boldsymbol{f}$, the semi-algebraic formulas computed by this algorithm consist of polynomials of degree bounded by $n(d-1)d^n$. Up to our knowledge, this improves all previously known bounds.

Throughout this section, our input is a parametric polynomial system $\boldsymbol{f} = (f_1, \dots, f_m) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$. We require that $\boldsymbol{f}$ satisfies Assumptions (A) and that the ideal $\langle \boldsymbol{f} \rangle$ is radical.

Let $\mathcal{G}$ be the reduced Gröbner basis of the ideal $\langle \boldsymbol{f} \rangle \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x}) > \mathsf{grevlex}(\boldsymbol{y})$. Let $\mathbb{K}$ denote the rational function field $\mathbb{Q}(\boldsymbol{y})$. We recall that $\mathcal{B} \subset \mathbb{Q}[\boldsymbol{x}]$ is the basis of $\mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ derived from $\mathcal{G}$ and $\mathcal{H}$ is the parametric Hermite matrix associated to $\boldsymbol{f}$ with respect to the basis $\mathcal{B}$.

5.1. Algorithm for the weak-version of Problem (1)

From Subsection 4.3, we know that, outside the algebraic set $\mathcal{W}_\infty := \cup_{g \in \mathcal{G}} V(\mathrm{lc}_{\boldsymbol{x}}(g))$, the parametric matrix $\mathcal{H}$ possesses good specialization property (see Proposition 10). We denote by $\boldsymbol{w}_\infty$ the square-free part of $\mathrm{lcm}_{g \in \mathcal{G}} \mathrm{lc}_{\boldsymbol{x}}(g)$. This polynomial $\boldsymbol{w}_\infty$ is returned as an output of Algorithm 1. Note that $V(\boldsymbol{w}_\infty) = \mathcal{W}_\infty$.

Lemma 13. When Assumption (A) holds and the ideal $\langle \boldsymbol{f} \rangle$ is radical, the determinant of $\mathcal{H}$ is not identically zero.

Proof. Recall that $\mathbb{K}$ denotes the rational function field $\mathbb{Q}(\boldsymbol{y})$. We prove that the ideal $\langle \boldsymbol{f} \rangle_{\mathbb{K}} \subset \mathbb{K}[\boldsymbol{x}]$ is radical.

Let $p \in \mathbb{K}[\boldsymbol{x}]$ such that there exists $n \in \mathbb{N}$ satisfying $p^n \in \langle \boldsymbol{f} \rangle_{\mathbb{K}}$. Therefore, there exists a polynomial $q \in \mathbb{Q}[\boldsymbol{y}]$ such that $q \cdot p^n \in \langle \boldsymbol{f} \rangle$. Then, $(q \cdot p)^n \in \langle \boldsymbol{f} \rangle$. As $\langle \boldsymbol{f} \rangle$ is radical, we have that $q \cdot p \in \langle \boldsymbol{f} \rangle$. Thus, $p \in \langle \boldsymbol{f} \rangle_{\mathbb{K}}$, which concludes that $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ is radical.

By Lemma 4, $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ is a radical zero-dimensional ideal in $\mathbb{Q}(\boldsymbol{y})$. Since $\mathcal{H}$ is also a Hermite matrix (in the classic sense) of $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$, $\mathcal{H}$ is full rank. Therefore, $\det(\mathcal{H})$ is not identically zero. □

Let $\boldsymbol{w}_{\mathcal{H}} \coloneqq \mathfrak{n}/\gcd(\mathfrak{n}, \boldsymbol{w}_\infty)$ where $\mathfrak{n}$ is the square-free part of the numerator of $\det(\mathcal{H})$. We denote by $\mathcal{W}_{\mathcal{H}}$ the vanishing set of $\boldsymbol{w}_{\mathcal{H}}$. By Lemma 13, $\mathcal{W}_{\mathcal{H}}$ is a proper Zariski closed subset of $\mathbb{C}^t$. Our algorithm relies on the following proposition.

Proposition 14. Assume that Assumption (A) holds and the ideal $\langle \boldsymbol{f} \rangle$ is radical. Then, for each connected component $\mathcal{S}$ of the semi-algebraic set $\mathbb{R}^t \setminus (\mathcal{W}_\infty \cup \mathcal{W}_{\mathcal{H}})$, the number of real solutions of $\boldsymbol{f}(\eta, \cdot)$ is invariant when η varies over $\mathcal{S}$.

Proof. By Lemma 12, $\mathcal{W}_\infty$ contains the following sets:

- The non-proper points of the restriction of π to $\mathcal{V}$.
- The point $\eta \in \mathbb{C}^t$ such that the fiber $\pi^{-1}(\eta) \cap \mathcal{V}$ is infinite.
- The image by π of the irreducible components of $\mathcal{V}$ whose dimensions are smaller than t.

Now we consider the set $K(\pi, \mathcal{V}) \coloneqq \mathrm{sing}(\mathcal{V}) \cup \mathrm{crit}(\pi, \mathcal{V})$. Let $\Delta \coloneqq \mathrm{jac}(\boldsymbol{f}, \boldsymbol{x})$ be the Jacobian matrix of $\boldsymbol{f}$ with respect to the variables $\boldsymbol{x}$. The ideal generated by the $n \times n$-minors of Δ is denoted by I_Δ. Note that, since $\boldsymbol{f}$ is radical, $K(\pi, \mathcal{V})$ is the algebraic set defined by the ideal $\langle \boldsymbol{f} \rangle + I_\Delta$.

By Proposition 10, for $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$, $\langle \boldsymbol{f} \rangle$ is a zero-dimensional ideal and the quotient ring $\mathbb{C}[\boldsymbol{x}]/\langle \boldsymbol{f}(\eta, \cdot) \rangle$ has dimension δ. Moreover, if $\eta \in \mathbb{C}^t \setminus (\mathcal{W}_\infty \cup \mathcal{W}_{\mathcal{H}})$, the system $\boldsymbol{f}(\eta, \cdot)$ has δ distinct complex solutions as the rank of $\mathcal{H}(\eta)$ is δ. Therefore, every complex root of $\boldsymbol{f}(\eta, \cdot)$ is of multiplicity one (we use the definition of multiplicity given in [4, Sec. 4.5]).

Now we prove that, for such a point η, the fiber $\pi^{-1}(\eta)$ does not intersect $K(\pi, \mathcal{V})$. Assume by contradiction that there exists a point $(\eta, \chi) \in \mathbb{C}^{t+n}$ lying in $\pi^{-1}(\eta) \cap K(\pi, \mathcal{V})$. Note that χ is a solution of $\boldsymbol{f}(\eta, \cdot)$, i.e., $\boldsymbol{f}(\eta, \chi) = 0$.

As $(\eta, \chi) \in K(\pi, \mathcal{V})$, then it is contained in $V(I_\Delta)$. Hence, as the derivation in Δ does not involve $\boldsymbol{y}$, χ cancels all the $n \times n$-minors of the Jacobian matrix $\mathrm{jac}(\boldsymbol{f}(\eta, \cdot), \boldsymbol{x})$. [4, Proposition 4.16] implies that χ has multiplicity greater than one. This contradicts to the claim that $\boldsymbol{f}(\eta, \cdot)$ admits only complex solutions of multiplicity one.

Therefore, we conclude that, for $\eta \in \mathbb{C}^t \setminus (\mathcal{W}_\infty \cup \mathcal{W}_{\mathcal{H}})$, $\pi^{-1}(\eta)$ does not intersect $K(\pi, \mathcal{V})$.

So, using what we prove above and Lemma 12, we deduce that, for $\eta \in \mathbb{R}^t \setminus (\mathcal{W}_\infty \cup \mathcal{W}_{\mathcal{H}})$, then there exists an open neighborhood O_η of η for the Euclidean topology such that $\pi^{-1}(O_\eta)$ does not intersect $K(\pi, \mathcal{V}) \cup \pi^{-1}(\mathcal{W}_\infty)$.

Therefore, by Thom's isotopy lemma [11], the projection π realizes a locally trivial fibration over $\mathbb{R}^t \setminus (\mathcal{W}_\infty \cup \mathcal{W}_{\mathcal{H}})$. So, for any connected component C of $\mathbb{R}^t \setminus (\mathcal{W}_\infty \cup \mathcal{W}_{\mathcal{H}})$ and any $\eta \in C$, we have that $\pi^{-1}(C) \cap \mathcal{V} \cap \mathbb{R}^{t+n}$ is homeomorphic to $C \times (\pi^{-1}(\eta) \cap \mathcal{V} \cap \mathbb{R}^{t+n})$.

As a consequence, the number of distinct real solutions of $\boldsymbol{f}(\eta, \cdot)$ is invariant when η varies over each connected component of $\mathbb{R}^t \setminus (\mathcal{W}_\infty \cup \mathcal{W}_{\mathcal{H}})$. ☐

To describe Algorithm 2, we need to introduce the following subroutines:

- CleanFactors which takes as input a polynomial $p \in \mathbb{Q}[\boldsymbol{y}, \boldsymbol{x}]$ and the polynomial $\boldsymbol{w}_\infty$. It computes the square-free part of p with all the common factors with $\boldsymbol{w}_\infty$ removed.
- Signature which takes as input a symmetric matrix with entries in $\mathbb{Q}$ and evaluates its signature.

- SamplePoints which takes as input a set of polynomials $g_1, \ldots, g_s \in \mathbb{Q}[\boldsymbol{y}]$ and computes a finite subset $\mathcal{R}$ of $\mathbb{Q}^t$ that intersects every connected component of the semi-algebraic set defined by $\wedge_{i=1}^{s} g_i \neq 0$. An explicit description of SamplePoints is given in the proof of Theorem II in Section 3.

The pseudo-code of Algorithm 2 is below. Its proof of correctness follows immediately from Proposition 14 and Corollary 11.

Algorithm 2: Weak-RRC-Hermite

Input: A polynomial sequence $\boldsymbol{f} \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ such that $\langle \boldsymbol{f} \rangle$ is radical and Assumptions (A) holds.

Output: A set of sample points and the corresponding numbers of real solutions solving the weak version of Problem (1)

```
[𝓗, w_∞] ← DRL-Matrix(f)
w_𝓗 ← CleanFactors(numer(det(𝓗)), w_∞)
L ← SamplePoints(w_𝓗 ≠ 0 ∧ w_∞ ≠ 0)
for η ∈ L do
    r_η ← Signature(𝓗(η))
end
return {(η, r_η) | η ∈ L}
```

Remark 15. As we have seen, Algorithm 2 obtains a polynomial which serves similarly as discriminant varieties [35] or border polynomials [49] through computing the determinant of parametric Hermite matrices. Whereas, the two latter strategies rely on algebraic elimination based on Gröbner bases to compute the projection of $\mathsf{crit}(\pi, \mathcal{V})$ on the $\boldsymbol{y}$-space. Since it is well-known that the computation of such a Gröbner basis could be heavy, our algorithm has a chance to be more practical. In Section 7, we provide experimental results to support this claim.

Remark 16. It is worth noticing that, even though the design of Algorithm 2 employs the grevlex monomial ordering where $x_1 \succ \cdots \succ x_n$, we can replace it by any grevlex ordering with another lexicographical order among the $\boldsymbol{x}$'s. For instance, we can use the monomial ordering $\mathsf{grevlex}(x_n \succ \cdots \succ x_1)$. While every theoretical claim still holds for this ordering, the practical behavior could be different.

5.2. Computing semi-algebraic formulas

By Corollary 11, the number of real roots of the system $\boldsymbol{f}(\eta, \cdot)$ for a given point $\eta \in \mathbb{R}^t \setminus \mathcal{W}_\infty$ can be obtained by evaluating the signature of the parametric Hermite matrix $\mathcal{H}$. We recall that the signature of a matrix can be deduced from the sign pattern of its leading principal minors. More precisely, we recall the following criterion, introduced by [46] and [31] (see [23] for a summary on these works).

Lemma 17. [23, Theorem 2.3.6] Let S be a $\delta \times \delta$ symmetric matrix in $\mathbb{R}^{\delta \times \delta}$ and, for $1 \le i \le \delta$, S_i be the i-th leading principal minor of S, i.e., the determinant of the submatrix formed by the first i rows and i columns of S. By convention, we denote $S_0 = 1$.

We assume that $S_i \neq 0$ for $0 \le i \le \delta$. Let k be the number of sign variations between S_i and S_{i+1}. Then, the numbers of positive and negative eigenvalues of S are respectively $\delta - k$ and k. Thus, the signature of S is $\delta - 2k$.

This criterion leads us to the following idea. Assume that none of the leading principal minors of $\mathcal{H}$ is identically zero. We consider the semi-algebraic subset of $\mathbb{R}^t$ defined by the non-vanishing of those leading principal minors. Over a connected component $\mathcal{S}'$ of this semi-algebraic set, each leading principal minor is not zero and its sign is invariant. As a consequence, by Lemma 17 and Corollary 11, the number of distinct real roots of $\boldsymbol{f}(\eta, \cdot)$ when η varies over $\mathcal{S}' \setminus \mathcal{W}_\infty$ is invariant.

However, this approach does not apply directly if one of the leading principle minors of $\mathcal{H}$ is identically zero. We bypass this obstacle by picking randomly an invertible matrix $A \in \mathrm{GL}_\delta(\mathbb{Q})$ and working with the matrix $\mathcal{H}_A \coloneqq A^T \cdot \mathcal{H} \cdot A$. The lemma below states that, with a generic matrix A, all of the leading principal minors of $\mathcal{H}_A$ are not identically zero.

Lemma 18. There exists a Zariski dense subset $\mathscr{A}$ of $\mathrm{GL}_\delta(\mathbb{Q})$ such that for $A \in \mathscr{A}$, all of the leading principal minors of $\mathcal{H}_A \coloneqq A^T \cdot \mathcal{H} \cdot A$ are not identically zero.

Proof. For $1 \le r \le \delta$, we denote by $\mathfrak{M}_r$ the set of all $r \times r$ minors of $\mathcal{H}$.

Let $\eta \in \mathbb{Q}^t \setminus \mathcal{W}_\infty \cup \mathcal{W}_{\mathcal{H}}$. We have that $\mathcal{H}(\eta)$ is a full rank matrix in $\mathbb{Q}^{\delta\times\delta}$ and, for $A \in \mathrm{GL}_\delta(\mathbb{R})$, $\mathcal{H}_A(\eta) = A^T \cdot \mathcal{H}(\eta) \cdot A$.

We prove that there exists a Zariski dense subset $\mathscr{A}$ of $\mathrm{GL}_\delta(\mathbb{Q})$ such that, for $A \in \mathscr{A}$, all of the leading principal minors of $\mathcal{H}_A(\eta)$ are not zero. Then, as an immediate consequence, all the leading principal minors of $\mathcal{H}_A$ are not identically zero.

We consider the matrix $A = (a_{i,j})_{1\le i,j\le\delta}$ where $\boldsymbol{a} = (a_{i,j})$ are new variables. Then, the r-th leading principal minor $M_r(\boldsymbol{a})$ of $A^T \cdot \mathcal{H}(\eta) \cdot A$ can be written as

$$M_r(\boldsymbol{a}) = \sum_{\mathfrak{m}\in\mathfrak{M}_r} a_{\mathfrak{m}} \cdot \mathfrak{m}(\eta),$$

where the $a_{\mathfrak{m}}$'s are elements of $\mathbb{Q}[\boldsymbol{a}]$.

As $\mathcal{H}(\eta)$ is a full rank symmetric matrix by assumption, there exists a matrix $Q \in \mathrm{GL}_\delta(\mathbb{R})$ such that $Q^T \cdot \mathcal{H}(\eta) \cdot Q$ is a diagonal matrix with no zero on its diagonal. Hence, the evaluation of $\boldsymbol{a}$ at the entries of Q gives $M_r(\boldsymbol{a})$ a non-zero value. As a consequence, $M_r(\boldsymbol{a})$ is not identically zero.

Let $\mathscr{A}_r$ be the non-empty Zariski open subset of $\mathrm{GL}_\delta(\mathbb{Q})$ defined by $M_r(\boldsymbol{a}) \neq 0$. Then, the set of the matrices $A \in \mathscr{A}_r$ such that the $r \times r$ leading principal minor of $A^T \cdot \mathcal{H}(\eta) \cdot A$ is not zero.

Taking $\mathscr{A}$ as the intersection of $\mathscr{A}_r$ for $1 \le r \le \delta$, then, for $A \in \mathscr{A}$, none of the leading principal minors of $A^T \cdot \mathcal{H}(\eta) \cdot A$ equals zero. Consequently, each leading principal minor of $A^T \cdot \mathcal{H} \cdot A$ is not identically zero. ☐

Our algorithm (Algorithm 3) for solving Problem (1) through parametric Hermite matrices is described below. As it depends on the random choice of the matrix A, Algorithm 3 is probabilistic. One can easily modify it to be a Las Vegas algorithm by detecting the cancellation of the leading principal minors for each choice of A.

Algorithm 3: RRC-Hermite

Input: A polynomial sequence $\boldsymbol{f} \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ such that the ideal $\langle \boldsymbol{f} \rangle$ is radical and $\boldsymbol{f}$ satisfies Assumption (A)

Output: The descriptions of a collection of semi-algebraic sets $\mathcal{S}_i$ solving Problem (1)

```
H, w_∞ ← DRL-Matrix(f)
Choose randomly a matrix A in Q^{δ×δ}
H_A ← A^T · H · A
(M_1, ..., M_δ) ← LeadingPrincipalMinors(H_A)
L ← SamplePoints(w_∞ ∧ (∧_{i=1}^{δ} M_i ≠ 0))
for η ∈ L do
    r_η ← Signature(H(η))
end
return {(sign (M_1(η), ..., M_δ(η)), η, r_η) | η ∈ L}
```

Proposition 19. Assume that $\boldsymbol{f}$ satisfies Assumptions (A) and that the ideal $\langle \boldsymbol{f} \rangle$ is radical. Let A be a matrix in $\mathrm{GL}_\delta(\mathbb{Q})$ such that all of the leading principal minors $M_1, \ldots, M_\delta$ of $\mathcal{H}_A := A^T \cdot \mathcal{H} \cdot A$ are not identically zero. Then, Algorithm 3 computes correctly a solution for Problem (1).

Proof. Note that for $\eta \in \mathbb{R}^t \setminus \mathcal{W}_\infty$, we have that $\mathcal{H}_A(\eta) = A^T \cdot \mathcal{H}(\eta) \cdot A$. Therefore, the signature of $\mathcal{H}(\eta)$ equals to the signature of $\mathcal{H}_A(\eta)$.

Let $M_1, \ldots, M_\delta$ be the leading principal minors of $\mathcal{H}_A$ and $\mathcal{S}$ be the algebraic set defined by $\wedge_{i=1}^{\delta} M_i \neq 0$. Over each connected component $\mathcal{S}'$ of $\mathcal{S}$, the sign of each M_i is invariant and not zero. Therefore, by Lemma 17, the signature of $\mathcal{H}_A(\eta)$, and therefore of $\mathcal{H}(\eta)$, is invariant when η varies over $\mathcal{S}' \setminus \mathcal{W}_\infty$. As a consequence, by Corollary 11, the number of distinct real roots of $\boldsymbol{f}(\eta, \cdot)$ is also invariant when η varies over $\mathcal{S}' \setminus \mathcal{W}_\infty$. We finish the proof of correctness of Algorithm 3. $\square$

6. Complexity analysis

6.1. Degree bound of parametric Hermite matrices on generic input

In this subsection, we consider an affine regular sequence $\boldsymbol{f} = (f_1, \ldots, f_n) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ according to the variables $\boldsymbol{x}$, i.e., the homogeneous components of largest degree in $\boldsymbol{x}$ of the f_i's form a homogeneous regular sequence (see Section 2). Additionally, we require that $\boldsymbol{f}$ satisfies Assumptions (A) and (B).

Let d be the highest value among the total degrees of the f_i's. Since the homogeneous regular sequences are generic among the homogeneous polynomial sequences (see, e.g., [2, Proposition 1.7.4] or [37]), the same property of genericity holds for affine regular sequences (thanks to the definition we use).

As in previous sections, $\mathcal{G}$ denotes the reduced Gröbner basis of $\langle \boldsymbol{f} \rangle$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x}) > \mathsf{grevlex}(\boldsymbol{y})$. Let δ be the dimension of the $\mathbb{K}$-vector space $\mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ where $\mathbb{K} = \mathbb{Q}(\boldsymbol{y})$. By Bézout's inequality, $\delta \leq d^n$. We derive from $\mathcal{G}$ a basis $\mathcal{B} = \{b_1, \ldots, b_\delta\}$ of $\mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ consisting of monomials in the variables $\boldsymbol{x}$. Finally, the parametric Hermite matrix of $\boldsymbol{f}$ with respect to $\mathcal{B}$ is denoted by $\mathcal{H} = (h_{i,j})_{1 \leq i,j \leq \delta}$.

For a polynomial $p \in \mathbb{Q}[\boldsymbol{y}, \boldsymbol{x}]$, we denote by $\deg(p)$ the total degree of p in $(\boldsymbol{y}, \boldsymbol{x})$ and $\deg_{\boldsymbol{x}}(p)$ the partial degree of p in the variables $\boldsymbol{x}$.

As Assumption (B) holds, by Lemma 7, the entries of the parametric Hermite matrix $\mathcal{H}$ associated to $\boldsymbol{f}$ with respect to the basis $\mathcal{B}$ are elements of $\mathbb{Q}[\boldsymbol{y}]$. To establish a degree bound on the entries of $\mathcal{H}$, we need to introduce the following assumption.

Assumption C. For any $g \in \mathcal{G}$, we have that $\deg(g) = \deg_{\boldsymbol{x}}(g)$.

Proposition 20 below states that Assumption (C) is generic. Its direct consequence is a proof for Proposition 8.

Proposition 20. Let $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_d$ be the set of polynomials in $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]$ having total degree bounded by d. There exists a non-empty Zariski open subset $\mathscr{F}_D$ of $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_d^n$ such that Assumption (C) holds for $\boldsymbol{f} \in \mathscr{F}_D \cap \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]^n$.

Consequently, for $\boldsymbol{f} \in \mathscr{F}_D \cap \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]^n$, $\boldsymbol{f}$ satisfies Assumption (B).

Proof. Let y_{t+1} be a new indeterminate. For any polynomial $p \in \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$, we consider the homogenized polynomial $p_h \in \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]$ of p defined as follows:

$$p_h = y_{t+1}^{\deg(p)} p\left(\frac{x_1}{y_{t+1}}, \dots, \frac{x_n}{y_{t+1}}, \frac{y_1}{y_{t+1}}, \dots, \frac{y_t}{y_{t+1}}\right).$$

Let $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]_d^h$ be the set of homogeneous polynomials in $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]$ whose degrees are exactly d. By [47, Corollary 1.85], there exists a non-empty Zariski subset $\mathscr{F}_D^h$ of $\left(\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]_d^h\right)^n$ such that the variables $\boldsymbol{x}$ is in Noether position with respect to $\boldsymbol{f}_h$ for every $\boldsymbol{f}_h \in \mathscr{F}_D^h$.

For $\boldsymbol{f}_h \in \mathscr{F}_D^h$, let $\boldsymbol{G}_h$ be the reduced Gröbner basis of $\boldsymbol{f}_h$ with respect to the grevlex ordering $\mathsf{grevlex}(\boldsymbol{x} \succ \boldsymbol{y} \succ y_{t+1})$. By [3, Proposition 7], if the variables $\boldsymbol{x}$ is in Noether position with respect to $\boldsymbol{f}_h$, then the leading monomials appearing in $\boldsymbol{G}_h$ depend only on $\boldsymbol{x}$.

Let $\boldsymbol{f}$ and $\boldsymbol{G}$ be the image of $\boldsymbol{f}_h$ and $\boldsymbol{G}_h$ by substituting $y_{t+1} = 1$. We show that $\boldsymbol{G}$ is a Gröbner basis of $\boldsymbol{f}$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x} \succ \boldsymbol{y})$.

Since $\boldsymbol{G}_h$ generates $\langle \boldsymbol{f}_h \rangle$, $\boldsymbol{G}$ is a generating set of $\langle \boldsymbol{f} \rangle$. As the leading monomials of elements in $\boldsymbol{G}_h$ do not depend on y_{t+1}, the substitution $y_{t+1} = 1$ does not affect these leading monomials.

For a polynomial $p \in \langle \boldsymbol{f} \rangle \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$, then p writes $p = \sum_{i=1}^{n} c_i \cdot f_i$, where the c_i's lie in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$. We homogenize the polynomials $c_i \cdot f_i$ on the right hand side to obtain a homogeneous polynomial $P_h \in \langle \boldsymbol{f}_h \rangle$. Note that P_h is not necessarily the homogenization p_h of p but only the product of p_h with a power of y_{t+1}. Then, there exists a polynomial $g_h \in \boldsymbol{G}_h$ such that the leading monomial of g_h divides the leading monomial of P_h. Since the leading monomial of g_h depends only on $\boldsymbol{x}$, it also divides the leading monomial of p_h, which is the leading monomial of p. So, the leading monomial of the image of g_h in $\boldsymbol{G}$ divides the leading monomial of p. We conclude that $\boldsymbol{G}$ is a Gröbner basis of $\boldsymbol{f}$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x} \succ \boldsymbol{y})$ and the set of leading monomials in $\boldsymbol{G}$ depends only on the variables $\boldsymbol{x}$.

Let $\mathscr{F}_D$ be the subset of $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_d^n$ such that for every $\boldsymbol{f} \in \mathscr{F}_D$, its homogenization $\boldsymbol{f}_h$ is contained in $\mathscr{F}_D^h$. Since the two spaces $\left(\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]_d^h\right)^n$ and $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_d^n$ are both exactly

$\mathbb{C}^{\binom{d+n+t}{n+t}\times n}$ (by considering each monomial coefficient as a coordinate), $\mathscr{F}_D$ is also a non-empty Zariski open subset of $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_d^n$.

Assume now that the polynomial sequence $\boldsymbol{f}$ belongs to $\mathscr{F}_D$. We consider the two monomial orderings over $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ below:

- The elimination ordering $\mathsf{grevlex}(\boldsymbol{x}) > \mathsf{grevlex}(\boldsymbol{y})$ is abbreviated by O_1. The leading monomial of $p \in \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ with respect to O_1 is denoted by $\mathrm{lm}_1(p)$. The reduced Gröbner basis of $\boldsymbol{f}$ with respect to O_1 is $\mathcal{G}$.

- The grevlex ordering $\mathsf{grevlex}(\boldsymbol{x} > \boldsymbol{y})$ is abbreviated by O_2. The leading monomial of $p \in \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ with respect to O_2 is denoted by $\mathrm{lm}_2(p)$. The reduced Gröbner basis of $\boldsymbol{f}$ with respect to O_2 is denoted by $\mathcal{G}_2$.

As proven above, the set $\{\mathrm{lm}_2(g_2) \mid g_2 \in \mathcal{G}_2\}$ does not depend on $\boldsymbol{y}$. With this property, we will show, for any $g_2 \in \mathcal{G}_2$, there exists a polynomial $g \in \mathcal{G}$ such that $\mathrm{lm}_1(g)$ divides $\mathrm{lm}_2(g_2)$.

By definition, $\mathrm{lm}_2(g_2)$ is greater than any other monomial of g_2 with respect to the ordering O_2. Since $\mathrm{lm}_2(g_2)$ depends only on the variables $\boldsymbol{x}$, it is then greater than any monomial of g_2 with respect to the ordering O_1. Hence, $\mathrm{lm}_2(g_2)$ is also $\mathrm{lm}_1(g_2)$. Consequently, since $\mathcal{G}$ is a Gröbner basis of $\boldsymbol{f}$ with respect to O_1, there exists a polynomial $g \in \mathcal{G}$ such that $\mathrm{lm}_1(g)$ divides $\mathrm{lm}_1(g_2) = \mathrm{lm}_2(g_2)$.

Next, we prove that for every $g \in \mathcal{G}$, $\mathrm{lm}_1(g)$ is also $\mathrm{lm}_2(g)$. For this, we rely on the fact that $\mathcal{G}$ is reduced. Assume by contradiction that there exists a polynomial $g \in \mathcal{G}$ such that $\mathrm{lm}_1(g) \neq \mathrm{lm}_2(g)$. Thus, $\mathrm{lm}_2(g)$ must contain both $\boldsymbol{x}$ and $\boldsymbol{y}$. Let $t_{\boldsymbol{x}}$ be the part in only variables $\boldsymbol{x}$ of $\mathrm{lm}_2(g)$. Note that $\mathrm{lm}_1(g)$ is greater than $t_{\boldsymbol{x}}$ with respect to O_1. There exists an element $g_2 \in \mathcal{G}_2$ such that $\mathrm{lm}_2(g_2)$ divides $\mathrm{lm}_2(g)$. Since $\mathrm{lm}_2(g_2)$ depends only on the variables $\boldsymbol{x}$, we have that $\mathrm{lm}_2(g_2)$ divides $t_{\boldsymbol{x}}$. Then, by what we proved above, there exists $g' \in \mathcal{G}$ such that $\mathrm{lm}_1(g)$ divides $\mathrm{lm}_2(g_2)$, so $\mathrm{lm}_1(g)$ divides $t_{\boldsymbol{x}}$. This implies that $\mathcal{G}$ is not reduced, which contradicts the definition of $\mathcal{G}$.

So, $\mathrm{lm}_1(g) = \mathrm{lm}_2(g)$ for every $g \in \mathcal{G}$ and, consequently, $\deg(g) = \deg_{\boldsymbol{x}}(g)$. We conclude that there exists a non-empty Zariski open subset $\mathscr{F}_D$ (as above) of $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_d^n$ such that Assumption (C) holds for every $\boldsymbol{f} \in \mathscr{F}_D \cap \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]^n$.

Additionally, one easily notices that Assumption (C) implies Assumption (B). As a consequence, $\boldsymbol{f}$ also satisfies Assumption (B) for any $\boldsymbol{f} \in \mathscr{F}_D \cap \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]^n$. □

Recall that, when Assumption (B) holds, by Lemma 7, the trace of any multiplication map $\mathcal{L}_p$ is a polynomial in $\mathbb{Q}[\boldsymbol{y}]$ where $p \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$. We now estimate the degree of $\mathsf{trace}(\mathcal{L}_p)$. Since the map $p \mapsto \mathsf{trace}(\mathcal{L}_p)$ is linear, it is sufficient to consider p as a monomial in the variables $\boldsymbol{x}$.

Proposition 21. Assume that Assumption (C) holds. Then, for any monomial m in the variables $\boldsymbol{x}$, the degree in $\boldsymbol{y}$ of $\mathsf{trace}(\mathcal{L}_m)$ is bounded by $\deg(m)$. As a consequence, the total degree of the entry $h_{i,j} = \mathsf{trace}(\mathcal{L}_{b_i \cdot b_j})$ of $\mathcal{H}$ is at most the sum of the total degrees of b_i and b_j, i.e.,

$$\deg(h_{i,j}) \leq \deg(b_i) + \deg(b_j).$$

Proof. Let m be a monomial in $\mathbb{Q}[\boldsymbol{x}]$. The multiplication matrix $\mathcal{L}_m$ is built as follows.

For $1 \leq i \leq \delta$, the normal form of $b_i \cdot m$ as a polynomial in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ writes

$$\mathrm{NF}_{\mathcal{G}}(b_i \cdot m) = \sum_{j=1}^{\delta} c_{i,j} \cdot b_j.$$

Note that this normal form is the remainder of the successive divisions of $b_i \cdot m$ by polynomials in $\mathcal{G}$. As Assumption (C) holds, Assumption (B) also holds. Therefore, those divisions do not introduce any denominator. So, every term appearing during these normal form reductions are polynomials in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$.

Let $p \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$. For any $g \in \mathcal{G}$, by Assumption (C), the total degree in $(\boldsymbol{y}, \boldsymbol{x})$ of every term of g is at most the degree of $\mathrm{lm}_{\boldsymbol{x}}(g)$. Thus, a division of p by g involves only terms of total degree $\deg(p)$. Thus, during the polynomial division of p to $\mathcal{G}$, only terms of degree at most $\deg(p)$ will appear. Hence the degree of $\mathrm{NF}_{\mathcal{G}}(p)$ is bounded by $\deg(p)$.

Note that $\mathrm{trace}(\mathcal{L}_m) = \sum_{i=1}^{\delta} c_{i,i}$. As the degree of $c_{i,i} \cdot b_i$ is bounded by $\deg(b_i) + \deg(m)$, the degree of $c_{i,i}$ is at most $\deg(m)$. Then, we obtain that $\deg(\mathrm{trace}(\mathcal{L}_m)) \leq \deg(m)$.

Finally, the degree bound of $h_{i,j}$ follows immediately:

$$\deg(h_{i,j}) = \deg(\mathrm{trace}(\mathcal{L}_{b_i \cdot b_j})) \leq \deg(b_i \cdot b_j) = \deg(b_i) + \deg(b_j).$$

□

Lemma 22. Assume that $\boldsymbol{f}$ satisfies Assumption (C). Then the degree of a minor M consisting of the rows $(r_1, \dots, r_\ell)$ and the columns $(c_1, \dots, c_\ell)$ of $\mathcal{H}$ is bounded by

$$\sum_{i=1}^{\ell} \left(\deg(b_{r_i}) + \deg(b_{c_i})\right).$$

Particularly, the degree of $\det(\mathcal{H})$ is bounded by $2\sum_{i=1}^{\delta} \deg(b_i)$.

Proof. We expand the minors M into terms of the form $(-1)^{\mathrm{sign}\,(\sigma)} h_{r_1,\sigma(c_1)} \dots h_{r_\ell,\sigma(c_\ell)}$, where σ is a permutation of $\{c_1, \dots, c_\ell\}$ and $\mathrm{sign}\,(\sigma)$ is its signature. We then bound the degree of each of those terms as follows using Proposition 21:

$$\deg\left(\prod_{i=1}^{\ell} h_{r_i,\sigma(c_i)}\right) = \sum_{i=1}^{\ell} \deg(h_{r_i,\sigma(c_i)}) \leq \sum_{i=1}^{\ell} \left(\deg(b_{r_i}) + \deg(b_{\sigma(c_i)})\right) = \sum_{i=1}^{\ell} \left(\deg(b_{r_i}) + \deg(b_{c_i})\right).$$

Hence, taking the sum of all those terms, we obtain the inequality:

$$\deg(M_i) \leq \sum_{i=1}^{\ell} \left(\deg(b_{r_i}) + \deg(b_{c_i})\right).$$

When M is taken as the determinant of $\mathcal{H}$, then

$$\deg(\det(\mathcal{H})) \leq 2\sum_{i=1}^{\delta} \deg(b_i).$$

□

Proposition 21 implies that, when Assumption (C) holds, the degree pattern of $\mathcal{H}$ depends only on the degree of the elements of $\mathcal{B} = \{b_1, \dots, b_\delta\}$. We rearrange $\mathcal{B}$ in the increasing order of degree, i.e., $\deg(b_i) \le \deg(b_j)$ for $1 \le i < j \le \delta$. So, $b_1 = 1$ and $\deg(b_1) = 0$. The degree bounds of the entries of $\mathcal{H}$ are expressed by the matrix below

$$\begin{bmatrix} 0 & \deg(b_2) & \dots & \deg(b_\delta) \\ \deg(b_2) & 2\deg(b_2) & \dots & \deg(b_\delta) + \deg(b_2) \\ \vdots & \vdots & \ddots & \vdots \\ \deg(b_\delta) & \deg(b_\delta) + \deg(b_2) & \dots & 2\deg(b_\delta) \end{bmatrix}.$$

Moreover, using the regularity of $\boldsymbol{f}$, we are able to establish explicit degree bounds for the elements of $\mathcal{B}$ and then, for the minors of $\mathcal{H}$.

Lemma 23. Assume that $\boldsymbol{f}$ is an affine regular sequence and let $\mathcal{B}$ be the basis defined as above. Then the highest degree among the elements of $\mathcal{B}$ is bounded by $n(d-1)$ and

$$2\sum_{i=1}^{\delta} \deg(b_i) \le n(d-1)d^n.$$

Proof. For $p \in \mathbb{K}[\boldsymbol{x}]$, let $p_h \in \mathbb{K}[x_1, \dots, x_{n+1}]$ be the homogenization of p with respect to the variable x_{n+1}, i.e.,

$$p_h = x_{n+1}^{\deg_{\boldsymbol{x}}(p)}\, p\left(\frac{x_1}{x_{n+1}}, \dots, \frac{x_n}{x_{n+1}}\right).$$

The dehomogenization map α is defined as:

$$\begin{aligned} \alpha :\ \mathbb{K}[x_1, \dots, x_{n+1}] &\to \mathbb{K}[x_1, \dots, x_n], \\ p(x_1, \dots, x_{n+1}) &\mapsto p(x_1, \dots, x_n, 1). \end{aligned}$$

Also, the homogeneous component of largest degree of p with respect to the variables $\boldsymbol{x}$ is denoted by ${}^{H}p$. Throughout this proof, we use the following notations:

- $I = \langle \boldsymbol{f} \rangle_{\mathbb{K}}$ and $\mathcal{G}$ is the reduced Gröbner basis of I w.r.t. $\mathsf{grevlex}(x_1 \succ \cdots \succ x_n)$.
- $I_h = \langle p_h \mid p \in \boldsymbol{f} \rangle_{\mathbb{K}}$ and $\mathcal{G}_h$ is the reduced Gröbner basis of I_h w.r.t. $\mathsf{grevlex}(x_1 \succ \cdots \succ x_{n+1})$.

The Hilbert series of the homogeneous ideal I_h writes

$$\mathrm{HS}_{I_h}(z) = \sum_{r=0}^{\infty} \left(\dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{x}]_r - \dim_{\mathbb{K}}(I_h \cap \mathbb{K}[\boldsymbol{x}]_r)\right) \cdot z^r,$$

where $\mathbb{K}[\boldsymbol{x}]_r = \{p \mid p \in \mathbb{K}[\boldsymbol{x}] :\ \deg_{\boldsymbol{x}}(p) = r\}$

Since $\boldsymbol{f}$ is an affine regular sequence, by definition (see Section 2), ${}^{H}\boldsymbol{f} = ({}^{H}f_1, \dots, {}^{H}f_n)$ forms a homogeneous regular sequence. Equivalently, by [47, Proposition 1.44], the homogeneous polynomial sequence $((f_1)_h, \dots, (f_n)_h, x_{n+1})$ is regular. Particularly, $((f_1)_h, \dots, (f_n)_h)$ is a homogeneous regular sequence and, by [36, Theorem 1.5], we obtain

$$\mathrm{HS}_{I_h}(z) = \frac{\prod_{i=1}^{n}\left(1 - z^{\deg(f_i)}\right)}{(1-z)^{n+1}} = \frac{\prod_{i=1}^{n}\left(1 + \ldots + z^{\deg(f_i)-1}\right)}{1-z}.$$

On the other hand, as $((f_1)_h, \ldots, (f_n)_h, x_{n+1})$ is a homogeneous regular sequence, by [3, Proposition 7], the leading terms of $\mathcal{G}_h$ w.r.t. $\mathsf{grevlex}(x_1 > \cdots > x_{n+1})$ do not depend on the variables x_{n+1}. Thus, the dehomogenization map α does not affect the set of leading terms of $\mathcal{G}_h$. Besides, $\alpha(\mathcal{G}_h)$ is a Gröbner basis of I with respect to $\mathsf{grevlex}(\boldsymbol{x})$ (see, e.g., the proof of [20, Lemma 27]). Hence, the leading terms of $\mathcal{G}_h$ coincides with the leading terms of $\mathcal{G}$.

As a consequence, the set of monomials in $(x_1, \ldots, x_{n+1})$ which are not contained in the initial ideal of I_h with respect to $\mathsf{grevlex}(x_1 > \cdots > x_{n+1})$ is exactly

$$\{b \cdot x_{n+1}^j \mid b \in \mathcal{B}, j \in \mathbb{N}\}.$$

As a consequence, $\dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{x}]_r - \dim_{\mathbb{K}}(I_h \cap \mathbb{K}[\boldsymbol{x}]_r) = \sum_{j=0}^{r} |\mathcal{B} \cap \mathbb{K}[\boldsymbol{x}]_j|$. Let $H(z) = \sum_{r=0}^{\infty} |\mathcal{B} \cap \mathbb{K}[\boldsymbol{x}]_r| \cdot z^r$. We have that

$$(1-z) \cdot \mathrm{HS}_{I_h}(z) = (1-z) \sum_{r=0}^{\infty} \sum_{j=0}^{r} |\mathcal{B} \cap \mathbb{K}[\boldsymbol{x}]_j| \cdot z^r = \sum_{r=0}^{\infty} |\mathcal{B} \cap \mathbb{K}[\boldsymbol{x}]_r| \cdot z^r = H(z).$$

Then,

$$H(z) = \prod_{i=1}^{n} \left(1 + \ldots + z^{\deg(f_i)-1}\right).$$

As a direct consequence, $\max_{1 \le i \le \delta} \deg(b_i)$ is bounded by $\sum_{i=1}^{n} \deg(f_i) - n \le n(d-1)$.

Let G_1 and G_2 be two polynomials in $\mathbb{Z}[z]$. We write $G_1 \le G_2$ if and only if for any $r \ge 0$, the coefficient of z^r in G_2 is greater than or equal to the one in G_1.

Since $\deg(f_i) \le d$ for every $1 \le i \le n$, then

$$H(z) = \prod_{i=1}^{n} \left(1 + \ldots + z^{\deg(f_i)-1}\right) \le \prod_{i=1}^{n} \left(1 + \ldots + z^{d-1}\right).$$

As a consequence, $H'(z) = \sum_{r=1}^{\infty} (r\ |\mathcal{B} \cap \mathbb{K}[\boldsymbol{x}]_r|) \cdot z^{r-1} \le \left(\prod_{i=1}^{n} \left(1 + \ldots + z^{d-1}\right)\right)'$. Expanding $G'(z)$, we obtain

$$H'(z) \le \frac{n\left(\sum_{i=0}^{d-1} z^i\right)^{n-1} \left(\sum_{i=0}^{d-1} z^i - dz^{d-1}\right)}{1-z} = n \left(\sum_{i=0}^{d-1} z^i\right)^{n-1} \sum_{i=0}^{d-2} z^i \left(1 + \ldots + z^{d-i-2}\right).$$

By substituting $z = 1$ in the above inequality, we obtain

$$H'(1) \le nd^{n-1} \sum_{i=0}^{d-2} (d-i-1) = \frac{n(d-1)d^n}{2}.$$

Thus, we have that $\sum_{i=1}^{\delta} \deg(b_i) = \sum_{r=0}^{\infty} r\ |\mathcal{B} \cap \mathbb{K}[\boldsymbol{x}]_r| = H'(1) \le \frac{n(d-1)d^n}{2}$. □

Corollary 24 below follows immediately from Lemmas 22 and 23.

Corollary 24. Assume that $\boldsymbol{f}$ is a regular sequence that satisfies Assumption (C). Then the degree of any minor of $\mathcal{H}$ is bounded by $n(d-1)d^n$.

Remark 25. Note that Assumption (C) requires a condition on the degrees of polynomials in the Gröbner basis $\mathcal{G}$ of $\langle \boldsymbol{f} \rangle$. We remark that it is possible to establish similar bounds for the degrees of entries of our parametric Hermite matrix and its minors when the system $\boldsymbol{f}$ satisfies a weaker property than Assumption (C) (we still keep the regularity assumption).

Indeed, we only need to assume that, for any $g \in \mathcal{G}$, the homogeneous component of the highest degree in $\boldsymbol{x}$ of g does not depend on the parameters $\boldsymbol{y}$. Let $d_{\boldsymbol{y}}$ be an upper bound of the partial degrees in $\boldsymbol{y}$ of elements of $\mathcal{G}$. Under the change of variables $x_i \mapsto x_i^{d_{\boldsymbol{y}}}$, $\boldsymbol{f}$ is mapped to a new polynomial sequence that satisfies Assumption (C). Therefore, we easily deduce the two following bounds, which are similar to the ones of Proposition 21 and Corollary 24.

- $\deg(h_{i,j}) \le d_{\boldsymbol{y}}(\deg(b_i) + \deg(b_j))$;
- The degree of any minor of $\mathcal{H}$ is bounded by $d_{\boldsymbol{y}}\; n(d-1)d^n$.

Even though these bounds are not sharp anymore, they still allow us to compute the parametric Hermite matrices using evaluation & interpolation scheme and control the complexity of this computation in the instances where Assumption (C) does not hold.

6.2. Complexity analysis of our algorithms

In this subsection, we analyze the complexity of our algorithms on generic systems.

Let $\boldsymbol{f} = (f_1, \dots, f_n) \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ be a regular sequence, where $\boldsymbol{y} = (y_1, \dots, y_t)$ and $\boldsymbol{x} = (x_1, \dots, x_n)$, satisfying Assumptions (A) and (C). To simplify the asymptotic complexity, we assume that n, t and d are greater than or equal to 2.

We denote by $\mathcal{G}$ the reduced Gröbner basis of $\boldsymbol{f}$ with respect to the ordering $\mathsf{grevlex}(\boldsymbol{x}) \succ \mathsf{grevlex}(\boldsymbol{y})$. The basis $\mathcal{B}$ is taken as all the monomials in $\boldsymbol{x}$ that are irreducible by $\mathcal{G}$. Then, $\mathcal{H}$ is the parametric Hermite matrix associated of $\boldsymbol{f}$ with respect to $\mathcal{B}$.

We start by estimating the arithmetic complexity for computing the parametric Hermite matrix $\mathcal{H}$ and its minors. We denote $\lambda \coloneqq n(d-1)$ and $\mathfrak{D} \coloneqq n(d-1)d^n$.

Proposition 26. Assume that $\boldsymbol{f} = (f_1, \dots, f_n) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ is a regular sequence that satisfies Assumptions (A) and (C). Let δ be the dimension of the $\mathbb{K}$-vector space $\mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ where $\mathbb{K} = \mathbb{Q}(\boldsymbol{y})$. Let $\mathcal{H}$ be the parametric Hermite matrix associated to $\boldsymbol{f}$ constructed using $\mathsf{grevlex}(\boldsymbol{x})$ ordering. Then, by Lemma 7, the entries of the parametric Hermite matrix $\mathcal{H}$ lie in $\mathbb{Q}[\boldsymbol{y}]$.

Using the evaluation & interpolation scheme, one can compute $\mathcal{H}$ within

$$O^{\sim}\left(\binom{t+2\lambda}{t}\left(n\binom{d+n+t}{n+t} + n^{\omega+1}d^{\omega n+1} + d^{(\omega+1)n}\right)\right)$$

arithmetic operations in $\mathbb{Q}$, where, by Bézout's bound, δ is bounded by d^n.

Moreover, each minor (including the determinant) of $\mathcal{H}$ can be computed using

$$O^{\sim}\left(\binom{t+\mathfrak{D}}{t}\left(d^{2n}\binom{t+2\lambda}{t} + d^{\omega n}\right)\right)$$

arithmetic operations in $\mathbb{Q}$.

Proof. By Lemma 23 and Proposition 21, the highest degree among the entries of $\mathcal{H}$ is bounded by $2\lambda = 2n(d-1)$. The evaluation & interpolation scheme of Subsection 4.4 requires computing $\binom{t+2\lambda}{t}$ specialized Hermite matrices. We first analyze the complexity for computing each of those specialized Hermite matrices.

The evaluation of $\boldsymbol{f}$ at each point $\eta \in \mathbb{Q}^t$ costs $O\left(n\binom{d+n+t}{n+t}\right)$ arithmetic operations in $\mathbb{Q}$.

As the highest degree in the Gröbner basis of $\boldsymbol{f}(\eta, \cdot)$ w.r.t. the $\mathsf{grevlex}(\boldsymbol{x})$ ordering is bounded by $n(d-1)+1$, the computation of this Gröbner basis can be done within $O(nd^{\omega n})$ arithmetic operations in $\mathbb{Q}$ (see [16, Theorem 5.1]).

Next, we compute the matrices representing the $\mathcal{L}_{x_i}$'s. Using [16, Algo. 4], we obtain an arithmetic complexity of $O\left(dn^{\omega+1}\delta^{\omega}\right)$ ([16, Prop. 5]) for computing such n matrices, where ω is the exponential constant for matrix multiplication. Using $\delta \leq d^n$, we obtain the bound $O\left(n^{\omega+1}d^{\omega n+1}\right)$.

The traces of these matrices are then computed using $n\delta$ additions in $\mathbb{Q}$. The subroutine BMatrices consists of essentially δ multiplication of $\delta \times \delta$ matrices (with entries in $\mathbb{Q}$). This leads to an arithmetic complexity $O(\delta^{\omega+1})$, which is then bounded by $O(d^{(\omega+1)n})$. Next, the computation of each entry $h_{i,j}$ is simply a vector multiplication of length δ, whose complexity is $O(\delta)$. Doing so for δ^2 entries, TraceComputing takes in overall $O(\delta^3)$ arithmetic operations in $\mathbb{Q}$.

Thus, as $\delta \leq d^n$, the complexity of the evaluation step lies in

$$O\left(\binom{t+2\lambda}{t}\left(n\binom{d+n+t}{n+t} + n^{\omega+1}d^{\omega n+1} + d^{(\omega+1)n}\right)\right).$$

Finally, we interpolate δ^2 entries which are polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree at most 2λ. Using the multivariate interpolation algorithm of [8], the complexity of this step therefore lies in $O\left(\delta^2\binom{t+2\lambda}{t}\log^2\binom{t+2\lambda}{t}\log\log\binom{t+2\lambda}{t}\right)$.

Summing up the both steps, we conclude that the parametric Hermite matrix $\mathcal{H}$ can be obtained within

$$O\tilde{~}\left(\binom{t+2\lambda}{t}\left(n\binom{d+n+t}{n+t} + n^{\omega+1}d^{\omega n+1} + d^{(\omega+1)n}\right)\right)$$

arithmetic operations in $\mathbb{Q}$.

Similarly, the minors of $\mathcal{H}$ can be computed using the technique of evaluation & interpolation. By Corollary 24, the degree of every minor of $\mathcal{H}$ is bounded by $\mathfrak{D}$. We specialize $\mathcal{H}$ at $\binom{t+\mathfrak{D}}{t}$ points in $\mathbb{Q}^t$ and compute the corresponding minor of each specialized Hermite matrix. This step takes

$$O\left(\binom{t+\mathfrak{D}}{t}\left(\delta^2\binom{t+2\lambda}{t} + \delta^{\omega}\right)\right)$$

arithmetic operations in $\mathbb{Q}$. Finally, using the multivariate interpolation algorithm of [8], it requires

$$O\left(\binom{t+\mathfrak{D}}{t}\log^2\binom{t+\mathfrak{D}}{t}\log\log\binom{t+\mathfrak{D}}{t}\right)$$

arithmetic operations in $\mathbb{Q}$ to interpolate the final minor. Therefore, using $\delta \leq d^n$, the whole complexity for computing each minor of $\mathcal{H}$ lies within

$$O\tilde{~}\left(\binom{t+\mathfrak{D}}{t}\left(d^{2n}\binom{t+2\lambda}{t} + d^{\omega n}\right)\right).$$

$\square$

We note that the complexity of computing the matrix $\mathcal{H}$ in Proposition 26 is also bounded by the complexity of computing its minor. Indeed, we have that

$$\begin{aligned}\binom{d+n+t}{n+t} &= \frac{(d+n+t)\dots(d+n+1)(d+n)\dots(d+1)}{(n+t)!}\\ &\le \frac{(d+n+t)\dots(d+n+1)}{t!}\,\frac{(d+n)\dots(d+1)}{n!}\\ &\le \frac{(\mathfrak{D}+t)\dots(\mathfrak{D}+1)}{t!}(2d^n) = \binom{\mathfrak{D}+t}{t}(2d^n).\end{aligned}$$

Asymptotically, $n^{\omega}d^{\omega n+1}$ is bounded by $O^{\sim}\left(d^{(\omega+1)n}\right)$. For $t \ge 2$, $\binom{t+\mathfrak{D}}{t} \ge \mathfrak{D}^2/2 \ge d^{(\omega-1)n}$. Hence, we obtain

$$\binom{t+2\lambda}{t}\left(n\binom{d+n+t}{n+t} + n^{\omega+1}d^{\omega n+1} + d^{(\omega+1)n}\right) \in O^{\sim}\left(\binom{t+2\lambda}{t}\binom{t+\mathfrak{D}}{t}d^{2n}\right),$$

which proves our claim above.

Finally, we state our main result, which is Theorem I below. It estimates the arithmetic complexity of Algorithms 2 and 3.

Theorem I. Let $\boldsymbol{f} \subset \mathbb{Q}[\boldsymbol{x},\boldsymbol{y}]$ be a regular sequence such that the ideal $\langle \boldsymbol{f} \rangle$ is radical and $\boldsymbol{f}$ satisfies Assumptions (A) and (C). Recall that $\mathfrak{D}$ denotes $n(d-1)d^n$. Then, we have the following statements:

i) The arithmetic complexity of Algorithm 2 lies in

$$O^{\sim}\left(\binom{t+\mathfrak{D}}{t}\, 2^{3t}\; n^{2t+1}d^{2nt+n+2t+1}\right).$$

ii) Algorithm 3, which is probabilistic, computes a set of semi-algebraic descriptions solving Problem (1) within

$$O^{\sim}\left(\binom{t+\mathfrak{D}}{t}\, 2^{3t}\; n^{2t+1}d^{3nt+2(n+t)+1}\right)$$

arithmetic operations in $\mathbb{Q}$ in case of success.

iii) The semi-algebraic descriptions output by Algorithm 3 consist of polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree bounded by $\mathfrak{D}$.

Proof. As Assumption (C) holds, we have that $\boldsymbol{w}_{\infty} = 1$ and $\boldsymbol{w}_{\mathcal{H}}$ is the square-free part of $\det(\mathcal{H})$.

Therefore, after computing the parametric Hermite matrix $\mathcal{H}$ and its determinant, whose complexity is given by Proposition 26, Algorithm 2 essentially consists of computing sample points of the connected components of the algebraic set $\mathbb{R}^t \setminus V(\det(\mathcal{H}))$.

By Corollary 24, the degree of $\det(\mathcal{H})$ is bounded by $\mathfrak{D}$. Applying Corollary 3, we obtain the following arithmetic complexity for this computation of sample points

$$O^{\sim}\left(\binom{t+\mathfrak{D}}{t}\, 2^{3t}\mathfrak{D}^{2t+1}\right) \simeq O^{\sim}\left(\binom{t+\mathfrak{D}}{t}\, 2^{3t}\; n^{2t+1}d^{2nt+n+2t+1}\right).$$

Also by Corollary 3, the finite subset of $\mathbb{Q}^t$ output by SamplePoints has cardinal bounded by $2^t\mathfrak{D}^t$. Thus, evaluating the specializations of $\mathcal{H}$ at those points and their signatures costs in total $O\left(2^t\mathfrak{D}^t\left(\delta^2\binom{2\lambda+t}{t}+\delta^{\omega+1/2}\right)\right)$ arithmetic operations in $\mathbb{Q}$ using [4, Algorithm 8.43].

Therefore, the complexity of SamplePoints dominates the whole complexity of the algorithm. We conclude that Algorithm 2 runs within

$$O^{\sim}\left(\binom{t+\mathfrak{D}}{t}2^{3t}\ n^{2t+1}d^{2nt+n+2t+1}\right)$$

arithmetic operations in $\mathbb{Q}$.

For Algorithm 3, we start by choosing randomly a matrix A and compute the matrix $\mathcal{H}_A = A^T\cdot\mathcal{H}\cdot A$. Then, we compute the leading principal minors $M_1,\dots,M_\delta$ of $\mathcal{H}_A$. Using Proposition 26, this step admits the arithmetic complexity bound

$$O^{\sim}\left(\delta\binom{t+\mathfrak{D}}{t}\left(d^{2n}\binom{t+2\lambda}{t}+d^{\omega n}\right)\right).$$

Next, Algorithm 3 computes sample points for the connected components of the semi-algebraic set defined by $\wedge_{i=1}^{\delta}M_i\neq 0$. Since the degree of each M_i is bounded by $\mathfrak{D}$, Corollary 3 gives the arithmetic complexity

$$O^{\sim}\left(\binom{t+\mathfrak{D}}{t}d^{nt+n}\ 2^{3t}\ \mathfrak{D}^{2t+1}\right)\simeq O^{\sim}\left(\binom{t+\mathfrak{D}}{t}2^{3t}\ n^{2t+1}d^{3nt+2(n+t)+1}\right).$$

It returns a finite subset of $\mathbb{Q}^t$ whose cardinal is bounded by $(2\delta\mathfrak{D})^t$. The evaluation of the leading principal minors' sign patterns at those points has the arithmetic complexity lying in $O\left(2^t\delta^{t+1}\mathfrak{D}^{2t}\right)\simeq O\left(2^tn^{2t}d^{3nt+n+2t}\right)$.

Again, the complexity of SamplePoints dominates the whole complexity of Algorithm 3. The proof of Theorem I is then finished. ☐

Probability aspect. The main probabilistic source of our algorithms 2 and 3 comes from the use of the geometric resolution [26] in the computation of sample points per connected components described in Section 3. Since the geometric resolution depends on the specialization and lifting procedures, it makes use of various random choices. As explained in [26], the bad choices are enclosed in strict algebraic subsets of certain affine spaces, which implies that almost any random choice leads to a correct computation. In general, even though one can check whether the points output by geometric resolution are solutions of the input system, some solutions can be missing. Thus, the geometric resolution is not Las Vegas.

Besides, Algorithm 3 depends also on the choice of the matrix Q. By Lemma 18, any choice of Q from a prescribed dense Zariski open subset of $\mathrm{GL}(n,\mathbb{C})$ will work. As the purpose of choosing Q is to ensure that none of the leading principal minors of $Q^T\cdot\mathcal{H}\cdot Q$ are identically zero. One can check easily whether a good matrix Q is found.

7. Practical implementation & Experimental results

7.1. Remark on the implementation of Algorithm 3

Recall that Algorithm 3 leads us to compute sample points per connected components of the non-vanishing set of the leading principal minors $(M_1,\dots,M_\delta)$. Comparing to

Algorithm 2 in which we only compute sample points for $\mathbb{R}^t \setminus V(M_\delta)$, the complexity of Algorithm 3 contains an extra factor of d^{nt} due to the higher number of polynomials given as input to the subroutine SamplePoints. Even though the complexity bounds of these two algorithms both lie in $d^{O(nt)}$, the extra factor d^{nt} mentioned above sometimes becomes the bottleneck of Algorithm 3 for tackling practical problems. Therefore, we introduce the following optimization in our implementation of Algorithm 3.

We start by following exactly the steps (1-4) of Algorithm 3 to obtain the leading principal minors $(M_1, \ldots, M_\delta)$ and the polynomial $\boldsymbol{w}_\infty$. Then, by calling the subroutine SamplePoints on the input $M_\delta \neq 0 \wedge \boldsymbol{w}_\infty \neq 0$, we compute a set of sample points (and their corresponding numbers of real roots) $\{(\eta_1, r_1), \ldots, (\eta_\ell, r_\ell)\}$ that solves the weak-version of Problem (1). We obtain from this output all the possible numbers of real roots that the input system can admit.

For each value $0 \leq r \leq \delta$, we define

$$\Phi_r = \{\sigma = (\sigma_1, \ldots, \sigma_\delta) \in \{-1, 1\}^\delta \mid \text{ the sign variation of } \sigma \text{ is } (\delta - r)/2\}.$$

If $r \not\equiv \delta \pmod 2$, $\Phi_r = \emptyset$.

For $\sigma \in \Phi_r$ and $\eta \in \mathbb{R}^t \setminus V(\boldsymbol{w}_\infty)$ such that $\mathbf{sign}\,(M_i(\eta)) = \sigma_i$ for every $1 \leq i \leq \delta$, the signature of $\mathcal{H}(\eta)$ is r. As a consequence, for any η in the semi-algebraic set defined by

$$(\boldsymbol{w}_\infty \neq 0) \wedge (\vee_{\sigma \in \Phi_r} (\wedge_{i=1}^{\delta} \mathrm{sign}\,(M_i) = \sigma_i)),$$

the system $\boldsymbol{f}(\eta, .)$ has exactly r distinct real solutions.

Therefore, $(\mathcal{S}_{r_i})_{1 \leq i \leq \ell}$ is a collection of semi-algebraic sets solving Problem (1). Then, we can simply return $\{(\Phi_{r_i}, \eta_i, r_i) \mid 1 \leq i \leq \ell\}$ as the output of Algorithm 3 without any further computation. Note that, by doing so, we may return sign conditions which are not realizable.

We discuss now about the complexity aspect of the steps described above. For $r \equiv \delta \pmod 2$, the cardinal of Φ_r is $\binom{\delta}{(\delta - r - 2)/2}$. In theory, the total cardinal of all the Φ_{r_i}'s $(1 \leq i \leq \ell)$ can go up to $2^{\delta - 1}$, which is doubly exponential in the number of variables n. However, in the instances that are actually tractable by the current state of the art, 2^δ is still smaller than δ^{3t}. And when it is the case, following this approach has better performance than computing the sample points of the semi-algebraic set defined by $\wedge_{i=1}^{\delta} M_i \neq 0$. Otherwise, when 2^δ exceeds δ^{3t}, we switch back to the computation of sample points.

This implementation of Algorithm 3 does not change the complexity bound given in Theorem I.

7.2. Implementation infrastructure

To implement our algorithm, we need three main ingredients: (i) Gröbner bases computations, in order to obtain monomial basis of quotient algebras that we use to compute our parametrized Hermite matrices, (ii) an implementation of an algorithm computing sample points connected components of semi-algebraic sets, (iii) a computer algebra system to manipulate polynomials and matrices.

In our implementation, we use the Maple computer algebra system and its programming language to implement the overall algorithm. We use J.-Ch Faugère's FGb library [21], implemented in C, for computing Gröbner bases.

In order to compute sample points per connected components of semi-algebraic sets, we use the RAGlib [40] (Real Algebraic Library) package which is implemented using the Maple programming language and the FGb library. The algorithm implemented therein is the one of [19] and its complexity remains to be established. Even if they share similar ingredients, it is not the same as the one of Section 3 which provides the state-of-the-art complexity result for this problem. Hence, our implementation might not meet the best promised by complexity results. Still, we see in the experiments below that it already can tackle problems which are out of reach of the current software state-of-the-art.

7.3. Experiments

This subsection provides numerical results of several algorithms related to the real root classification. We report on the performance of each algorithm for different test instances.

The computation is carried out on a computer of Intel(R) Xeon(R) CPU E7-4820 2GHz and 1.5 TB of RAM. The timings are given in seconds (s.), minutes (m.) and hours (h.). The symbol ∞ means that the computation cannot finish within 120 hours.

Throughout this subsection, the column hermite reports on the computational data of our algorithms based on parametric Hermite matrices described in Section 5. It uses the notations below:

- mat: the timing for computing a parametric Hermite matrix $\mathcal{H}$.
- det: the runtime for computing the determinant of $\mathcal{H}$.
- min: the timing for computing the leading principal minors of $\mathcal{H}$.
- sp: the runtime for computing at least one points per each connected component of the semi-algebraic set $\mathbb{R}^t \setminus V(\det(\mathcal{H}))$.
- deg: the highest degree among the leading principal minors of $\mathcal{H}$.

Generic systems. In this paragraph, we report on the results obtained with generic inputs, i.e., randomly chosen dense polynomials $(f_1, \ldots, f_n) \subset \mathbb{Q}[y_1, \ldots, y_t][x_1, \ldots, x_n]$. The total degrees of input polynomials are given as a list $d = [\deg(f_1), \ldots, \deg(f_n)]$.

We first compare the algorithms using Hermite matrices (Section 5) with the folklore Sturm-based algorithm sketched in the introduction for solving Problem (1). The column sturm of Fig. (1) shows the experimental results of the Sturm-based algorithm. It contains the following sub-columns:

- elim: the timing for computing the eliminating polynomial.
- sres: the timing for computing the subresultant coefficients in the Sturm-based algorithm.
- sp-s: the timing for computing sample points per connected components of the non-vanishing set of the last subresultant coefficient.
- deg-s: the highest degree among the subresultant coefficients.

We observe that the sum of mat-h and min-h is smaller than the sum of elim and sres. Hence, obtaining the input for the sample point computation in hermite strategy is easier than in sturm strategy. We also remark that the degree deg-h is much smaller than deg-s, that explains why the computation of sample points using Hermite matrices is faster than using the subresultant coefficients.

We conclude that the parametric Hermite matrix approach outperforms the Sturm-based one both on the timings and the degree of polynomials in the output formulas.

t	d	hermite					sturm				
		mat	min	sp	total	deg	elim	sres	sp-s	total	deg-s
2	$[2,2]$	.07 s	.01 s	.3 s	.4 s	8	.01 s	.1 s	2 s	2.2 s	12
2	$[3,2]$	.1 s	.12 s	4.8 s	5 s	18	.05 s	.5 s	15 s	16 s	30
2	$[2,2,2]$	.3 s	.3 s	33 s	34 s	24	.08 s	2 s	8 m	8 m	56
2	$[3,3]$	.3 s	.8 s	3 m	3 m	36	.1 s	3 s	20 m	20 m	72
3	$[2,2]$	.1 s	.02 s	26 s	27 s	8	.07 s	.1 s	40 s	40 s	12
3	$[3,2]$	.2 s	.2 s	3 h	3 h	18	.1 s	1 s	∞	∞	30
3	$[2,2,2]$	.5 s	7 s	32 h	32 h	24	.15 s	10 m	∞	∞	56
3	$[4,2]$	.6 s	12 s	90 h	90 h	32	.2 s	12 m	∞	∞	56
3	$[3,3]$	1 s	27 s	∞	∞	36	.2 s	15 m	∞	∞	72

Figure 1: Generic random dense systems

In Fig. (2), we compare our algorithm using parametric Hermite matrices with two Maple packages for solving parametric polynomial systems: RootFinding[Parametric] [22] and RegularChains[ParametricSystemTools] [48]. The new notations used in Fig. (2) are explained below.

- The column rf stands for the RootFinding[Parametric] package. To solve a parametric polynomial systems, it consists of computing a discriminant variety $\mathcal{D}$ and then computing an open CAD of $\mathbb{R}^t \setminus \mathcal{D}$. This package does not return explicit semi-algebraic formulas but an encoding based on the real roots of some polynomials.

  This column contains:

  - dv : the runtime of the command DiscriminantVariety that computes a set of polynomials defining a discriminant variety $\mathcal{D}$ associated to the input system.
  - cad : the runtime of the command CellDecomposition that outputs semi-algebraic formulas by computing an open CAD for the semi-algebraic set $\mathbb{R}^t \setminus \mathcal{D}$.

- The column rc stands for the RegularChains[ParametricSystemTools] package of Maple. The algorithms implemented in this package is given in [48]. It also contains two sub-columns:

  - bp : the runtime of the command BorderPolynomial that returns a set of polynomials.

- rrc : the runtime of the command RealRootClassification. We call this command with the option output='samples' to compute at least one point per connected component of the complementary of the real algebraic set defined by border polynomials.

Note that, in a strategy for solving the weak-version of Problem (1), DiscriminantVariety and BorderPolynomial can be completely replaced by parametric Hermite matrices.

On generic systems, the determinant of our parametric Hermite matrix coincides with the output of DiscriminantVariety, which we denote by $\boldsymbol{w}$. Whereas, because of the elimination BorderPolynomial returns several polynomials, one of them is $\boldsymbol{w}$.

In Fig. (2), the timings for computing a parametric Hermite matrix is negligible. Comparing the columns det, dv and bp, we remark that the time taken to obtain $\boldsymbol{w}$ through the determinant of parametric Hermite matrices is much smaller than using DiscriminantVariety or BorderPolynomial.

For computing the polynomial $\boldsymbol{w}$, using parametric Hermite matrices allows us to reach the instances that are out of reach of DiscriminantVariety, for example, the instances $\{t = 3,\ d = [2,2,2]\}$, $\{t = 3\ d = [4,2]\}$, $\{t = 3,\ d = [3,3]\}$ and $\{t = 4,\ d = [2,2]\}$ in Fig. (2) below. Moreover, we succeed to compute the semi-algebraic formulas for $\{t = 3,\ d = [2,2,2]\}$, $\{t = 3\ d = [4,2]\}$ and $\{t = 4,\ d = [2,2]\}$. Using the implementation in Subsection 7.1, we obtain the semi-algebraic formulas of degrees bounded by $\deg(\boldsymbol{w})$.

Therefore, for these generic systems, our algorithm based on parametric Hermite matrices outperforms DiscriminantVariety and BorderPolynomial for obtaining a polynomial that defines the boundary of semi-algebraic sets over which the number of real solutions are invariant. Moreover, using the minors of parametric Hermite matrices, we can compute semi-algebraic formulas of problems that are out of reach of CellDecomposition and RealRootClassification.

t	d	hermite					rf			rc		
		mat	det	sp	total	deg	dv	cad	total	bp	rrc	total
2	$[2,2]$	.07 s	.01 s	.3 s	.4 s	8	.1 s	.3 s	.4 s	.1 s	1 s	1.1 s
2	$[3,2]$	.1 s	.2 s	4.8 s	5 s	18	1 m	5 s	1 m	.3 s	12 s	12 s
2	$[2,2,2]$	.3 s	.3 s	33 s	34 s	24	17m	32 s	17m	23 s	2 m	2 m
2	$[3,3]$	.3 s	.8 s	3 m	3 m	36	2 h	4 m	2 h	8 s	4 m	4 m
3	$[2,2]$	.1 s	.02 s	26 s	27 s	8	1 s	35 s	36 s	.2 s	12m	12m
3	$[3,2]$	.2 s	.2 s	3 h	3 h	18	2 h	84 h	86 h	3 s	37 h	37 h
3	$[2,2,2]$	.5 s	7 s	32 h	32 h	24	∞	∞	∞	20m	∞	∞
3	$[4,2]$	.6 s	12 s	90 h	90 h	32	∞	∞	∞	12m	∞	∞
3	$[3,3]$	.7 s	27 s	∞	∞	36	∞	∞	∞	15m	∞	∞
4	$[2,2]$	.2 s	.1 s	8 m	8 m	8	4 s	∞	∞	1 s	∞	∞

Figure 2: Generic random dense systems

In what follows, we consider the systems coming from some applications as test instances. These examples allow us to observe the behavior of our algorithms on non-generic systems.

Kuramoto model. This application is introduced in [34], which is a dynamical system used to model synchronization among some given coupled oscillators. Here we consider only the model constituted by 4 oscillators. The maximum number of real solutions of steady-state equations of this model was an open problem before it is solved in [28] using numerical homotopy continuation methods. However, to the best of our knowledge, there is no exact algorithm that is able to solve this problem. We present in what follows the first solution using symbolic computation. Moreover, our algorithm can return the semi-algebraic formulas defining the regions over which the number of real solutions is invariant.

As explained in [28], we consider the system $\boldsymbol{f}$ of the following equations

$$\begin{cases} y_i - \sum_{j=1}^{4}(s_i c_j - s_j c_i) & = 0 \\ s_i^2 + c_i^2 & = 1 \end{cases} \quad \text{for } 1 \leq i \leq 3,$$

where (s_1, s_2, s_3) and (c_1, c_2, c_3) are variables and (y_1, y_2, y_3) are parameters. We are asked to compute the maximum number of real solutions of $\boldsymbol{f}(\eta, .)$ when η varies over $\mathbb{R}^3$. This leads us to solve the weak version of Problem (1) for this parametric system.

We first construct the parametric Hermite matrix $\mathcal{H}$ associated to this system. This matrix is of size 14×14. The polynomial $\boldsymbol{w}_\infty$ has the factors $y_1 + y_2$, $y_2 + y_3$, $y_3 + y_1$ and $y_1 + y_2 + y_3$. The polynomial $\boldsymbol{w}_{\mathcal{H}}$ has degree 48 (c.f. [28]). We denote by $\boldsymbol{w}$ the polynomial $\boldsymbol{w}_\infty \cdot \boldsymbol{w}_{\mathcal{H}}$.

Note that the polynomial system has real roots only if $|y_i| \leq 3$ (c.f. [28]). So we only need to consider the compact connected components of $\mathbb{R}^3 \setminus V(\boldsymbol{w})$. Since the polynomial $\boldsymbol{w}$ is invariant under any permutation acting on (y_1, y_2, y_3), we exploit this symmetry to accelerate the computation of sample points.

Following the critical point method, we compute the critical points of the map $(y_1, y_2, y_3) \mapsto y_1 + y_2 + y_3$ restricted to $\mathbb{R}^3 \setminus V(\boldsymbol{w})$; this map is also symmetric. We apply the change of variables

$$(y_1, y_2, y_3) \mapsto (e_1, e_2, e_3),$$

where $e_1 = y_1 + y_2 + y_3$, $e_2 = y_1 y_2 + y_2 y_3 + y_3 y_1$ and $e_3 = y_1 y_2 y_3$ are elementary symmetric polynomials of (y_1, y_2, y_3). This change of variables reduces the number of distinct solutions of zero-dimensional systems involved in the computation and, therefore, reduces the computation time.

From the sample points obtained by this computation, we derive the possible number of real solutions and conclude that the system $\boldsymbol{f}$ has at most 10 distinct real solutions when (y_1, y_2, y_3) varies over $\mathbb{R}^3 \setminus V(\boldsymbol{w})$. This agrees with the result given in [28]. We show below a list of parameter values such that the system has respectively 2, 4, 6, 8 and 10 distinct real solutions.

Number of solutions	(y_1, y_2, y_3)
2 solutions	$[-2, -0.03, 0.22]$
4 solutions	$[1, -0.09, 0.16]$
6 solutions	$[0, -0.7, -0.48]$
8 solutions	$[0.08, -0.03, 0.22]$
10 solutions	$\left[\frac{274945023031}{2199023255552}, \frac{-68723139707}{549755813888}, \frac{-549808278091}{4398046511104}\right]$

Fig. (3) reports on the timings for computing the parametric Hermite matrix (mat), for computing its determinant (det) and for computing the sample points (sp). We stop both of the commands DiscriminantVariety and BorderPolynomial after 240 hours without obtaining the polynomial $\boldsymbol{w}$.

hermite				dv	bp
mat	det	sp	total		
2 m	1 h	85 h	86 h	∞	∞

Figure 3: Kuramoto model for 4 oscillators

Static output feedback. The second non-generic example comes from the problem of static output feedback [29]. Given the matrices $A \in \mathbb{R}^{\ell\times\ell}$, $B \in \mathbb{R}^{\ell\times 2}$, $C \in \mathbb{R}^{1\times\ell}$ and a parameter vector $P = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \in \mathbb{R}^2$, the characteristic polynomial of $A + BPC$ writes

$$f(s, \boldsymbol{y}) = \det(sI_l - A - BKC) = f_0(s) + y_1 f_1(s) + y_2 f_2(s),$$

where s is a complex variable.

We want to find a matrix P such that all the roots of $f(s, \boldsymbol{y})$ must lie in the open left half-plane. By substituting s by $x_1 + ix_2$, we obtain the following system of real variables (x_1, x_2) and parameters (y_1, y_2):

$$\begin{cases} \Re(f(x_1 + ix_2, \boldsymbol{y})) & = 0 \\ \Im(f(x_1 + ix_2, \boldsymbol{y})) & = 0 \\ x_1 & < 0 \end{cases}$$

Note that the total degree of these equations equals ℓ.

We are now interested in solving the weak-version of Problem (1) on the system $\Re(f) = \Im(f) = 0$. We observe that this system satisfies Assumptions (A) and (B). Let $\mathcal{H}$ be the parametric Hermite matrix $\mathcal{H}$ of this system with respect to the usual basis we consider in this paper. This matrix $\mathcal{H}$ behaves very differently from generic systems.

Computing the determinant of $\mathcal{H}$ (which is an element of $\mathbb{Q}[\boldsymbol{y}]$) and taking its square-free part allows us to obtain the same output $\boldsymbol{w}$ as DiscriminantVariety. However, this direct approach appears to be very inefficient as the determinant appears as a large power of the output polynomial.

For example, for a value ℓ, we observe that the system consists of two polynomials of degree ℓ. The determinant of $\mathcal{H}$ appears as $\boldsymbol{w}^{2\ell}$, where $\boldsymbol{w}$ has degree $2(\ell - 1)$. The bound we establish on the degree of this determinant is $2(\ell - 1)\ell^2$, which is much larger than what happens in this case. Therefore, we need to introduce the optimization below to adapt our implementation of Algorithm 2 to this problem.

We observe that, on these examples, the polynomial $\boldsymbol{w}$ can be extracted from a smaller minor instead of computing the determinant $\mathcal{H}$. To identify such a minor, we reduce $\mathcal{H}$ to a matrix whose entries are univariate polynomials with coefficients lying in a finite field $\mathbb{Z}/p\mathbb{Z}$ as follow.

Let u be a new variable. We substitute each y_i by random linear forms in $\mathbb{Q}[u]$ in $\mathcal{H}$ and then compute $\mathcal{H} \bmod p$. Then, the matrix $\mathcal{H}$ is turned into a matrix $\mathcal{H}_u$ whose entries are elements of $\mathbb{Z}/p\mathbb{Z}[u]$. The computation of the leading principal minors of $\mathcal{H}_u$ is much easier than the one of $\mathcal{H}$ since it involves only univariate polynomials and does not suffer from the growth of bit-sizes as for the rational numbers.

Next, we compute the sequence of the leading principal minors of $\mathcal{H}_u$ in decreasing order, starting from the determinant. Once we obtain a minor, of some size r, that is not divisible by $\overline{\boldsymbol{w}}_u$, we stop and take the index $r+1$. Then, we compute the square-free part of the $(r+1)\times(r+1)$ leading principal minor of $\mathcal{H}$, which can be done through evaluation-interpolation method. This yields a Monte Carlo implementation that depends on the choice of the random linear forms in $\mathbb{Q}[u]$ and the finite field to compute the polynomial $\boldsymbol{w}$.

In Fig. (4), we report on some computational data for the static output feedback problem. Here we choose the prime p to be 65521 so that the elements of the finite field $\mathbb{Z}/p\mathbb{Z}$ can be represented by a machine word of 32 bits. We consider different values of ℓ and the matrices A, B, C are chosen randomly. On these examples, our algorithm returns the same output as the one of DisciminantVariety. Whereas, BorderPolynomial (bp) returns a list of polynomials which contains our output and other polynomials of higher degree.

The timings of our algorithm are given by the two following columns:

- The column mat shows the timings for computing parametric Hermite matrices $\mathcal{H}$.
- The column comp-w shows the timings for computing the polynomials $\boldsymbol{w}$ from $\mathcal{H}$ using the strategy described as above.

We observe that our algorithm (mat + comp-w) wins some constant factor comparing to DiscriminantVariety (dv). On the other hand, BorderPolynomial (bp) performs less efficiently than the other two algorithms in these examples.

Since the degrees of the polynomials $\boldsymbol{w}$ here (given as deg-w) are small comparing with the bounds in the generic case. Hence, unlike the generic cases, the computation of the sample points in these problems is negligible as being reported in the column sp.

ℓ	hermite			dv	bp	sp	deg-w
	mat	comp-w	total				
5	2 s	1 s	3 s	30 s	1.5 m	.2 s	8
6	12 s	5 s	17 s	90 s	30 m	.4 s	10
7	1 m	6 m	7 m	16 m	4 h	1 s	12
8	4 m	50 m	1 h	1.5 h	34 h	3 s	14

Figure 4: Static output feedback

Acknowledgments. We thank the anonymous reviewers for their comments which helped to improve a lot the initial submission.

References

[1] Alman, J., Williams, V. V., 2021. A refined laser method and faster matrix multiplication. In: Proceedings of the Thirty-Second Annual ACM-SIAM Symposium on Discrete Algorithms. SODA '21. Society for Industrial and Applied Mathematics, USA, p. 522–539.

[2] Bardet, M., Dec. 2004. Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie. Theses, Université Pierre et Marie Curie - Paris VI.

[3] Bardet, M., Faugère, J.-C., Salvy, B., 2015. On the complexity of the F5 Gröbner basis algorithm. Journal of Symbolic Computation 70, 49–70.

[4] Basu, S., Pollack, R., Roy, M.-F., 2006. Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics). Springer-Verlag, Berlin, Heidelberg.

[5] Bayer, D., Stillman, M., 06 1987. A theorem on refining division orders by the reverse lexicographic order. Duke Math. J. 55 (2), 321–328.

[6] Bonnard, B., Faugère, J.-C., Jacquemard, A., Safey El Din, M., Verron, T., 2016. Determinantal sets, singularities and application to optimal control in medical imagery. In: Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation. pp. 103–110.

[7] Brown, C. W., Davenport, J. H., 2007. The complexity of quantifier elimination and cylindrical algebraic decomposition. In: Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation. ISSAC '07. Association for Computing Machinery, New York, NY, USA, p. 54–60.

[8] Canny, J. F., Kaltofen, E., Yagati, L., 1989. Solving systems of nonlinear polynomial equations faster. In: Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation. ISSAC '89. Association for Computing Machinery, New York, NY, USA, p. 121–128.

[9] Collins, G. E., 1976. Quantifier elimination for real closed fields by cylindrical algebraic decomposition: a synopsis. ACM SIGSAM Bulletin 10 (1), 10–12.

[10] Corvez, S., Rouillier, F., 2002. Using computer algebra tools to classify serial manipulators. In: International Workshop on Automated Deduction in Geometry. Springer, pp. 31–43.

[11] Coste, M., Shiota, M., dec 1992. Thom's first isotopy lemma: a semialgebraic version, with uniform bounds(real singularities and real algebraic geometry). RIMS Kokyuroku 815, 176–189.

[12] Cox, D. A., Little, J., O'Shea, D., 2007. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics). Springer-Verlag, Berlin, Heidelberg.

[13] Dahan, X., Schost, É., 2004. Sharp estimates for triangular sets. In: Gutierrez, J. (Ed.), Symbolic and Algebraic Computation, International Symposium ISSAC 2004, Santander, Spain, July 4-7, 2004, Proceedings. ACM, pp. 103–110.

[14] Davenport, J. H., Heintz, J., Feb. 1988. Real quantifier elimination is doubly exponential. J. Symb. Comput. 5 (1–2), 29–35.

[15] Elliott, J., Giesbrecht, M., Schost, É., 2020. On the bit complexity of finding points in connected components of a smooth real hypersurface. In: Emiris, I. Z., Zhi, L. (Eds.), ISSAC '20: International Symposium on Symbolic and Algebraic Computation, Kalamata, Greece, July 20-23, 2020. ACM, pp. 170–177.

[16] Faugère, J., Gaudry, P., Huot, L., Renault, G., 2013. Polynomial systems solving by fast linear algebra. CoRR abs/1304.6039.

[17] Faugere, J.-C., 1999. A new efficient algorithm for computing Gröbner bases (F4). Journal of pure and applied algebra 139 (1-3), 61–88.

[18] Faugère, J. C., 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of the 2002 international symposium on Symbolic and algebraic computation. pp. 75–83.

[19] Faugère, J.-C., Moroz, G., Rouillier, F., Safey El Din, M., 2008. Classification of the perspective-three-point problem, discriminant variety and real solving polynomial systems of inequalities. In: Proceedings of the twenty-first international symposium on Symbolic and algebraic computation. pp. 79–86.

[20] Faugère, J.-C., Safey El Din, M., Spaenlehauer, P.-J., 2013. On the complexity of the generalized minrank problem. Journal of Symbolic Computation 55, 30–58.

[21] Faugère, J.-C., September 2010. FGb: A Library for Computing Gröbner Bases. In: Fukuda, K., Hoeven, J., Joswig, M., Takayama, N. (Eds.), Mathematical Software - ICMS 2010. Vol. 6327 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, Berlin, Heidelberg, pp. 84–87.

[22] Gerhard, J., Jeffrey, D. J., Moroz, G., Jun. 2010. A package for solving parametric polynomial systems. ACM Commun. Comput. Algebra 43 (3/4), 61–72.

[23] Ghys, É., Ranicki, A., 2016. Signatures in algebra, topology and dynamics. Ensaios Matemáticos 30, 1 – 173.

[24] Gianni, P. M., Teo Mora, T., 1987. Algebraic solution of systems of polynomial equations using Gröebner bases. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 5th Inter-

national Conference, AAECC-5, Menorca, Spain, June 15-19, 1987, Proceedings. pp. 247–257.

[25] Giusti, M., Heintz, J., Morais, J. E., Pardo, L. M., 1995. When polynomial equation systems can be "solved" fast? In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 11th International Symposium, AAECC-11, Paris, France, July 17-22, 1995, Proceedings. pp. 205–231.

[26] Giusti, M., Lecerf, G., Salvy, B., 2001. A gröbner free alternative for polynomial system solving. Journal of complexity 17 (1), 154–211.

[27] Hardt, R. M., 1980. Semi-algebraic local-triviality in semi-algebraic mappings. American Journal of Mathematics 102 (2), 291–302.

[28] Harris, K., Hauenstein, J. D., Szanto, A., 2020. Smooth points on semi-algebraic sets.

[29] Henrion, D., Sebek, M., 2008. Plane geometry and convexity of polynomial stability regions. In: Proceedings of the Twenty-First International Symposium on Symbolic and Algebraic Computation. ISSAC '08. Association for Computing Machinery, New York, NY, USA, p. 111–116.

[30] Hermite, C., 1856. Sur le nombre des racines d'une équation algébrique comprises entre des limites données. extrait d'une lettre á m. borchardt. J. Reine Angew. Math. 52, 39–51.

[31] Jacobi, C. G., 1857. Uber eine elementare transformation eins in bezug auf jedes von zwei variablensystemen linearen und homogenen ausdrucks. Journal fur die reine und angewandte Mathematik 53., 265 – 270.

[32] Kalkbrener, M., 1997. On the stability of gröbner bases under specializations. Journal of Symbolic Computation 24 (1), 51–58.

[33] Kronecker, L., 1882. Grundzüge einer arithmetischen theorie der algebraischen grössen. Journal für die reine und angewandte Mathematik 92, 1–122.

[34] Kuramoto, Y., 1975. Self-entrainment of a population of coupled non-linear oscillators. In: Araki, H. (Ed.), International Symposium on Mathematical Problems in Theoretical Physics. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 420–422.

[35] Lazard, D., Rouillier, F., 2007. Solving parametric polynomial systems. Journal of Symbolic Computation 42 (6), 636–667.

[36] Moreno-Socıas, G., 2003. Degrevlex gröbner bases of generic complete intersections. Journal of Pure and Applied Algebra 180 (3), 263 – 283.

[37] Pardue, K., 2010. Generic sequences of polynomials. Journal of Algebra 324 (4), 579 – 590.

[38] Pedersen, P., Roy, M.-F., Szpirglas, A., 1993. Counting real zeros in the multivariate case. In: Eyssette, F., Galligo, A. (Eds.), Computational Algebraic Geometry. Birkhäuser Boston, Boston, MA, pp. 203–224.

[39] Rouillier, F., 1999. Solving zero-dimensional systems through the rational univariate representation. Appl. Algebra Eng. Commun. Comput. 9 (5), 433–461.

[40] Safey El Din, M., 2017. Real alebraic geometry library, raglib (version 3.4).
URL https://www-polsys.lip6.fr/~safey/RAGLib/

[41] Safey El Din, M., Schost, E., 2003. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In: Proc. of the 2003 Int. Symp. on Symb. and Alg. Comp. ISSAC '03. ACM, NY, USA, p. 224–231.

[42] Safey El Din, M., Schost, É., Jan. 2017. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. J. ACM 63 (6), 48:1–48:37.

[43] Safey El Din, M., Schost, E., 2018. Bit complexity for multi-homogeneous polynomial system solving—application to polynomial minimization. Journal of Symbolic Computation 87, 176 – 206.

[44] Schost, É., 2003. Computing parametric geometric resolutions. Applicable Algebra in Engineering, Communication and Computing 13 (5), 349–393.

[45] Shafarevich, I. R., 2013. Basic Algebraic Geometry 1: Varieties in Projective Space. Springer Berlin Heidelberg, Berlin, Heidelberg.

[46] Sylvester, J. J., 1852. A demonstration of the theorem that every homogeneous quadratic polynomial is reducible by real orthogonal substitution to the form of a sum of positive and negative squares. Philosophical Magazine IV., 138 – 142.

[47] Verron, T., Sep. 2016. Regularisation of Gröbner basis computations for weighted and determinantal systems, and application to medical imagery. Theses, Université Pierre et Marie Curie - Paris VI.

[48] Yang, L., Hou, X., Xia, B., 2001. A complete algorithm for automated discovering of a class of inequality-type theorems. Science in China Series F Information Sciences 44 (1), 33–49.

[49] Yang, L., Xia, B., 2005. Real solution classification for parametric semi-algebraic systems. In: Dolzmann, A., Seidl, A., Sturm, T. (Eds.), Algorithmic Algebra and Logic. Proceedings of the A3L 2005, April 3-6, Passau, Germany; Conference in Honor of the 60th Birthday of Volker Weispfenning. pp. 281–289.

[50] Yang, L., Zeng, Z., 2000. Equi-cevaline points on triangles. In: Computer Mathematics: Proceedings

of the Fourth Asian Symposium (ASCM 2000). World Scientific Publishing Company Incorporated, p. 130.

[51] Yang, L., Zeng, Z., 2005. An open problem on metric invariants of tetrahedra. In: Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation. ISSAC '05. Association for Computing Machinery, New York, NY, USA, p. 362–364.