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

Huu Phuoc Le, Mohab Safey El Din

SOLVING PARAMETRIC SYSTEMS OF POLYNOMIAL EQUATIONS OVER THE REALS THROUGH HERMITE MATRICES

Huu Phuoc Le
Sorbonne Université, CNRS,
Laboratoire d'Informatique de Paris 6, LIP6,
Équipe POLSYS
F-75252, Paris Cedex 05, France
huu-phuoc.le@lip6.fr

Mohab Safey El Din
Sorbonne Université, CNRS,
Laboratoire d'Informatique de Paris 6, LIP6,
Équipe POLSYS
F-75252, Paris Cedex 05, France
mohab.safey@lip6.fr

November 28, 2020

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

[†]Mohab Safey El Din and Huu Phuoc Le are supported by the ANR grants ANR-18-CE33-0011 SESAME, and ANR-19-CE40-0018 DE RERUM NATURA, the joint ANR-FWF ANR-19-CE48-0015 ECARP project, the PGMO grant CAMISADO and the European Union's Horizon 2020 research and innovative training network program under the Marie Skłodowska-Curie grant agreement N° 813211 (POEMA).

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 $\boldsymbol{y}$

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

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 (Hardt, 1980), 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.

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 $\mathcal{V} \cap \pi^{-1}(\eta_j)$.

Example 2. *Consider the equation $x^2 + y_1 x + y_2 = 0$ where y_1 and y_2 are the parameters and x is the unique variable. While $y_1^2 - 4y_2 \neq 0$, this equation always has exactly two distinct complex solutions. On the other hand, its number of distinct real solutions can take any value from 0 to 2, depending on the sign of the discriminant $y_1^2 - 4y_2$. One possible output for Problem (1) on this toy example is the following:*

$$\begin{cases} y_1^2 - 4y_2 < 0, & (0,1), \quad 0 \text{ real solution} \\ y_1^2 - 4y_2 = 0, & (2,1), \quad 1 \text{ real solution} \\ y_1^2 - 4y_2 > 0, & (1,0), \quad 2 \text{ real solutions} \end{cases}$$

Observe that another possible output is

$$\begin{cases} y_1^2 - 4y_2 < 0, & (0,1), \quad 0 \text{ real solution} \\ y_1^2 - 4y_2 > 0, & (1,0), \quad 2 \text{ real solutions} \end{cases}$$

as the above two inequalities define semi-algebraic sets whose union is dense in $\mathbb{R}^2$.

Problem (1) appears in many areas of engineering sciences such as robotics or medical imagery (see, e.g., Yang and Zeng (2000); Corvez and Rouillier (2002); Yang and Zeng (2005); Faugère et al. (2008); Bonnard et al. (2016)). In those applications, the behavior of mechanisms or complex systems depends on intrinsic parameters that are related by polynomial equations or inequalities. Thus, the polynomial systems arising from those applications are naturally parametric and most of the time the end-user is interested in classifying the number of real roots with respect to parameters' values.

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 Collins (1976). 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 (Davenport and Heintz, 1988; Brown and Davenport, 2007) 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 Yang and Xia (2005) (the h_i's are called *border polynomials*) and Lazard and Rouillier (2007) (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 (Yang and Xia, 2005) and (Lazard and Rouillier, 2007) 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.

That being said, 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 (Coste and Shiota, 1992) that one can choose $\cup_{i=1}^r V(h_i)$ to be the set critical values of the restriction of π to $\mathcal{V}$ (see e.g. Bonnard et al. (2016)). 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. (Basu et al., 2006, 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 (Basu et al., 2006, 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 $n(d-1)d^n$. At this stage of our exposition, this is not clear that it is doable.

We describe in detail our contributions in the next paragraph but we can already state that, when $\boldsymbol{f}$ enjoys some genericity properties that are made clear further, the algorithm we design outputs semi-algebraic formulas involving polynomials of degree bounded by $n(d-1)d^n$ and which are computed using $(n(d-1)d^n)^{O(t)}$ arithmetic operations in $\mathbb{Q}$.

To achieve these results, we revisit tools for univariate real root counting, such as Sturm and Sturm-Habicht sequences and Hermite's quadratic form to adapt them in our multivariate setting. This leads us to mention González-Vega et al. (1998); Liang et al. (2008) or Henrion (2010) which provide algorithms for classifying the real roots of a univariate polynomial with coefficients in $\mathbb{Q}[\boldsymbol{y}]$, hence restricted to the case where $n = 1$ (either using Sturm-based techniques or Hermite's quadratic forms).

1.3 Main results

We start by revisiting Sturm-based methods in a multivariate context. We basically use the algorithm of Schost (2003) to compute a rational parametrization of $\mathcal{V} = V(\boldsymbol{f})$ with respect to the $\boldsymbol{x}$-variables. More precisely, we compute a sequence of polynomials $(w, v_1, \ldots, v_n)$ 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

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

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 $(w, v_1, \ldots, v_n)$, is Zariski dense in $\mathcal{V}$, i.e., the Zariski closure of $\mathcal{Z}$ coincides with $\mathcal{V}$.

Then, using the bi-rational equivalence between $\mathcal{Z}$ and its projection on the $(u, \boldsymbol{y})$-space, we establish that semi-algebraic formulas solving Problem (1) can be obtained through the computation of the subresultant sequence associated to $\left(w, \frac{\partial w}{\partial u}\right)$. This is admittedly *folklore* in symbolic computation but, as far as we know, is not explicitly written in the literature. In particular, the analysis of degree bounds derived from this strategy is one of our contributions.

Before stating our first complexity result, we need to introduce the complexity model which is used. Throughout this paper, we measure only the arithmetic complexity of algorithms, i.e., the number of arithmetic operations $+, -, \times, \div$, in the base field $\mathbb{Q}$. 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 $O\tilde{}$ 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 $O\left(N^\omega\right)$ arithmetic operations in $\mathbb{Q}$. The value of ω can be bounded from above by 2.3729, which is a recent result established in Le Gall (2014).

Under some genericity assumptions on the input system, Theorem I establishes the complexity result of our Sturm-based algorithm and also the degree bound for polynomials involved in the semi-algebraic formulas solving Problem (1) obtained this way. Its proof is given in Section 4, where all the genericity assumptions are clarified.

Theorem I. *Let $\boldsymbol{f} = (f_1, \ldots, f_n) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ be a generic parametric system and d be the largest total degree among the $\deg(f_i)$'s.*

Then, there exists a probabilistic algorithm that computes semi-algebraic descriptions of a set of semi-algebraic sets solving Problem 1 within

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

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

These semi-algebraic formulas computed by this algorithm involve polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree bounded by $2d^{2n}$.

When reporting experimental results, we will see that, even though the complexity bound we obtain lies in $d^{O(nt)}$, this approach does not allow us to solve problems faster than the state-of-the-art. One bottleneck comes from the fact that the polynomials of the output semi-algebraic formulas have degree way higher than the bound $n(d-1)d^n$ which we will prove to apply under the same assumptions as Theorem I using different algorithmic strategies.

Note that the above Sturm-based approach as well as the ones which consist in computing polynomials in $\mathbb{Q}[\boldsymbol{y}]$ to define a set discriminating semi-algebraic sets in $\mathbb{R}^t$ enjoying the properties needed to solve Problem (1) combine two steps of algebraic elimination. The semi-algebraic formulas are obtained through intermediate data who have been obtained through an elimination step.

The rest of the paper then focuses on an alternative approach which computes semi-algebraic formulas solving Problem (1) by avoiding interlaced algebraic elimination steps. We will see (as announced earlier) that under genericity assumptions, this allows us to obtain a degree bound and an arithmetic cost which are better than the Sturm-based algorithm by one order of magnitude.

To do that, we rely on well-known properties of *Hermite quadratic forms* to count the real roots of zero-dimensional ideals ; see (Hermite, 1856). Basically, given a zero-dimensional ideal $I \subset \mathbb{Q}[\boldsymbol{x}]$, Hermite's quadratic form operates on the finite dimensional $\mathbb{Q}$-vector space $A := \mathbb{Q}[\boldsymbol{x}]/I$ as follows

$$\begin{aligned} A \times A &\to \mathbb{Q} \\ (h, k) &\mapsto \operatorname{trace}(\mathcal{L}_{h \cdot k}), \end{aligned}$$

where $\mathcal{L}_{h \cdot k}$ denotes the endomorphism $p \mapsto h \cdot k \cdot p$ of A.

The number of distinct real (resp. complex) roots of the algebraic set defined by I equals the signature (resp. rank) of Hermite's quadratic form ; see e.g. (Basu et al., 2006, Theorem 4.102). Recall that such quadratic form is represented by a symmetric matrix of size $\delta \times \delta$, where δ is the degree of I, once a basis of the finite dimensional vector space on which the form operates is fixed. Hence, the signature of a Hermite quadratic form can be computed once a matrix representation, which we call Hermite's matrix, of this quadratic form is known (Basu et al., 2006, Algo. 8.43).

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. (Basu et al., 2006, Chap. 12) and references therein) which are adapted to obtain practically fast algorithms following Safey El Din and Schost (2003). 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

$$O^{\sim}\left(\binom{D+t}{t}(2t)^4 s^{t+1} 2^{3t} D^{2t+1}\right).$$

(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 Lazard and Rouillier (2007) or the border polynomials of Yang et al. (2001). We will see in the section reporting experiments that our approach outperforms the other twos on every example we consider.

To return semi-algebraic formulas, we follow a slightly different routine:

(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 $\wedge_{i=1}^{\delta} M_i \neq 0$ where the M_i's are the leading principal minors of $\mathcal{H}$. Again, this is done by the algorithm given in Section 3.

(c) For $1 \leq i \leq \ell$, evaluate the sign pattern of $(M_1, \ldots, M_\delta)$ at the sample point η_i. From this sign pattern, we obtain a semi-algebraic formula representing the connected component corresponding to η_i.

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

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 (Kalkbrener, 1997). 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 Bayer and Stillman (1987); Bayer and Stillman (1987). Further, we denote by $grevlex(\boldsymbol{x})$ the graded reverse lexicographical ordering applied to the sequence of the variables $\boldsymbol{x} = (x_1, \ldots, x_n)$ (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. In particular, it 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 7.2, where the generic assumptions in use are given explicitly.

Theorem II. *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 II 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.

Organization of the paper This paper is structured as follows. Section 2 reviews fundamental notions of algebraic geometry and the theory of Gröbner bases that we use further. In Section 4, we discuss an algorithm based on Sturm's theorem for computing semi-algebraic formulas of the set $\mathcal{S}_i$. This provides an overview on the drawbacks and potential improvements of this approach. Section 5 lies the definition and some useful properties of parametric Hermite matrices. There, we also present an algorithm with some optimizations to compute such a matrix. In Section 6, 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 7. Finally, in Section 8, 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. This notion is the foundation of many algorithms in semi-algebraic geometry such as computing sample points of connected components (Bank et al., 2001; Safey El Din and Schost, 2003; Bank et al., 2005), polynomial optimization (Safey El Din, 2008; Guo et al., 2010) or answering connectivity queries using roadmaps (Safey El Din and Schost, 2011; Basu and Roy, 2014; Basu et al., 2014; Safey El Din and Schost, 2017). Next, we give the definitions of regular sequences, Hilbert series, Noether position and proper maps, which are used later in Subsection 7.1 for the complexity analysis of our algorithms. The fourth paragraph recalls some basic properties of Gröbner bases and quotient algebras of zero-dimensional ideals. We refer to Cox et al. (2007) 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. The zero-dimensional parametrization goes back to Kronecker (1882) and is widely used in computer algebra (see e.g. Gianni and Teo Mora (1987); Giusti et al. (2001, 1995)) to represent finite algebraic sets. In Section 3, the output of our algorithm for computing points per connected components of the non-vanishing locus of a given set of polynomials is encoded by this parametrization. On the other hand, the rational parametrization, which generalizes the notion of zero-dimensional parametrizations, is introduced in Schost (2003) as the data representation for the parametric geometric resolution algorithm. In Section 4, we compute a rational parametrization of the input system using the algorithm of Schost (2003) to reduce Problem (1) to the univariate case.

Algebraic sets and critical points We consider a sub-field $\mathbb{F}$ of $\mathbb{C}$. Let I be a polynomial ideal of $\mathbb{F}[x_1,\ldots,x_n]$, 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 $I(\mathcal{V}) \subset \mathbb{C}[x_1,\ldots,x_n]$ 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 $\varphi_1, \ldots, \varphi_t \in \mathbb{C}[x_1, \ldots, x_n]$ such that the $\varphi(\eta) = (\varphi_1(\eta), \ldots, \varphi_s(\eta))$ 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

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

and $\mathcal{V} \subset \mathbb{C}^n$ be a smooth equi-dimensional algebraic set. We denote by $\mathrm{crit}(\phi, \mathcal{V})$ 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 $\mathrm{crit}(\phi, \mathcal{V})$ 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., (Safey El Din and Schost, 2017, 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 equals 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

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

When I can be generated by a homogeneous regular sequence $(f_1, \ldots, f_m)$, the explicit form of the Hilbert series of I is known (see, e.g., Moreno-Socıas (2003)):

$$\mathrm{HS}_I(z) = \frac{\prod_{i=1}^{m} \left(1 - z^{\deg(f_i)}\right)}{(1-z)^n}.$$

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 (Bardet, 2004, 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 (Bardet, 2004, 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 Bardet et al. (2015)).

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 $\mathbb{R}^t$.

Example 3. *We consider the ideal $\langle x^2 + y^2 - 1 \rangle$. One can easily see that x is in Noether position with respect to this ideal as the equation $x^2 + y^2 - 1$ is monic in x.*

On the other hand, the variable x is not in Noether position with respect to the ideal $\langle xy-1\rangle$. This can be observed geometrically as the fiber at $y=0$ of the projection of $V(xy-1)$ to the y-space lies in infinity.

Another example is the ideal $\langle yx^2+2x-1\rangle$. The variable x is not in Noether position with respect to this ideal. The fiber at $y=0$ of the projection of $V(yx^2+2x-1)$ to the y-space contains a point $(1/2,0)$ and a point at infinity. So, this projection is not proper.

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, Cox et al. (2007)) 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 (Cox et al., 2007, 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 (Basu et al., 2006, 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 sequence of polynomials $(w,v_1,\ldots,v_n)\in(\mathbb{Q}[u])^{n+1}$ with a new variable u and $(a_1,\ldots,a_n)\in\mathbb{Q}^n$ such that w is square-free and $u=(\sum_{i=1}^n a_i\cdot v_i/w')\bmod w$. The solution set of $\mathscr{R}$, defined as

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

is finite and is denoted by $Z(\mathscr{R})$.

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 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 Dahan and Schost (2004)).

Rational parametrizations We consider now a parametric system $\boldsymbol{f}\in\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ where $\boldsymbol{y}=(y_1,\ldots,y_t)$ are parameters and $\boldsymbol{x}=(x_1,\ldots,x_n)$ are variables. Under some extra assumptions on the system $\boldsymbol{f}$, (Schost, 2003, Theorem 1) proves the existence of a sequence $(w,v_1,\ldots,v_n)\subset(\mathbb{Q}(\boldsymbol{y})[u])^n$ with a new variable u and a Zariski open subset $\mathcal{Y}\subset\mathbb{C}^t$ such that

- w is a square-free polynomial in $\mathbb{Q}(\boldsymbol{y})[u]$.
- $u=\sum_{i=1}^n a_ix_i$ for some $(a_1,\ldots,a_n)\in\mathbb{Q}^n$.
- For $\eta\in\mathcal{Y}$, η does not cancel any denominator of $(w,v_1,\ldots,v_n)$ and

$$V(\boldsymbol{f}(\eta,\cdot))=\left\{\left(\frac{v_1}{\partial w/\partial u}(\eta,\vartheta),\ldots,\frac{v_n}{\partial w/\partial u}(\eta,\vartheta)\right)\;\middle|\; w(\eta,\vartheta)=0,\frac{\partial w}{\partial u}(\eta,\vartheta)\neq 0\right\}.$$

The sequence $(w,v_1,\ldots,v_n)$ is called a *rational parametrization* of $\boldsymbol{f}$. It can be computed using the parametric geometric resolution algorithm which is described in Schost (2003).

Intuitively, this parametrization provides a generic description for the solutions of $\boldsymbol{f}(\eta, \cdot)$ when η ranges over $\mathbb{C}^t$. It generalizes the notion of zero-dimensional parametrizations to the parametric setting.

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 III. *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 $\mathscr{R}_1, \ldots, \mathscr{R}_k$ encodes at most $(2sD)^t$ points such that $\cup_{i=1}^k Z(\mathscr{R}_i)$ meets every connected component of $\mathcal{S}$ using

$$O^{\sim}\left(\binom{D+t}{t}(2t)^4 s^{t+1} 2^{3t} D^{2t+1}\right).$$

arithmetic operations in $\mathbb{Q}$.

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

Proof. By (Faugère et al., 2008, Lemma 1), there exists a non-empty Zariski open set $\mathcal{A} \times \mathcal{E} \subset \mathbb{C}^s \times \mathbb{C}$ such that for $(\boldsymbol{a} = (a_1, \ldots, a_s), e) \in \mathcal{A} \times \mathcal{E} \cap \mathbb{R}^s \times \mathbb{R}$, 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 (Basu et al., 2006, 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 Safey El Din and Schost (2003). 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 $(y_1, \ldots, y_t) \to (y_1, \ldots, y_i)$ (π_0 will simply denote $(y_1, \ldots, y_t) \to \{\bullet\}$). By slightly abusing notation, we will also denote by π_i projections from $\mathfrak{V}_{\boldsymbol{a},\varepsilon}^{\mathcal{I},\sigma}$ 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 $\mathrm{crit}(\pi_i, V)$ for $1 \leq i \leq \ell$. By (Safey El Din and Schost, 2003, Theorem 2), for a generic choice of $M \in \mathrm{GL}_t(\mathfrak{K})$, 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 $V^M \cap \mathfrak{K}^t$. 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 (Safey El Din and Schost, 2017, App. B)).

Recall that D denotes 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 (Safey El Din and Schost, 2018, Theorem 1) combined with the degree estimates in (Safey El Din and Schost, 2018, 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 $\mathrm{crit}(\pi_i, V_{\boldsymbol{a},\varepsilon}^{\mathcal{I},\sigma})$ of critical points of the restriction of π_i to $V_{\boldsymbol{a},\varepsilon}^{\mathcal{I},\sigma}$. Note that these systems have coefficients in $\mathbb{Q}[\varepsilon]$. To solve such systems, we rely on Schost (2003), which consists in specializing ε to a generic value $e \in \mathbb{Q}$ 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 (Schost, 2003, Corollary 1) and multi-homogeneous bounds on the degree of the critical points of π_i to $\mathfrak{V}_{\boldsymbol{a},\varepsilon}^{\mathcal{I},\sigma}$ as in (Safey El Din and Schost, 2018, 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 Schost (2003), 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

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

we need to compute 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

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

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

$$O^{\sim}\left(\Gamma\ (2t)^4\ s^t\ 2^{3t}\ D^{2t+1}\right).$$

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

$$O^{\sim}\left(\binom{D+t}{t} (2t)^4\ s^{t+1}\ 2^{3t}\ D^{2t+1}\right).$$

□

We end this section with a Corollary which is a consequence of the proof of (Basu et al., 2006, Theorem 13.18). Basically, once we have the parametrizations computed by the algorithm on which Theorem III 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 (Basu et al., 2006, Prop. 10.22). Hence, the proof of the corollary below follows *mutatis mutandis* the same steps as the one of (Basu et al., 2006, Theorem 13.18).

Corollary 4. *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

$$O^{\sim}\left(\binom{D+t}{t} (2t)^4 s^{t+1} 2^{3t} D^{2t+1}\right).$$

arithmetic operations in $\mathbb{Q}$.

4 Sturm based classical algorithm

In this section, we describe an algorithm based on Sturm's theorem for solving Problem (1) and discuss its shortcomings.

We consider a sequence $\boldsymbol{f} = (f_1, \ldots, f_m) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ where $\boldsymbol{y} = (y_1, \ldots, y_t)$ and $\boldsymbol{x} = (x_1, \ldots, x_n)$. Let d be an upper bound of the total degree of the f_i's. We require that the input system $\boldsymbol{f}$ satisfies the properties below.

Assumption B. *Let $\boldsymbol{f}$ be the above parametric polynomial system and $\mathcal{V}$ be the algebraic set defined by $\boldsymbol{f}$. We say that $\boldsymbol{f}$ satisfies Assumptions (B) if the following properties hold.*

- (B1) *The ideal generated by $\boldsymbol{f}$ is radical.*
- (B2) *The algebraic set $\mathcal{V}$ is equi-dimensional of dimension t.*
- (B3) *The restriction of $\pi : (\boldsymbol{y}, \boldsymbol{x}) \mapsto \boldsymbol{y}$ to $\mathcal{V}$ is dominant.*

It is well-known that the above assumptions are satisfied by sufficiently generic systems (see e.g. Safey El Din and Schost (2018)).

In what follows, we rely on the existence of a parametric geometric resolution (Schost, 2003) to reduce our initial multivariate problem to a univariate one.

Using (Schost, 2003, Proposition 2) with Assumption (B1), there exists a non-empty open Zariski set $\mathcal{A}$ of $\mathbb{C}^n$ such that, for $(a_1, \ldots, a_n) \in \mathbb{Q}^n \cap \mathcal{A}$, there exists a parametric geometric resolution $(w_{\boldsymbol{a}}, v_1, \ldots, v_n) \subset (\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}])^n$ of $\boldsymbol{f}$ that satisfies the following properties.

- $w_{\boldsymbol{a}}$ is a square-free polynomial in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$.
- $u = \sum_{i=1}^n a_i x_i$.
- There exists a non-empty Zariski open subset $\mathcal{Y}_{\boldsymbol{a}} \subset \mathbb{C}^t$ such that, for $\eta \in \mathcal{Y}_{\boldsymbol{a}}$, we have that

$$V(\boldsymbol{f}(\eta, \cdot)) = \left\{ \left(\frac{v_1}{\partial w_{\boldsymbol{a}}/\partial u}(\eta, \vartheta), \ldots, \frac{v_n}{\partial w_{\boldsymbol{a}}/\partial u}(\eta, \vartheta) \right) \;\middle|\; w_{\boldsymbol{a}}(\eta, \vartheta) = 0, \frac{\partial w_{\boldsymbol{a}}}{\partial u}(\eta, \vartheta) \neq 0 \right\}.$$

  The set $\mathcal{Y}_{\boldsymbol{a}}$ can be chosen as the set where the leading coefficient of $w_{\boldsymbol{a}}$, the resultant of $w_{\boldsymbol{a}}$ and $\partial w_{\boldsymbol{a}}/\partial u$, and the denominators appearing in the coefficients of $v_1, \ldots, v_n$ do not vanish.

As a consequence, for $\eta \in \mathcal{Y}_{\boldsymbol{a}}$, the number of complex solutions of $\boldsymbol{f}(\eta, \cdot)$ is invariant and equals to the partial degree of $w_{\boldsymbol{a}}$ in u. We denote by D the partial degree of $w_{\boldsymbol{a}}$ in u. By Bézout's inequality (see e.g. Heintz (1983)), D is bounded above by d^n.

Let $\eta \in \mathbb{C}^t$ and $w_{\boldsymbol{a}}(\eta, \cdot)$ be the specialization of the $\boldsymbol{y}$ variables in $w_{\boldsymbol{a}}$ at η. From the existence of such a parametric resolution, we deduce that, for $\eta \in \mathcal{Y}_{\boldsymbol{a}}$, the map $\varphi : (x_1, \ldots, x_n) \mapsto \sum_{i=1}^n a_i x_i$ is a bijection between the complex roots of $\boldsymbol{f}(\eta, \cdot)$ and $w_{\boldsymbol{a}}(\eta, \cdot)$.

Lemma 5. *Let $\boldsymbol{f}$ be a parametric system satisfying Assumption (B) and $w_{\boldsymbol{a}}$ be the eliminating polynomial in the parametric geometric resolution of $\boldsymbol{f}$ as above. Then, we have*

$$V(\langle f_1, \ldots, f_m, u - \sum_{i=1}^n a_i x_i \rangle \cap \mathbb{Q}[\boldsymbol{y}][u]) = V(w_{\boldsymbol{a}}).$$

Consequently, the total degree of $w_{\boldsymbol{a}}$ is at most d^n.

Proof. We prove that, under Assumption (B), there exists a square-free polynomial $w \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ satisfying

$$V(\langle f_1, \ldots, f_m, u - \sum_{i=1}^n a_i x_i \rangle \cap \mathbb{Q}[\boldsymbol{y}][u]) = V(w).$$

Let $\pi_u : \mathbb{C}^{t+n+1} \to \mathbb{C}^{t+1}, (\boldsymbol{y}, \boldsymbol{x}, u) \mapsto (\boldsymbol{y}, u)$ and $\mathcal{V}_u$ be the algebraic set defined by $\langle \boldsymbol{f}, u - \sum_{i=1}^n a_i x_i \rangle$. Note that $\mathcal{V}$ and $\mathcal{V}_u$ are isomorphic taking the map $(\boldsymbol{y}, \boldsymbol{x}) \mapsto (\boldsymbol{y}, \boldsymbol{x}, \sum_{i=1}^n a_i x_i)$ as an isomorphism between them. Then, as the algebraic set $\mathcal{V}$ satisfies Assumption (B), $\mathcal{V}_u$ is equi-dimensional of dimension t and the restriction of $\Pi : \mathbb{C}^{t+n+1} \to \mathbb{C}^t, (\boldsymbol{y}, \boldsymbol{x}, u) \mapsto \boldsymbol{y}$ to $\mathcal{V}_u$ is dominant. Therefore, the Zariski closure of $\pi_u(\mathcal{V}_u)$ is an equi-dimensional algebraic set of dimension t. Hence, there exists a square-free polynomial $w \in \mathbb{Q}[\boldsymbol{y}][u]$ such that $V(w) = \overline{\pi_u(\mathcal{V}_u)}$. Therefore, we obtain $V(\langle f_1, \ldots, f_m, u - \sum_{i=1}^n a_i x_i \rangle \cap \mathbb{Q}[\boldsymbol{y}][u]) = \overline{\pi_u(\mathcal{V}_u)} = V(w)$.

It remains to show that $w_{\boldsymbol{a}}$ equals to w up to a constant. By the definition of parametric geometric resolution, for $\eta \in \mathcal{Y}_{\boldsymbol{a}}$, then $w_{\boldsymbol{a}}(\eta, \cdot)$ and $w(\eta, \cdot)$ share the same complex roots. Therefore, $w_{\boldsymbol{a}}$ equals to w up to a factor in $\mathbb{Q}[\boldsymbol{y}]$. However, both $w_{\boldsymbol{a}}$ and w do not contain such kind of factor by Assumption (B).

By Bézout's inequalities, the degree of $V(f_1, \ldots, f_n, u - \sum_{i=1}^n a_i x_i)$ is at most d^n. Hence, the degree of $\overline{\pi_u(\mathcal{V}_u)}$ is also bounded by d^n. Therefore, the total degree of $w_{\boldsymbol{a}}$ is bounded by d^n. □

Recall that $\mathcal{Y}_{\boldsymbol{a}}$ is the non-empty Zariski open subset of $\mathbb{C}^t$ where the leading coefficient of $w_{\boldsymbol{a}}$, the resultant of $w_{\boldsymbol{a}}$ and $\partial w_{\boldsymbol{a}}/\partial u$, and the denominators appearing in the coefficients of $v_1, \ldots, v_n$ do not vanish. Lemma 6 shows that the numbers of real roots of $\boldsymbol{f}(\eta, \cdot)$ and $w_{\boldsymbol{a}}(\eta, \cdot)$ also coincide over $\mathcal{Y}_{\boldsymbol{a}}$.

Lemma 6. *Let $\mathcal{Y}_{\boldsymbol{a}}$ as above. Then, for $\eta \in \mathcal{Y}_{\boldsymbol{a}} \cap \mathbb{R}^t$, the numbers of real solutions of $w_{\boldsymbol{a}}(\eta, \cdot)$ and $\boldsymbol{f}(\eta, \cdot)$ are equal.*

Proof. Let $\eta \in \mathbb{R}^t \cap \mathcal{Y}_{\boldsymbol{a}}$. By definition of $\mathcal{Y}_{\boldsymbol{a}}$, the restriction of $\varphi : (x_1, \ldots, x_n) \mapsto \sum_{i=1}^n a_i x_i$ to $V(\boldsymbol{f}(\eta, \cdot))$ is a bijection of between the complex roots of $\boldsymbol{f}(\eta, \cdot)$ and $w_{\boldsymbol{a}}(\eta, \cdot)$. As the sequence $\boldsymbol{f}(\eta, \cdot)$ contains polynomials of coefficients in $\mathbb{R}$, the non-real complex roots of $\boldsymbol{f}(\eta, \cdot)$ appears as pairs of conjugate complex points of $\mathbb{C}^n$. Assume that there exists a complex root whose image by φ is a real root of $w_{\boldsymbol{a}}(\eta, \cdot)$, then its conjugate is also mapped to the same real root. This contradicts the bijectivity of φ. Therefore, the numbers of real solutions of $\boldsymbol{f}(\eta, \cdot)$ and $w_{\boldsymbol{a}}(\eta, \cdot)$ coincide. □

For $h \in \mathbb{Q}[\boldsymbol{y}][u]$ of degree D in u, we denote by

$$\Sigma\left(h, \frac{\partial h}{\partial u}\right) = (s_0, \ldots, s_D) \subset \mathbb{Q}[\boldsymbol{y}]$$

the leading coeffients of the subresultant sequence associated to $(h, \partial h/\partial u)$ (see (Basu et al., 2006, Chap. 4)). Here we enumerate this sequence in a way such that s_0 is the leading coefficient of h as a polynomial in u and s_D is the resultant of h and $\partial h/\partial u$.

We recall the specialization property of subresultant coefficients (see e.g. (Basu et al., 2006, Proposition 8.74)). For $\eta \in \mathbb{R}^t$ that does not cancel the leading coefficient of h as a polynomial in u, then the subresultant coefficients of $h(\eta, \cdot)$ and $\partial h(\eta, \cdot)/\partial u$ are exactly the evaluation of $(s_0, \ldots, s_D)$ at η.

By (Basu et al., 2006, Theorem 4.32), the number of real roots of $h(\eta, \cdot)$ equals the generalized permanences minus variations (see (Basu et al., 2006, Notation 4.30)) of $(s_0, \ldots, s_D)_\eta$. Note that this value is uniquely defined upon a sign pattern of $(s_0, \ldots, s_D)_\eta$.

We can now describe Algorithm 1 which takes as input a sequence $\boldsymbol{f} = (f_1, \ldots, f_m) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ satisfying Assumption (B) and it outputs semi-algebraic formulas solving Problem (1).

It uses the following subroutines:

- EliminatingPolynomial which takes as input $\boldsymbol{f}$ and outputs an eliminating polynomial $w_{\boldsymbol{a}}$, i.e., the first polynomial in a parametric geometric resolution of $\boldsymbol{f}$.

  Such an algorithm can be derived from the probabilistic algorithm given in Schost (2003) that computes parametric geometric resolutions.

- SubresultantCoefficients which takes as input $w_{\boldsymbol{a}}$ and outputs $\Sigma(w_{\boldsymbol{a}}, \partial w_{\boldsymbol{a}}/\partial u) = (s_0, \ldots, s_D)$.

  We refer to (Basu et al., 2006, Algo. 8.77) for the explicit description of such an algorithm.

- SamplePoints which takes as input the subresultant coefficients $(s_0, \ldots, s_D) \subset \mathbb{Q}[\boldsymbol{y}]$ and outputs at least one point per connected components of the semi-algebraic set defined by $\{s_i \neq 0 \mid 1 \leq i \leq D,\ s_i \text{ is not a constant}\}$.

  We refer to Section 3 for the explicit description of such an algorithm.

- PermanencesMinusVariations which takes as input a sequence $(s_0, \ldots, s_D)_\eta$ and return its generalized permanences minus variations.

  Using (Basu et al., 2006, Notation 4.30), we can easily design such a subroutine.

Algorithm 1: RRC-Sturm

Input: A parametric system $\boldsymbol{f} \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ satisfying Assumption (B)
Output: Semi-algebraic descriptions solving Problem (1) for the input $\boldsymbol{f}$

$w_{\boldsymbol{a}} \leftarrow$ EliminatingPolynomial$(\boldsymbol{f})$
$(s_0, \ldots, s_D) \leftarrow$ SubresultantCoefficients $(w_{\boldsymbol{a}}, \partial w_{\boldsymbol{a}}/\partial u, u)$
$L \leftarrow$ SamplePoints$(\{s_i \neq 0 \mid 1 \leq i \leq D,\ s_i \text{ is not a constant}\})$
for $\eta \in L$ **do**
    $r_\eta \leftarrow$ PermanencesMinusVariations$((s_0, \ldots, s_D)_\eta)$
end
return $\{(\text{sign}\ (s_0, \ldots, s_D)_\eta, \eta, r_\eta) \mid \eta \in L\}$

Theorem I. *Let $\boldsymbol{f} = (f_1, \ldots, f_n) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ be a parametric system and d be the largest total degree among the $\deg(f_i)$'s. We assume that $\boldsymbol{f}$ satisfies Assumption (B).*

Then, Algorithm 1, which is probabilistic, computes semi-algebraic formulas solving Problem 1 within

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

arithmetic operations in $\mathbb{Q}$. These semi-algebraic formulas contains polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree bounded by $2d^{2n}$.

Proof. We start with the correctness statement. Recall that s_0 is the leading coefficient of $w_{\boldsymbol{a}}$ as a polynomial in u. By (Basu et al., 2006, Proposition 8.74), for $\eta \in \mathbb{C}^t$ that does not cancel s_0, the subresultant coefficients of $w_{\boldsymbol{a}}(\eta, \cdot)$ and $\partial w_{\boldsymbol{a}}(\eta, \cdot)/\partial u$ is the specialization of $(s_0, \ldots, s_D)$ at η. Therefore, from (Basu et al., 2006, Theorem 4.33), the number of real roots of $w_{\boldsymbol{a}}(\eta, \cdot)$ can be derived from the sign of the sequence $(s_0, \ldots, s_D)_\eta$ for $\eta \notin V(s_0)$.

On the other hand, the semi-algebraic set $\mathcal{S}$ defined by $\{s_i \neq 0 \mid 1 \leq i \leq D,\ s_i \text{ is not a constant}\}$ is composed of open semi-algebraic connected components, namely $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$. Over each of them, the subresultant coefficients s_i are sign-invariant. Thus, the number of distinct real roots of $w_{\boldsymbol{a}}(\eta, \cdot)$ is invariant when η varies in $\mathcal{S}_i$ for each $1 \leq i \leq \ell$.

Recall that $\mathcal{Y}_{\boldsymbol{a}} \subset \mathbb{C}^t$ is the non-empty Zariski open set in Lemma 6 such that for $\eta \in \mathcal{Y}_{\boldsymbol{a}}$, the numbers of real roots of $\boldsymbol{f}(\eta, \cdot)$ and $w_{\boldsymbol{a}}(\eta, \cdot)$ coincide. Therefore, the number of real solutions of $\boldsymbol{f}(\eta, \cdot)$ is also invariant when η varies in $\mathcal{S}_i \cap \mathcal{Y}_{\boldsymbol{a}}$.

Let L be the set of sample points of $\mathcal{S}$. We deduce from the above arguments that the semi-algebraic sets defined by $\wedge_{i=1}^{D} \text{sign}\ (s_i) = \text{sign}\ (s_i(\eta))$ for $\eta \in L$ satisfy the requirement of Problem 1. The correctness of our algorithm is then proven.

By Lemma 5, the total degree of $w_{\boldsymbol{a}}$ is bounded above by d^n. Using (Basu et al., 2006, Proposition 8.71) on the polynomial $w_{\boldsymbol{a}}$ and $\partial w_{\boldsymbol{a}}/\partial u$, we obtain the bound $\deg s_j \leq d^n(2j-1) \leq 2d^n$ for $0 \leq j \leq D$.

We are now able to analyze the complexity of Algorithm 1.

By (Schost, 2003, Corollary 1), running EliminatingPolynomial on input $\boldsymbol{f} = (f_1, \ldots, f_n)$ where the total degree of each f_i is bounded by d takes

$$O^{\sim}\left(\binom{4d^n + t}{t} d^n\right)$$

arithmetic operations in $\mathbb{Q}$.

The subresultant coefficients of $w_{\boldsymbol{a}}$ and $\partial w_{\boldsymbol{a}}/\partial u$ can be computed using an evaluation-interpolation scheme as follows. As the degree of s_i is bounded by $2d^{2n}$, we need to compute the subresultant coefficients of the evaluation of $(w_{\boldsymbol{a}}, \partial w_{\boldsymbol{a}}/\partial u)$ at $\binom{t+2d^{2n}}{t}$ distinct points. Note that $\binom{t+2d^{2n}}{t}$ is bounded by $2^t d^{2nt}$.

Using (Basu et al., 2006, Algo. 8.77), it yields an arithmetic complexity $O\left(d^{2n}\right)$ for each of those subresultant computations. Hence, in total, the specialized subresultant coefficients can be computed by $O\left(2^t d^{2nt+2n}\right)$.

Next, the cost of interpolating the s_i's can be bounded by $O^{\sim}\left(D\ 2^t d^{2nt} \log\left(2^t d^{2nt}\right)\right)$ using the interpolation given in Canny et al. (1989). Thus, the arithmetic complexity of SubresultantCoefficients lies in

$$O^{\sim}\left(D\ 2^t d^{2nt} \log\left(2^t d^{2nt}\right)\right).$$

We rely on Corollary 4 for estimating the complexity of SamplePoints. Using the algorithm of Section 3 (see Theorem III and Corollary 4) on the sequence $(s_0, \ldots, s_D)$, one can compute sample points per connected components

of the semi-algebraic set defined by $\{s_i \neq 0 \mid 1 \leq i \leq D,\ s_i \text{ is not a constant}\}$ in time

$$O^{\sim}\left(\binom{t+2d^{2n}}{t} t^4 d^{nt+n} 2^{3t}\ \left(2d^{2n}\right)^{2t+1}\right) \simeq O^{\sim}\left(\binom{t+2d^{2n}}{t} 2^{5t}\ d^{5nt+3n}\right).$$

By Corollary 4, this subroutine outputs a finite subset of $\mathbb{Q}^t$ whose cardinal is bounded by $4^t d^{3nt}$. Using (Basu et al., 2006, Algorithm 9.4) to compute the permanences minus variations leads to a complexity of $O\left(4^t d^{3nt+n}\right)$.

Summing up all the partial costs, we conclude that Algorithm 1 runs within

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

arithmetic operations in $\mathbb{Q}$. □

Example 7. *We will illustrate the algorithms of this paper using the sequence*

$$\boldsymbol{f} = (x_1^2 + x_2^2 - y_1,\ x_1x_2 + y_2x_2 + y_3x_1).$$

We choose $u = x_2$ when running Algorithm 1 (in a reasonable implementation, one would pick randomly a linear form but we choose this one to obtain smaller data).

We obtain the following rational parametrization (w, v_1, v_2) with

$$\begin{aligned}
w &= u^4 + 2y_3u^3 + (y_2^2 + y_3^2 - y_1)u^2 - 2y_1y_3u - y_1y_3^2,\\
v_2 &= 2\,y_3\,u^3 + \left(2\,{y_2}^2 + 2\,{y_3}^2 - 2\,y_1\right)u^2 - 6\,y_1\,y_3\,u - 4\,y_1\,{y_3}^2,\\
v_1 &= 2\,y_2\,u^3 + 2\,y_1\,y_3\,y_2.
\end{aligned}$$

The subresultant coefficients associated to $\left(w, \frac{\partial w}{\partial u}\right)$ are:

$$\begin{aligned}
&s_0 = 1, s_1 = 1, s_2 = -2y_2^2 + y_3^2 + 2y_1,\\
&s_3 = -y_2^6 - 2y_2^4y_3^2 - y_2^2y_3^4 + 3y_1y_2^4 - 14y_1y_2^2y_3^2 + y_1y_3^4 - 3y_1^2y_2^2 - 2y_1^2y_3^2 + y_1^3,\\
&s_4 = (y_2y_3)^2y_1(-y_2^6 - 3y_2^4y_3^2 - 3y_2^2y_3^4 - y_3^6 + 3y_1y_2^4 - 21y_1y_2^2y_3^2 + 3y_1y_3^4 - 3y_1^2y_2^2 - 3y_1^2y_3^2 + y_1^3).
\end{aligned}$$

Since s_0 and s_1 are constants, we then compute at least one point per connected component of the semi-algebraic set defined by

$$s_2 \neq 0 \wedge s_3 \neq 0 \wedge s_4 \neq 0.$$

This is done using e.g. the RAGlib *(Real Algebraic Geometry library) (Safey El Din, 2017). We obtain 35 points and find that the realizable sign conditions for (s_2, s_3, s_4) are*

$$[-1,-1,-1], [-1,-1,1], [-1,1,1], [1,-1,-1], [1,-1,1], [1,1,-1], [1,1,1].$$

Applying (Basu et al., 2006, Theorem 4.32), we deduce the corresponding numbers of real roots to these sign patterns

$$\begin{aligned}
0 \textit{ real root } &\rightarrow (s_2 < 0 \wedge s_3 < 0 \wedge s_4 > 0) \vee (s_2 < 0 \wedge s_3 > 0 \wedge s_4 > 0) \vee (s_2 > 0 \wedge s_3 < 0 \wedge s_4 > 0)\\
2 \textit{ real roots } &\rightarrow (s_2 < 0 \wedge s_3 < 0 \wedge s_4 < 0) \vee (s_2 > 0 \wedge s_3 < 0 \wedge s_4 < 0) \vee (s_2 > 0 \wedge s_3 > 0 \wedge s_4 < 0)\\
4 \textit{ real roots } &\rightarrow s_2 > 0 \wedge s_3 > 0 \wedge s_4 > 0
\end{aligned}$$

Note that the maximum degree of the polynomials involved in the above formulas is 11. By contrast, observe that the restriction of the projection $\pi : (\boldsymbol{y}, \boldsymbol{x}) \rightarrow \boldsymbol{y}$ to the real algebraic set defined by $\boldsymbol{f}$ is proper. Hence, applying a semi-algebraic variant of Thom's isotopy lemma as in (Bonnard et al., 2016), one can deduce that the set of critical values of this map discriminates the regions of the parameters' space over which the number of real roots of $\boldsymbol{f}$ remains invariant.

Using immediate Gröbner bases computations, one obtains that the Zariski closure of this set of critical values is defined by the vanishing of

$$y_1(-y_2^6 - 3y_2^4y_3^2 - 3y_2^2y_3^4 - y_3^6 + 3y_1y_2^4 - 21y_1y_2^2y_3^2 + 3y_1y_3^4 - 3y_1^2y_2^2 - 3y_1^2y_3^2 + y_1^3)$$

which has only degree 7.

5 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*.

5.1 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 (Cox et al., 2007, Section 5.3, Theorem 6). The multiplication maps of $A_{\mathbb{K}}$ are defined as follows.

Definition 8. *For any $p \in \mathbb{K}[\boldsymbol{x}]$, the multiplication map $\mathcal{L}_p$ is defined as*

$$\mathcal{L}_p : \begin{array}{rl} A_{\mathbb{K}} & \to A_{\mathbb{K}}, \\ \overline{q} & \mapsto \overline{p \cdot q}, \end{array}$$

where $\overline{q}$ and $\overline{p \cdot q}$ are respectively the classes of q and $p \cdot q$ in the quotient ring $A_{\mathbb{K}}$.

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 (Basu et al., 2006, 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 9. *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 $1 \leq i \leq n$ 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

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

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

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

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 $1 \leq i \leq n$, 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 9 allows us to apply the construction of Hermite matrices described in (Basu et al., 2006, Chap. 4) to parametric systems as follows.

Since the ideal $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ is zero-dimensional by Lemma 9, 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 10. *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 $H = (h_{i,j})_{1 \leq i,j \leq \delta}$ where $h_{i,j} = \operatorname{trace}(\mathcal{L}_{b_i \cdot b_j})$.*

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.

Example 11. *We consider the same system $\boldsymbol{f} = (x_1^2 + x_2^2 - y_1,\ x_1x_2 + y_2x_2 + y_3x_1)$ as in Example 7. The parametric Hermite matrix associated to $\boldsymbol{f}$ with respect to the basis $B_1 = \{1, x_2, x_1, x_2^2\}$ is*

$$\begin{bmatrix} 4 & -2y_3 & -2y_2 & -2(y_2^2+y_3^2+y_1) \\ * & -2(y_2^2+y_3^2+y_1) & 4y_2y_3 & 2(3y_2^2y_3 - y_3^3) \\ * & * & 2(y_2^2 - y_3^2 + y_1) & 2(y_2^3 - 3y_2y_3^2 - y_1y_2) \\ * & * & * & 2y_2^4 - 12y_2^2y_3^2 + 2y_3^4 - 4y_1y_2^2 + 2y_1^2 \end{bmatrix}.$$

Whereas, using the lexicographical ordering $x_1 \succ x_2$, we obtain the basis $B_2 = \{1, x_2, x_2^2, x_2^3\}$. The matrix associated to $\boldsymbol{f}$ with respect to B_2 is the following Hankel matrix:

$$\begin{bmatrix} 4 & -2y_3 & -2y_2^2 + 2y_3^2 + 2y_1 & 6y_2^2y_3 - 2y_3^3 \\ * & * & * & 2y_2^4 - 12y_2^2y_3^2 + 2y_3^4 - 4y_1y_2^2 + 2y_1^2 \\ * & * & * & -10y_2^4y_3 + 20y_2^2y_3^3 - 2y_3^5 + 10y_1y_2^2y_3 \\ * & * & * & -2y_2^6 + 30y_2^4y_3^2 - 30y_2^2y_3^4 + 2y_3^6 + 6y_1y_2^4 - 18y_1y_2^2y_3^2 - 6y_1^2y_2^2 + 2y_1^3 \end{bmatrix}.$$

We remark that all the entries of the matrices above lie in $\mathbb{Q}[\boldsymbol{y}]$ and that the entries of the second matrix are of higher degree than the first one's.

5.2 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 (Faugere, 1999; Faugère, 2002)).

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 $grevlex(\boldsymbol{x})$ for the grevlex ordering among the variables $\boldsymbol{x}$ (with $x_1 \succ \cdots \succ x_n$) and $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$ (with $y_1 \succ \cdots \succ y_t$) for the elimination ordering. We denote respectively by $\mathrm{lm}_{\boldsymbol{x}}(p)$ and $\mathrm{lc}_{\boldsymbol{x}}(p)$ the leading monomial and the leading coefficient of $p \in \mathbb{K}[\boldsymbol{x}]$ with respect to the ordering $grevlex(\boldsymbol{x})$.

Lemma 12. *Let $\mathcal{G}$ be the reduced Gröbner basis of $\langle \boldsymbol{f} \rangle$ with respect to the elimination ordering $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$. Then $\mathcal{G}$ is also a Gröbner basis of $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ with respect to the ordering $grevlex(\boldsymbol{x})$.*

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 $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ 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 $grevlex(\boldsymbol{x})$ 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 $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$. Let $\mathcal{B}$ be the set of all monomials in $\boldsymbol{x}$ that are not reducible by $\mathcal{G}$, which is finite by Lemmas 9 and 12. 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 C. *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 13. *Under Assumption (C), the entries of the parametric Hermite matrix $\mathcal{H}$ are elements of $\mathbb{Q}[\boldsymbol{y}]$.*

Proof. Since Assumption (C) 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 (C) 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 14 to Subsection 7.1 where we prove a more general result (see Proposition 30).

Proposition 14. *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 (C) is satisfied by any $\boldsymbol{f} \in \mathscr{F}_C \cap \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]^n$.*

5.3 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 $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$ 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 $\boldsymbol{f}(\eta, \cdot) = (\phi_\eta(f_1), \ldots, \phi_\eta(f_m))$. 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 $grevlex(\boldsymbol{x})$ is denoted by $\mathrm{lc}_{\boldsymbol{x}}(p)$. In this subsection, for $p \in \mathbb{C}[\boldsymbol{x}]$, we use $\mathrm{lm}(p)$ to denote the leading monomial of p with respect to the ordering $grevlex(\boldsymbol{x})$.

Let $\mathcal{W}_\infty \subset \mathbb{C}^t$ denote the algebraic set $\cup_{g \in \mathcal{G}} V(\mathrm{lc}_{\boldsymbol{x}}(g))$. In Proposition 16, 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 15 below, which is a direct consequence of (Kalkbrener, 1997, Theorem 3.1), provides the specialization property of $\mathcal{G}$. We give here a more elementary proof for this lemma than the one in Kalkbrener (1997).

Lemma 15. *Let $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$. Then the specialization $\mathcal{G}(\eta, \cdot) \coloneqq \{\phi_\eta(g) \mid g \in \mathcal{G}\}$ 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 $grevlex(\boldsymbol{x})$.*

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

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

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

For any $p \in \langle \boldsymbol{f} \rangle \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$, we prove that $\mathrm{lm}(\phi_\eta(f)) \in \mathcal{M}_G$. 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:

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

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 $grevlex(\boldsymbol{x})$. □

Proposition 16. *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 15, 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. □

Using Proposition 16 and (Basu et al., 2006, 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 17. *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 16, $\mathcal{H}(\eta)$ is a Hermite matrix of the zero-dimensional ideal $\langle \boldsymbol{f}(\eta, \cdot) \rangle$. Then, (Basu et al., 2006, 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 $\boldsymbol{f}(\eta, \cdot)$. □

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 18. *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 (Lazard and Rouillier, 2007, 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 (Shafarevich, 2013, 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. (Cox et al., 2007, 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 $\dim(\overline{\pi(\mathcal{V}_{<t})}) \leq t-1$, 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 12, $\mathcal{G}$ 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 $\eta \notin \mathcal{W}_{\infty}$, 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. □

5.4 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 $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$ 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 5.1. 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 2 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 $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$ 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 (Faugere, 1999; Faugère, 2002).

- 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 $grevlex(\boldsymbol{x})$.

  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 $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$, it is not necessarily the reduced Gröbner basis of $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ with respect to $grevlex(\boldsymbol{x})$. Using (Cox et al., 2007, 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 $grevlex(\boldsymbol{x})$. 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 5.3 (as we have less leading coefficients).

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

  This computation is done directly by reducing every $x_i \cdot b_j$ $(1 \leq i \leq n, 1 \leq j \leq \delta)$ 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 $(1 \leq i \leq \delta)$ 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 Rouillier (1999).

  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

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

  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 2 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 $\mathrm{lcm}_{g \in \mathcal{G}}(\mathrm{lc}_{\boldsymbol{x}}(g))$ for further usage. Note that $V(\boldsymbol{w}_\infty) = \mathcal{W}_\infty$.

Algorithm 2: 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 $\mathcal{B}$

$\mathcal{G}, \mathcal{B} \leftarrow \mathsf{GrobnerBasis}(\boldsymbol{f}, grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y}))$
$\mathcal{G}' \leftarrow \mathsf{ReduceGB}(\mathcal{G})$
$\boldsymbol{w}_\infty \leftarrow \mathsf{sqfree}(\mathrm{lcm}_{g \in \mathcal{G}}(\mathrm{lc}_{\boldsymbol{x}}(g)))$
$(\mathcal{L}_{x_1}, \ldots, \mathcal{L}_{x_n}) \leftarrow \mathsf{XMatrices}(\mathcal{G}', \mathcal{B})$
$(\mathcal{L}_{b_1}, \ldots, \mathcal{L}_{b_\delta}) \leftarrow \mathsf{BMatrices}((\mathcal{L}_{x_1}, \ldots, \mathcal{L}_{x_n}), \mathcal{B})$
$\mathcal{H} \leftarrow \mathsf{TraceComputing}(\mathcal{L}_{b_1}, \ldots, \mathcal{L}_{b_\delta})$
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 6 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 $\mathrm{trace}(\mathcal{L}_{b_i})$ (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 $\{c_i \cdot b_i \mid 1 \le i \le \delta\}$. It usually does not contain any denominator and is handled easier in practice.

Evaluation & interpolation scheme for generic systems Here we assume that the input system $\boldsymbol{f}$ satisfies Assumption (C). By Lemma 13, 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 2) on the input $\boldsymbol{f}(\eta, \cdot)$ to compute the classic Hermite matrix associated to $\boldsymbol{f}(\eta, \cdot)$ with respect to the ordering $grevlex(\boldsymbol{x})$. 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 (C) holds, then $\mathcal{W}_\infty$ is empty. By Proposition 16, the Hermite matrix of $\boldsymbol{f}(\eta, \cdot)$ with respect to $grevlex(\boldsymbol{x})$ 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 Faugère et al. (2013). That algorithm constructs the Macaulay matrix and carries out matrix reductions to obtain simultaneously the normal forms that XMatrices requires.

Assume a degree bound Λ is known, we estimate the arithmetic complexity for computing the parametric Hermite matrix in Proposition 19 below. We postpone to Subsection 7.1 for proving an explicit bound for Λ when the input system satisfies some extra generic assumptions.

Proposition 19. *Assume that the system $\boldsymbol{f} = (f_1, \ldots, f_m) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ satisfying 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 $grevlex(\boldsymbol{x})$ ordering. Then, by Lemma 13, the entries of the parametric Hermite matrix $\mathcal{H}$ lie in $\mathbb{Q}[\boldsymbol{y}]$.*

Let Λ be an upper degree bound of the entries of $\mathcal{H}$. Using the evaluation & interpolation scheme, one can compute $\mathcal{H}$ within

$$O^{\sim}\left(\binom{t+\Lambda}{t}\left(m\binom{d+n+t}{n+t} + \delta^{\omega+1} + \delta^2 \log^2\binom{t+\Lambda}{t}\right)\right)$$

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

Proof. As the degrees of the entries of $\mathcal{H}$ are bounded by Λ. Following the evaluation & interpolation scheme requires one to compute $\binom{t+\Lambda}{t}$ 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 $O\left(m\binom{d+n+t}{n+t}\right)$ arithmetic operations in $\mathbb{Q}$.

Next, we compute the matrices representing the $\mathcal{L}_{x_i}$'s using the linear algebra approach given in Faugère et al. (2013). It yields an arithmetic complexity of $O(n\delta^\omega)$, where ω is the exponential constant for matrix multiplication.

The traces of those 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 $O(\delta^{\omega+1})$. Next, the computation of each entries $h_{i,j}$ is simply a vector multiplication of length δ, whose complexity is $O(\delta)$. Thus, TraceComputing takes in overall $O(\delta^3)$ arithmetic operations in $\mathbb{Q}$.

Thus, every specialized Hermite matrix can be computed using $O(\delta^{\omega+1})$ arithmetic operations in $\mathbb{Q}$. In total, the complexity of the evaluation step lies in $O\left(\binom{t+\Lambda}{t}\left(m\binom{d+n+t}{n+t} + \delta^{\omega+1}\right)\right)$.

Finally, we interpolation δ^2 entries which are polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree at most Λ. Using the multivariate interpolation algorithm of Canny et al. (1989), the complexity of this step therefore lies in $O^{\sim}\left(\delta^2\binom{t+\Lambda}{t}\log^2\binom{t+\Lambda}{t}\right)$.

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

$$O^{\sim}\left(\binom{t+\Lambda}{t}\left(m\binom{d+n+t}{n+t} + \delta^{\omega+1} + \delta^2 \log^2\binom{t+\Lambda}{t}\right)\right)$$

arithmetic operations in $\mathbb{Q}$. □

6 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 6.1 aims to solve the weak version of Problem (1). The second algorithm, given in Subsection 6.2 outputs the semi-algebraic formulas of the cells $\mathcal{S}_i$ that solves Problem (1). Further, in Section 7, 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 $n(d-1)d^n$, which is better than the degree bound $2d^{2n}$ obtained by Algorithm 1 and all previously known bounds.

Throughout this section, our input is a parametric polynomial system $\boldsymbol{f} = (f_1, \ldots, f_m) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$. 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 $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$. 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 $\mathcal{B}$.

6.1 Algorithm for the weak-version of Problem (1)

From Subsection 5.3, 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 16). 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 2. Note that $V(\boldsymbol{w}_\infty) = \mathcal{W}_\infty$.

Lemma 20. *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 9, $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ 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 $\boldsymbol{w}_{\mathcal{H}} := \mathfrak{n} / \gcd(\mathfrak{n}, \boldsymbol{w}_\infty)$ 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 20, $\mathcal{W}_{\mathcal{H}}$ is a proper Zariski closed subset of $\mathbb{C}^t$. Our algorithm relies on the following proposition.

Proposition 21. *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 18, $\mathcal{W}_\infty$ 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 $K(\pi, \mathcal{V}) := \mathrm{sing}(\mathcal{V}) \cup \mathrm{crit}(\pi, \mathcal{V})$. Let $\Delta := \mathrm{jac}(\boldsymbol{f}, \boldsymbol{x})$ 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 16, 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 (Basu et al., 2006, 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 $\mathrm{jac}(\boldsymbol{f}(\eta, \cdot), \boldsymbol{x})$. (Basu et al., 2006, 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 18, 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 (Coste and Shiota, 1992), 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 $\mathcal{C}$ of $\mathbb{R}^t \setminus (\mathcal{W}_\infty \cup \mathcal{W}_{\mathcal{H}})$ and any $\eta \in \mathcal{C}$, we have that $\pi^{-1}(\mathcal{C}) \cap \mathcal{V} \cap \mathbb{R}^{t+n}$ is homeomorphic to $\mathcal{C} \times (\pi^{-1}(\eta) \cap \mathcal{V} \cap \mathbb{R}^{t+n})$.

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 3, 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 III in Section 3.

The pseudo-code of Algorithm 3 is below. Its proof of correctness follows immediately from Proposition 21 and Corollary 17.

Algorithm 3: 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)

$[\mathcal{H}, \boldsymbol{w}_\infty] \leftarrow$ DRL-Matrix$(\boldsymbol{f})$
$\boldsymbol{w}_\mathcal{H} \leftarrow$ CleanFactors$(\mathrm{numer}(\det(\mathcal{H})), \boldsymbol{w}_\infty)$
$L \leftarrow$ SamplePoints$(\boldsymbol{w}_\mathcal{H} \neq 0 \wedge \boldsymbol{w}_\infty \neq 0)$
for $\eta \in L$ **do**
    $r_\eta \leftarrow$ Signature$(\mathcal{H}(\eta))$
end
return $\{(\eta, r_\eta) \mid \eta \in L\}$

Example 22. *We continue with the system in Example 11. The determinant of its parametric Hermite matrix is*

$$\boldsymbol{w}_\mathcal{H} = 16y_1(-y_2^6 - 3y_2^4y_3^2 - 3y_2^2y_3^4 - y_3^6 + 3y_1y_2^4 - 21y_1y_2^2y_3^2 + 3y_1y_3^4 - 3y_1^2y_2^2 - 3y_1^2y_3^2 + y_1^3).$$

We notice that $\boldsymbol{w}_\mathcal{H}$ coincides exactly with the output returned by the procedure DISCRIMINANTVARIETY *of Maple's package* ROOTFINDING[PARAMETRIC] *that computes a discriminant variety (Lazard and Rouillier, 2007).*

Computing at least one point per connected component of the semi-algebraic set $\mathbb{R}^3 \setminus V(\boldsymbol{w}_\mathcal{H})$ using RAGlib *gives us* 28 *points. We evaluate the signatures of $\mathcal{H}$ specialized at those points and find that the input system can have* 0, 2 *or* 4 *distinct real solutions when the parameters vary.*

Remark 23. *As we have seen, Algorithm 3 obtains a polynomial which serves similarly as discriminant varieties (Lazard and Rouillier, 2007) or border polynomials (Yang and Xia, 2005) 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 $\mathrm{crit}(\pi, \mathcal{V})$ on the $\boldsymbol{y}$-space. Since it is well-known that the computation of such Gröbner basis could be heavy, our algorithm has a chance to be more practical. In Section 8, we provide experimental results to support this claim.*

Remark 24. *It is worth noticing that, even though the design of Algorithm 3 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 $grevlex(x_n \succ \cdots \succ x_1)$. While every theoretical claim still holds for this ordering, the practical behavior could be different. We demonstrate this remark in Example 25 below.*

Example 25. *We consider the polynomial sequence $(f_1, f_2, f_3) \subset \mathbb{Q}[y_1, y_2, y_3][x_1, x_2, x_3]$*

$$\begin{aligned} f_1 &= x_1x_2 - x_3, \\ f_2 &= x_1^3 + 4x_1^2x_3 + 2x_2^3 - x_2^2x_3 + x_2x_3^2 - 2x_3^3 + 3x_1^2 - x_1x_3 - 3x_2^2 - 3x_3^2 - x_2 + 4x_3 + 4, \\ f_3 &= y_3x_1x_2 + y_1x_1 + y_2x_2 + 1. \end{aligned}$$

By computing the reduced Gröbner basis of the ideal generated by f_1, f_2, f_3 with respect to the ordering $grevlex(x_1 \succ x_2 \succ x_3) \succ grevlex(y_1 \succ y_2 \succ y_3)$, one note that this system above does not satisfy Assumption (C). Hence, the algebraic set $\mathcal{W}_\infty$ defining the locus over which our parametric Hermite matrix does not well specialize is non-empty.

The polynomials w_∞ and $w_\mathcal{H}$ computed in Algorithm 3 with respect to the monomial ordering $grevlex(x_1 \succ x_2 \succ x_3)$ have respectively the degrees 13 *and* 18.

On the other hand, using the monomial ordering $grevlex(x_3 \succ x_2 \succ x_1)$ in Algorithm 3, one obtains a polynomial $\tilde{w}_\infty$ of degree 7 *and the same polynomial $w_\mathcal{H}$ as above.*

Therefore, the degree of the input given into the subroutine SamplePoints *is reduced by using the second ordering (*25 *compared with* 31*). In practice, this choice of ordering accelerates significantly the computation of sample points.*

6.2 Computing semi-algebraic formulas

By Corollary 17, 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 Sylvester (1852) and Jacobi (1857) (see Ghys and Ranicki (2016) for a summary on these works).

Lemma 26. *(Ghys and Ranicki, 2016, Theorem 2.3.6) Let S be a $\delta \times \delta$ symmetric matrix in $\mathbb{R}^{\delta \times \delta}$ and, for $1 \leq i \leq \delta$, S_i be the i-th leading principal minor of S, i.e., the determinant of the sub-matrix 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 $0 \leq i \leq \delta$. 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 26 and Corollary 17, 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 27. *There exists a Zariski dense subset $\mathcal{A}$ of $\mathrm{GL}_\delta(\mathbb{Q})$ such that for $A \in \mathcal{A}$, all of the leading principal minors of $\mathcal{H}_A \coloneqq A^T \cdot \mathcal{H} \cdot A$ are not identically zero.*

Proof. For $1 \leq r \leq \delta$, 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 $\mathcal{A}$ of $\mathrm{GL}_\delta(\mathbb{Q})$ such that, for $A \in \mathcal{A}$, 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 $A = (a_{i,j})_{1 \leq i,j \leq \delta}$ 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 $\mathcal{A}_r$ 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 $A \in \mathcal{A}_r$ such that the $r \times r$ leading principal minor of $A^T \cdot \mathcal{H}(\eta) \cdot A$ is not zero.

Taking $\mathcal{A}$ as the intersection of $\mathcal{A}_r$ for $1 \leq r \leq \delta$, then, for $A \in \mathcal{A}$, 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 4) for solving Problem (1) through parametric Hermite matrices is described below. As it depends on the random choice of the matrix A, Algorithm 4 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 4: 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)

$\mathcal{H}, \boldsymbol{w}_\infty \leftarrow$ DRL-Matrix$(\boldsymbol{f})$
Choose randomly a matrix A in $\mathbb{Q}^{\delta \times \delta}$
$\mathcal{H}_A \leftarrow A^T \cdot \mathcal{H} \cdot A$
$(M_1, \ldots, M_\delta) \leftarrow$ LeadingPrincipalMinors$(\mathcal{H}_A)$
$L \leftarrow$ SamplePoints $\left(\boldsymbol{w}_\infty \wedge \left(\wedge_{i=1}^{\delta} M_i \neq 0\right)\right)$
for $\eta \in L$ **do**
    $r_\eta \leftarrow$ Signature$(\mathcal{H}(\eta))$
end
return $\{(\text{sign}\ (M_1(\eta), \ldots, M_\delta(\eta)), \eta, r_\eta) \mid \eta \in L\}$

Proposition 28. *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 4 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 26, 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 17, 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 4. □

Example 29. *From the parametric Hermite matrix $\mathcal{H}$ computed in Example 11, we obtain the sequence of leading principal minors below:*

$$
\begin{aligned}
M_1 &= 4,\\
M_2 &= 4(-2y_2^2 + y_3^2 + 2y_1),\\
M_3 &= 8(-y_2^4 - 2y_2^2y_3^2 - y_3^4 - y_1y_2^2 - y_1y_3^2 + 2y_1^2),\\
M_4 &= 16y_1(-y_2^6 - 3y_2^4y_3^2 - 3y_2^2y_3^4 - y_3^6 + 3y_1y_2^4 - 21y_1y_2^2y_3^2 + 3y_1y_3^4 - 3y_1^2y_2^2 - 3y_1^2y_3^2 + y_1^3).
\end{aligned}
$$

Since M_1 is constant, we compute at least one point per connected component of the semi-algebraic set defined by

$$M_2 \neq 0 \wedge M_3 \neq 0 \wedge M_4 \neq 0.$$

The computation using RAGlib *outputs a set of 48 sample points and finds the following realizable sign conditions of (M_2, M_3, M_4):*

$$[-1, 1, 1], [-1, -1, 1], [1, -1, -1], [-1, -1, -1], [1, 1, -1].$$

By evaluating the signature of $\mathcal{H}$ at each of those sample points, we deduce the semi-algebraic formulas corresponding to every possible number of real solutions

$$
\begin{aligned}
0 \textit{ real root } &\rightarrow (M_2 < 0 \wedge M_3 > 0 \wedge M_4 > 0) \vee (M_2 < 0 \wedge M_3 < 0 \wedge M_4 > 0)\\
2 \textit{ real roots } &\rightarrow (M_2 > 0 \wedge M_3 < 0 \wedge M_4 < 0) \vee (M_2 < 0 \wedge M_3 < 0 \wedge M_4 < 0)\\
&\qquad \vee (M_2 > 0 \wedge M_3 > 0 \wedge M_4 < 0)\\
4 \textit{ real roots } &\rightarrow (M_2 > 0 \wedge M_3 > 0 \wedge M_4 > 0).
\end{aligned}
$$

We recall that the semi-algebraic formulas obtained in Example 7 involve the subresultant coefficients s_2, s_3 and s_4 of degree 2, 6 and 11 respectively. Whereas, the degrees of the minors M_2, M_3 and M_4 that we obtain from the parametric Hermite matrix are only 2, 4 and 7.

7 Complexity analysis

7.1 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 (C).

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., (Bardet, 2004, Proposition 1.7.4) or Pardue (2010)), 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 $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$. 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 (C) holds, by Lemma 13, 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 D. *For any $g \in \mathcal{G}$, we have that $\deg(g) = \deg_{\boldsymbol{x}}(g)$.*

Proposition 30 below states that Assumption (D) is generic. Its direct consequence is a proof for Proposition 14.

Proposition 30. *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 (D) 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 (C).

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:

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

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 (Verron, 2016, 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 G_h be the reduced Gröbner basis of $\boldsymbol{f}_h$ with respect to the grevlex ordering $grevlex(\boldsymbol{x} \succ \boldsymbol{y} \succ y_{t+1})$. By (Bardet et al., 2015, Proposition 7), if the variables $\boldsymbol{x}$ is in Noether position with respect to $\boldsymbol{f}_h$, then the leading monomials appearing in G_h depend only on $\boldsymbol{x}$.

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

Since G_h generates $\langle \boldsymbol{f}_h \rangle$, G is a generating set of $\langle \boldsymbol{f} \rangle$. As the leading monomials of elements in 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 $g_h \in G_h$ 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 G divides the leading monomial of p. We conclude that G is a Gröbner basis of $\boldsymbol{f}$ with respect to the ordering $grevlex(\boldsymbol{x} \succ \boldsymbol{y})$ and the set of leading monomials in 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 $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$ 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 $grevlex(\boldsymbol{x} \succ \boldsymbol{y})$ 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 (D) holds for every $\boldsymbol{f} \in \mathscr{F}_D \cap \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]^n$.

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

Recall that, when Assumption (C) holds, by Lemma 13, 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 $\mathrm{trace}(\mathcal{L}_p)$. Since the map $p \mapsto \mathrm{trace}(\mathcal{L}_p)$ is linear, it is sufficient to consider p as a monomial in the variables $\boldsymbol{x}$.

Proposition 31. *Assume that Assumption (D) holds. Then, for any monomial m in the variables $\boldsymbol{x}$, the degree in $\boldsymbol{y}$ of $\mathrm{trace}(\mathcal{L}_m)$ is bounded by $\deg(m)$. As a consequence, the total degree of the entry $h_{i,j} = \mathrm{trace}(\mathcal{L}_{b_i \cdot b_j})$ 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 (D) holds, Assumption (C) 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 (D), 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 32. *Assume that $\boldsymbol{f}$ satisfies Assumption (D). Then the degree of a minor M consisting of the rows $(r_1, \ldots, r_\ell)$ and the columns $(c_1, \ldots, c_\ell)$ 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 $(-1)^{\text{sign }(\sigma)}h_{r_1,\sigma(c_1)}\dots h_{r_\ell,\sigma(c_\ell)}$, where σ is a permutation of $\{c_1,\dots,c_\ell\}$ and sign (σ) is its signature. We then bound the degree of each of those terms as follows using Proposition 31:

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

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 31 implies that, when Assumption (D) 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., $\deg(b_i)\leq\deg(b_j)$ for $1\leq i<j\leq\delta$. 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 33. *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*

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

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

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), ${}^H\boldsymbol{f} = ({}^Hf_1, \ldots, {}^Hf_n)$ forms a homogeneous regular sequence. Equivalently, by (Verron, 2016, Proposition 1.44), the homogeneous polynomial sequence $((f_1)_h, \ldots, (f_n)_h, x_{n+1})$ is regular. Particularly, $((f_1)_h, \ldots, (f_n)_h)$ is a homogeneous regular sequence and, by (Moreno-Socıas, 2003, 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 (Bardet et al., 2015, Proposition 7), the leading terms of $\mathcal{G}_h$ w.r.t $grevlex(x_1 \succ \cdots \succ x_{n+1})$ 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 $grevlex(\boldsymbol{x})$ (see, e.g., the proof of (Faugère et al., 2013, 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 $grevlex(x_1 \succ \cdots \succ x_{n+1})$ 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

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

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

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

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

Thus, we have that

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

□

Corollary 34 below follows immediately from Lemmas 32 and 33.

Corollary 34. *Assume that $\boldsymbol{f}$ is a regular sequence that satisfies Assumption (D). Then the degree of any minor of $\mathcal{H}$ is bounded by $n(d-1)d^n$.*

Example 35. *We consider again the system $\boldsymbol{f} = (x_1^2 + x_2^2 - y_1,\ x_1x_2 + y_2x_2 + y_3x_1)$ in Example 11. Note that $\boldsymbol{f}$ forms a regular sequence.*

The Gröbner basis $\mathcal{G}$ of $\boldsymbol{f}$ with respect to the ordering $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$ is

$$\mathcal{G} = \{x_2^3 + y_3x_2^2 + (y_2^2 - y_1)x_2 + y_2y_3x_1 - y_1y_3, x_1^2 + x_2^2 - y_1, x_1x_2 + x_1y_3 + x_2y_2\}.$$

So, $\boldsymbol{f}$ satisfies Assumption (D). The matrix with respect to the basis $B_1 = \{1, x_2, x_1, x_2^2\}$ has the following degree pattern:

$$\begin{bmatrix} 0 & 1 & 1 & 2 \\ 1 & 2 & 2 & 3 \\ 1 & 2 & 2 & 3 \\ 2 & 3 & 3 & 4 \end{bmatrix}$$

This degree pattern agrees with the result of Proposition 31. The determinant of this matrix is of degree 7, which is indeed smaller than $n(d-1)d^n = 8$

Whereas, using the basis $B_2 = \{1, x_2, x_2^2, x_2^3\}$ leads to another parametric Hermite matrix of different degrees. For $1 \leq i, j \leq 4$, the degree of its (i,j)-entry, which is equals to $\operatorname{trace}(\mathcal{L}_{x_2^{i+j-2}})$, is bounded by $\deg(x_2^{i-1}) + \deg(x_2^{j-1}) = i + j - 2$ using Proposition 31. Applying Lemma 32, the determinant is bounded by $2\sum_{i=0} \deg(x_2^i) = 12$.

By computing the parametric Hermite matrix of $\boldsymbol{f}$ with respect to B_2, we obtain the degree pattern

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \end{bmatrix}$$

on its entries and a determinant of degree 11. Again, both of our theoretical bounds hold for this matrix.

Remark 36. *Note that Assumption (D) 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 (D) (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 (D). Therefore, we easily deduce the two following bounds, which are similar to the ones of Proposition 31 and Corollary 34.

- $\deg(h_{i,j}) \leq d_{\boldsymbol{y}}(\deg(b_i) + \deg(b_j))$;
- *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 (D) does not hold.

7.2 Complexity analysis of our algorithms

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

Let $\boldsymbol{f} = (f_1, \ldots, f_n) \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ be a regular sequence, where $\boldsymbol{y} = (y_1, \ldots, y_t)$ and $\boldsymbol{x} = (x_1, \ldots, x_n)$, satisfying Assumptions (A) and (D). We denote by $\mathcal{G}$ be the reduced Gröbner basis of $\boldsymbol{f}$ with respect to the ordering $grevlex(\boldsymbol{x}) \succ grevlex(\boldsymbol{y})$. 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 37. *Assume that $\boldsymbol{f} = (f_1, \ldots, f_n) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ is a regular sequence that satisfies Assumptions (A) and (D). Then, the following holds.*

i) The parametric Hermite matrix $\mathcal{H}$ can be computed using

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

arithmetic operations in $\mathbb{Q}$.

ii) Each minor (including the determinant) of $\mathcal{H}$ can be computed using

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

arithmetic operations in $\mathbb{Q}$.

Proof. For the computation of the matrix, we rely on Proposition 19 which estimates the complexity of the evaluation & interpolation scheme described in Subsection 5.4.

By Lemma 33 and Proposition 31, the highest degree among the entries of $\mathcal{H}$ is bounded by $2\lambda = 2n(d-1)$. Therefore, we replace Λ in Proposition 19 by 2λ in the complexity statement of Proposition 19 to obtain

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

Similarly, the minors of $\mathcal{H}$ can be computed using the technique of evaluation & interpolation.

By Corollary 34, 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 Canny et al. (1989), it requires

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

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

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

□

Finally, we state our main result, which is Theorem II below. It estimates the arithmetic complexity of Algorithms 3 and 4.

Theorem II. *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 (D). Recall that $\mathfrak{D}$ denotes $n(d-1)d^n$. Then, we have the following statements:*

i) The arithmetic complexity of Algorithm 3 lies in

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

ii) Algorithm 4, 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 4 consist of polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree bounded by $\mathfrak{D}$.

Proof. As Assumption (D) 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 37, Algorithm 3 essentially consists of computing sample points of the connected components of the algebraic set $\mathbb{R}^t \setminus V(\det(\mathcal{H}))$.

By Corollary 34, the degree of $\det(\mathcal{H})$ is bounded by $\mathfrak{D}$. Applying Corollary 4, we obtain the following arithmetic complexity for this computation of sample points

$$O^{\sim}\left(\binom{t+\mathfrak{D}}{t}\, t^4\, 2^{3t} \mathfrak{D}^{2t+1}\right) \simeq O^{\sim}\left(\binom{t+\mathfrak{D}}{t}\, 2^{3t}\, n^{2t+1} d^{2nt+n+2t+1}\right).$$

Also by Corollary 4, 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 (Basu et al., 2006, Algorithm 8.43).

Therefore, the complexity of SamplePoints dominates the whole complexity of the algorithm. We conclude that Algorithm 3 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 4, 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 $M_1, \ldots, M_\delta$ of $\mathcal{H}_A$. Using Proposition 37, this step admits the arithmetic complexity bound

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

Next, Algorithm 4 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 4 gives the arithmetic complexity

$$O^{\sim}\left(\binom{t+\mathfrak{D}}{t}\, t^4\, d^{nt+n}\, 2^{3t}\, \mathfrak{D}^{2t+1}\right) \simeq O^{\sim}\left(\binom{t+\mathfrak{D}}{t}\, 2^{3t}\, n^{2t+1} d^{3nt+2(n+t)+1}\right).$$

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

Again, the complexity of SamplePoints dominates the whole complexity of Algorithm 4. The proof of Theorem II is then finished. □

8 Practical implementation & Experimental results

8.1 Remark on the implementation of Algorithm 4

Recall that Algorithm 4 leads us to compute sample points per connected components of the non-vanishing set of the leading principal minors $(M_1, \ldots, M_\delta)$. Comparing to Algorithm 3 in which we only compute sample points for $\mathbb{R}^t \setminus V(M_\delta)$, the complexity of Algorithm 4 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 4 for tackling practical problems. Therefore, we introduce the following optimization in our implementation of Algorithm 4.

We start by following exactly the steps (1-4) of Algorithm 4 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 $\text{sign}\,(M_i(\eta)) = \sigma_i$ 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

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

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 4 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 4 does not change the complexity bound given in Theorem II.

8.2 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 6. 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 6) with the Sturm-based algorithm (Section 4) 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 algorithms using parametric Hermite matrices with two Maple packages for solving parametric polynomial systems: ROOTFINDING[PARAMETRIC] (Gerhard et al., 2010) and REGULARCHAINS[PARAMETRICSYSTEMTOOLS] (Yang et al., 2001). 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 Yang et al. (2001). 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 8.1, 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	∞	∞	∞	20 m	∞	∞
3	$[4,2]$	.6 s	12 s	90 h	90 h	32	∞	∞	∞	12 m	∞	∞
3	$[3,3]$	.7 s	27 s	∞	∞	36	∞	∞	∞	15 m	∞	∞
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 Kuramoto (1975), 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 Harris et al. (2020) 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 Harris et al. (2020), 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. Harris et al. (2020)). 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. Harris et al. (2020)). 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 $e_1 = y_1 + y_2 + y_3$, $e_2 = y_1y_2 + y_2y_3 + y_3y_1$ and $e_3 = y_1y_2y_3$ 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 $\mathbb{R}^3$.

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 (Henrion and Sebek, 2008). 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 (C). 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 3 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

References

Bank, B., Giusti, M., Heintz, J., Mbakop, G.M., 2001. Polar varieties and efficient real elimination. Mathematische Zeitschrift 238, 115–144.

Bank, B., Giusti, M., Heintz, J., Pardo, L.M., 2005. Generalized polar varieties: Geometry and algorithms. Journal of complexity 21, 377–412.

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

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

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

Basu, S., Roy, M., 2014. Divide and conquer roadmap for algebraic sets. Discrete & Computational Geometry 52, 278–343. doi:10.1007/s00454-014-9610-9.

Basu, S., Roy, M., Safey El Din, M., Schost, É., 2014. A baby step-giant step roadmap algorithm for general algebraic sets. Foundations of Computational Mathematics 14, 1117–1172. doi:10.1007/s10208-014-9212-1.

Bayer, D., Stillman, M., 1987. A criterion for detecting m-regularity. Inventiones Mathematicae 87, 1.

Bayer, D., Stillman, M., 1987. A theorem on refining division orders by the reverse lexicographic order. Duke Math. J. 55, 321–328.

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.

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, Association for Computing Machinery, New York, NY, USA. p. 54–60. doi:10.1145/1277548.1277557.

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, Association for Computing Machinery, New York, NY, USA. p. 121–128.

Collins, G.E., 1976. Quantifier elimination for real closed fields by cylindrical algebraic decomposition: a synopsis. ACM SIGSAM Bulletin 10, 10–12. doi:10.1145/1093390.1093393.

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.

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

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.

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.

Davenport, J.H., Heintz, J., 1988. Real quantifier elimination is doubly exponential. J. Symb. Comput. 5, 29–35. doi:10.1016/S0747-7171(88)80004-X.

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

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

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.

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.

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.

Gerhard, J., Jeffrey, D.J., Moroz, G., 2010. A package for solving parametric polynomial systems. ACM Commun. Comput. Algebra 43, 61–72. doi:10.1145/1823931.1823933.

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

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 International Conference, AAECC-5, Menorca, Spain, June 15-19, 1987, Proceedings, pp. 247–257. doi:10.1007/3-540-51082-6_83.

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. doi:10.1007/3-540-60114-7_16.

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

González-Vega, L., Recio, T., Lombardi, H., Roy, M.F., 1998. Sturm—habicht sequences, determinants and real roots of univariate polynomials, in: Quantifier Elimination and Cylindrical Algebraic Decomposition. Springer, pp. 300–316.

Guo, F., Safey El Din, M., Zhi, L., 2010. Global optimization of polynomials using generalized critical values and sums of squares, in: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, pp. 107–114.

Hardt, R.M., 1980. Semi-algebraic local-triviality in semi-algebraic mappings. American Journal of Mathematics 102, 291–302.

Harris, K., Hauenstein, J.D., Szanto, A., 2020. Smooth points on semi-algebraic sets. arXiv:2002.04707.

Heintz, J., 1983. Definability and fast quantifier elimination in algebraically closed fields. Theor. Comput. Sci. 24, 239–277.

Henrion, D., 2010. Detecting rigid convexity of bivariate polynomials. Linear Algebra and its Applications 432, 1218 – 1233. doi:https://doi.org/10.1016/j.laa.2009.10.033.

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, Association for Computing Machinery, New York, NY, USA. p. 111–116. doi:10.1145/1390768.1390786.

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.

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

Kalkbrener, M., 1997. On the stability of gröbner bases under specializations. Journal of Symbolic Computation 24, 51–58.

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

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.

Lazard, D., Rouillier, F., 2007. Solving parametric polynomial systems. Journal of Symbolic Computation 42, 636–667.

Le Gall, F., 2014. Powers of tensors and fast matrix multiplication, in: Proceedings of the 39th international symposium on symbolic and algebraic computation, pp. 296–303.

Liang, S., Jeffrey, D.J., Maza, M.M., 2008. The complete root classification of a parametric polynomial on an interval, in: Proceedings of the twenty-first international symposium on Symbolic and algebraic computation, pp. 189–196.

Moreno-Socıas, G., 2003. Degrevlex gröbner bases of generic complete intersections. Journal of Pure and Applied Algebra 180, 263 – 283.

Pardue, K., 2010. Generic sequences of polynomials. Journal of Algebra 324, 579 – 590.

Rouillier, F., 1999. Solving zero-dimensional systems through the rational univariate representation. Appl. Algebra Eng. Commun. Comput. 9, 433–461. doi:10.1007/s002000050114.

Safey El Din, M., 2008. Computing the global optimum of a multivariate polynomial over the reals, in: Proceedings of the twenty-first international symposium on Symbolic and algebraic computation, pp. 71–78.

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

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., ACM, NY, USA. p. 224–231. doi:10.1145/860854.860901.

Safey El Din, M., Schost, É., 2011. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. Discrete & Computational Geometry 45, 181–220. doi:10.1007/s00454-009-9239-2.

Safey El Din, M., Schost, É., 2017. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. J. ACM 63, 48:1–48:37. doi:10.1145/2996450.

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.

Schost, É., 2003. Computing parametric geometric resolutions. Applicable Algebra in Engineering, Communication and Computing 13, 349–393.

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

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.

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

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, 33–49.

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.

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.

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, Association for Computing Machinery, New York, NY, USA. p. 362–364. doi:10.1145/1073884.1073934.