Solving parameter-dependent semi-algebraic systems

Louis Gaillard
ENS de Lyon,
F-69007 Lyon, France

Mohab Safey El Din
Sorbonne Université, CNRS, LIP6
F-75005 Paris, France

ABSTRACT

We consider systems of polynomial equations and inequalities in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ where $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_t)$. The $\boldsymbol{y}$ indeterminates are considered as *parameters* and we assume that when specialising them *generically*, the set of common complex solutions, to the obtained equations, is finite.

We consider the problem of real root classification for such parameter-dependent problems, i.e. identifying the possible number of real solutions depending on the values of the parameters and computing a description of the regions of the space of parameters over which the number of real roots remains invariant.

We design an algorithm for solving this problem. The formulas it outputs enjoy a determinantal structure. Under genericity assumptions, we show that its arithmetic complexity is polynomial in both the maximum degree d and the number s of the input inequalities and exponential in $nt + t^2$. The output formulas consist of polynomials of degree bounded by $(2s + n)d^{n+1}$. This is the first algorithm with such a singly exponential complexity. We report on practical experiments showing that a first implementation of this algorithm can tackle examples which were previously out of reach.

CCS CONCEPTS

• **Computing methodologies → Algebraic algorithms**; • **Theory of computation → Design and analysis of algorithms**.

KEYWORDS

Polynomial system solving; Real algebraic geometry; Gröbner bases.

ACM Reference Format:
Louis Gaillard and Mohab Safey El Din. 2024. Solving parameter-dependent semi-algebraic systems. In *International Symposium on Symbolic and Algebraic Computation 2024 (ISSAC 2024), July 16–19, 2024, Raleigh, USA.* ACM, New York, NY, USA, 10 pages.

1 INTRODUCTION

Problem statement. We consider polynomials $\boldsymbol{f} = (f_1, \ldots, f_p)$ and $\boldsymbol{g} = (g_1, \ldots, g_s)$ in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ with $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_t)$. The variables $\boldsymbol{x}$ (resp. $\boldsymbol{y}$) are seen as the *unknowns* (resp. *parameters*) of the system. Further, we denote by π the canonical projection $(\boldsymbol{y}, \boldsymbol{x}) \to \boldsymbol{y}$ on the space of parameters. We denote by $\mathcal{V} \subseteq \mathbb{C}^{t+n}$ the (complex) algebraic variety defined by $\boldsymbol{f} = 0$, and by $\mathcal{V}_{\mathbb{R}}$ its real trace $\mathcal{V} \cap \mathbb{R}^{t+n}$. In this paper, we assume the following.

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

In other words, for a *generic* specialization point η, the specialized system $\boldsymbol{f}(\eta, \cdot) = 0$ is zero-dimensional. Besides, can assume that the cardinality of $\pi^{-1}(\eta) \cap \mathcal{V}$ remains invariant when η ranges over $\mathcal{O}$. This is not the case for the set of real solutions.

We consider the (basic) semi-algebraic set $\mathcal{S} \subseteq \mathbb{R}^{t+n}$ defined by

$$f_1 = \cdots = f_p = 0, \quad g_1 > 0, \ldots, \ g_s > 0. \tag{1}$$

The goal of this paper is to provide an efficient algorithm for solving the real root classification problem over $\mathcal{S}$ as stated below.

Problem 1 (Real solution classification). *On input $(\boldsymbol{f}, \boldsymbol{g})$ with $\boldsymbol{f}$ satisfying Assumption A, compute $(\Phi_i, \eta_i, r_i)_{1 \le i \le \ell}$ such that, for $1 \le i \le \ell$, Φ_i is a semi-algebraic formula in $\mathbb{Q}[\boldsymbol{y}]$ defining the semi-algebraic set $\mathcal{T}_i \subseteq \mathbb{R}^t$, with $\eta_i \in \mathcal{T}_i$ and $r_i \ge 0$ such that*

- *for all $\eta \in \mathcal{T}_i$, the number of points in $\mathcal{S} \cap \pi^{-1}(\eta)$ is r_i,*
- *$\bigcup_{i=1}^{\ell} \mathcal{T}_i$ is dense in $\mathbb{R}^t$.*

Such a sequence $(\Phi_i, \eta_i, r_i)_{1 \le i \le \ell}$ is said to be a solution to Problem 1 which arises in many applications (see e.g. [4, 9, 13, 19, 24, 29]).

Prior works. First, as noticed in [21], the cylindrical algebraic decomposition (CAD) algorithm due to Collins [8] could be used to solve Problem 1. However, its doubly exponential complexity [5, 10] in the total number of variables makes it difficult to use.

More efficient approaches have been devised by using polynomial elimination methods combined with real algebraic geometry. They consist in computing some nonzero polynomials, say $h_1, \ldots, h_k$ in $\mathbb{Q}[\boldsymbol{y}]$, such that the number of points in $\mathcal{S} \cap \pi^{-1}(\eta)$ remains invariant when η ranges over some connected component of the semi-algebraic set defined by $h_1 \neq 0, \ldots, h_k \neq 0$. Such polynomials are called *border polynomials*, in the context of methods using the theory of regular chains (see e.g. [22, 27, 28]), or *discriminant polynomials* in the context of methods using algebraic elimination algorithms based on Gröbner bases (see e.g. [18, 23]) when the ideal generated by $\boldsymbol{f}$ is assumed to be radical and equidimensional. When d is the maximum degree of the input polynomials in $\boldsymbol{f}$ and $\boldsymbol{g}$, these h_i's can be proven to have degree bounded by $n(d-1)d^n$.

Once these polynomials are computed one then needs to describe the connected components of the set where none of them vanish. When this is done through the CAD algorithm, the cost of this is doubly exponential in t, the number of parameters. Using more advanced algorithms for computing semi-algebraic descriptions of connected components of semi-algebraic sets (see [2, Chap. 16]) through parametric roadmaps, one can obtain a complexity using $(n(d-1)d^n)^{O(t^4)}$ arithmetic operations in $\mathbb{Q}$ and which would output polynomials of degree lying in $(n(d-1)d^n)^{O(t^3)}$.

All in all, just a few is known about the complexity of these methods and it has been an open problem to obtain better complexity estimates or degree bounds on the polynomials of the output formulas required to solve Problem 1.

ISSAC 2024, July 16–19, 2024, Raleigh, USA

A first step towards this goal comes from the analysis of the algorithm in [21]. This algorithm is restricted to the case where the ideal generated by $\boldsymbol{f}$ is radical and the sequence $\boldsymbol{g}$ is empty. Under *genericity assumptions* on the input $\boldsymbol{f}$, this algorithm runs in time quasi-linear in $n^{O(t)}d^{3nt+O(n+t)}$ and the degrees of the polynomials in the output formulas lie in $n(d-1)d^n$. This is achieved using classical real root counting methods (through Hermite's quadratic forms) but combined in an innovative way with the theory of Gröbner bases. Additionally, the output formulas enjoy a nice determinantal encoding which allows one to evaluate them easily. This is at the foundations of new efficient algorithms for one-block quantifier elimination [20]. We also note that these techniques can lead to a new geometric approach for Cylindrical Algebraic Decomposition [7].

Still, several open problems remain. One is to obtain similar complexity bounds which do not depend on the aforementioned genericity assumptions. Another open problem is to extend such an approach to real root classification problems *involving inequalities*, hence extending significantly the range of applications which could be reached. In this paper, we tackle this second open problem.

Contributions. We present an algorithm solving Problem 1 revisiting the ideas in [21] to handle the case of systems of equations and inequalities. It uses a real root counting machinery based on Hermite's quadratic form [16] in some appropriate basis. In order to take the polynomial inequalities defined by $\boldsymbol{g}$ into account, this algorithm relies on a method originated in [3] using the so-called Tarski-query [2, Sec. 10.3] for determining the sign conditions realized by a family of polynomials on a finite set of points. These methods are devised to count the number of real solutions to some system of polynomial equations (with coefficients in $\mathbb{R}$), with finitely many complex roots, which do satisfy some extra polynomial inequalities.

Our contribution combines these methods with Gröbner bases computations in our context where the coefficients of our input polynomials depend on the parameters $\boldsymbol{y}$. A second key ingredient, used to control the number of calls to Tarski queries, in a way that is similar to the one used in [2, Chap. 10], is the use of efficient routines for computing sample points per connected components in semi-algebraic sets lying in the space of parameters [21, Sec. 3]. Hence, the semi-algebraic constraints depending on $\boldsymbol{y}$ actually encode some constraints on the signature of *parameter-dependent* Hermite matrices and thus, enjoy a nice determinantal structure.

Note that, by contrast with [18], this algorithm does not assume that the ideal generated by $\boldsymbol{f}$ is radical and equidimensional.

Since this algorithm makes use of Gröbner bases computations, extra genericity assumptions are needed to control its complexity. Hence, we assume that the homogeneous component of the f_i's of highest degree forms a regular sequence, which we abbreviate by the saying that $\boldsymbol{f}$ is a regular sequence. In addition, letting $\mathscr{G}$ be a reduced Gröbner basis for the ideal generated by $\boldsymbol{f}$ and the graded reverse lexicographical ordering, we assume the following.

Assumption B. *For any $p \in \mathscr{G}$, we have* $\deg p = \deg_{\boldsymbol{x}} p$.

These assumptions are known to be satisfied generically (see [21, Prop. 20]) and to enable nicer complexity bounds on Gröbner bases. Our main complexity result is the following one. We use the notation $g = \widetilde{O}(f)$ meaning that $g = O(f \log^{\kappa}(f))$ for some $\kappa > 0$.

Theorem 1.1. *Let $\boldsymbol{f} \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ be a regular sequence such that $\boldsymbol{f}$ satisfies both Assumptions A and B. Let $\mathfrak{D} := (2sd + n(d-1))d^n$. There exists an algorithm which computes a solution to Problem 1 using*

$$\widetilde{O}\left(\binom{t+\mathfrak{D}}{t}\binom{s}{t}^{t+1} 2^{3t^2+nt+8t+n} s^{t+2} (2s+n)^{2t+1} d^{t^2+4nt+3(n+t)+1}\right)$$

arithmetic operations in $\mathbb{Q}$ and outputs at most $(4d^n sr\mathfrak{D})^t$ formulas that consists of $O(d^n sr)$ polynomials of degree at most $\mathfrak{D}$.

We report on practical experiments performed with a first implementation of this algorithm. That implementation makes no use of the genericity assumptions made to enable a complexity analysis, it only uses Assumption A. Benchmark tests include random dense polynomial systems (hence, these are presumably generic). Practical performances which are achieved show that this algorithm outperforms the state-of-the-art software for solving Problem 1. We also fully solve an application related to the Perspective-Three-Point problem for which computing semi-algebraic formulas for the real root classification was an open problem.

Plan of the paper. Section 2 recalls the basics on Hermite's quadratic forms, using materials mostly from [2, Chap. 4]. Section 3 generalizes constructions and results on *parametric* Hermite matrices from [21] to the case where inequalities are involved. Section 4 describes the algorithm on which Theorem 1.1 relies and proves the complexity statements. Section 5 reports on practical experiments.

2 HERMITE'S QUADRATIC FORM

We recall some basic definitions and properties on Hermite's quadratic forms. For more details, we refer to [2, Chap. 4].

2.1 Definition

Let $\mathbb{K}$ be a field of characteristic 0 and $\boldsymbol{f} = (f_1, \ldots, f_p) \subset \mathbb{K}[\boldsymbol{x}]$ be generating a zero-dimensional ideal, denoted by $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$. The quotient ring $\mathcal{A}_{\mathbb{K}} := \mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ is a finite dimensional $\mathbb{K}$-vector space [2, Theorem 4.85] of dimension δ. A monomial basis $B = (b_1, \ldots, b_\delta)$ of $\mathcal{A}_{\mathbb{K}}$ can be derived from a Gröbner basis G of $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ with respect to (w.r.t.) an admissible monomial ordering $\succ$ over $\mathbb{K}[\boldsymbol{x}]$: it is the set of monomials that are not divisible by any leading monomial of elements in G. For $q \in \mathbb{K}[\boldsymbol{x}]$, we denote by $\overline{q}$ the class of q in $\mathcal{A}_{\mathbb{K}}$ and by $L_q : \overline{p} \in \mathcal{A}_{\mathbb{K}} \mapsto \overline{p \cdot q} \in \mathcal{A}_{\mathbb{K}}$ the multiplication by q in $\mathcal{A}_{\mathbb{K}}$.

Definition 2.1 (Hermite's quadratic form). *For $g \in \mathcal{A}_{\mathbb{K}}$,* Hermite's bilinear form $\mathrm{herm}(\boldsymbol{f}, g)$ *is defined by*

$$\begin{aligned} \mathrm{herm}(\boldsymbol{f}, g) \colon \mathcal{A}_{\mathbb{K}} \times \mathcal{A}_{\mathbb{K}} &\to \mathbb{K} \\ (p, q) &\mapsto \mathrm{Tr}(L_{gpq}), \end{aligned}$$

where Tr *denotes the trace. The corresponding quadratic form $p \mapsto \mathrm{Tr}(L_{gp^2})$ is called* Hermite's quadratic form $\mathrm{Herm}(\boldsymbol{f}, g)$. *The* Hermite matrix *associated to $(\boldsymbol{f}, g)$ w.r.t. the basis B is the matrix $\mathcal{H} = (h_{i,j})_{1 \le i,j \le \delta} \in \mathbb{K}^{\delta \times \delta}$ of* $\mathrm{Herm}(\boldsymbol{f}, g)$ *w.r.t. B,* i.e. $h_{i,j} = \mathrm{Tr}(L_{gb_ib_j})$.

For a matrix $\mathcal{H}$, $\mathcal{H}_{i,j}$ is its element at the i-th row and j-th column.

Proposition 2.2. *Let $B = (b_1, \ldots, b_\delta)$ be a basis of $\mathcal{A}_{\mathbb{K}}$, $g \in \mathcal{A}_{\mathbb{K}}$, $\mathcal{H}$ and $\mathcal{H}_g$ be the matrices of* $\mathrm{Herm}(\boldsymbol{f}, 1)$ *and* $\mathrm{Herm}(\boldsymbol{f}, g)$ *w.r.t. B. Let $M = (m_{i,j})$ be the matrix of L_g w.r.t. B. Then, $\mathcal{H}_g = \mathcal{H}M$.*

Proof. For $p, q \in \mathcal{A}_{\mathbb{K}}$, we have $\mathrm{herm}(\boldsymbol{f}, g)(p, q) = \mathrm{Tr}(L_{gpq}) = \mathrm{herm}(\boldsymbol{f}, 1)(p, gq)$. Thus, it holds that

$$(\mathcal{H}_g)_{i,j} = \mathrm{herm}(\boldsymbol{f}, 1)(b_i, gb_j) = \mathrm{herm}(\boldsymbol{f}, 1)\left(b_i, \sum_{k=1}^{\delta} m_{k,j} b_k\right)$$
$$= \sum_{k=1}^{\delta} m_{k,j} \mathcal{H}_{i,k} = (\mathcal{H}M)_{i,j}. \qquad \square$$

2.2 Real root counting

For now, we assume $\mathbb{K} = \mathbb{R}$ or $\mathbb{Q}$ (or any ordered field). For $r \in \mathbb{K}$, $\mathrm{sign}(r)$ is $-1, 0$ or 1 if $r < 0$, $r = 0$ or $r > 0$ respectively.

Definition 2.3 (Tarski-query). *Let Z be a finite set in $\mathbb{K}^n$ and $g \in \mathbb{K}[\boldsymbol{x}]$. We define the* Tarksi-query, $\mathrm{TaQ}(g, Z)$ *of g for Z by*

$$\sum_{x \in Z} \mathrm{sign}(g(x)) = \sharp\{x \in Z \mid g(x) > 0\} - \sharp\{x \in Z \mid g(x) < 0\}.$$

When Z is the finite set of real roots of a zero-dimensional system $\boldsymbol{f} = 0$, we denote it by $\mathrm{TaQ}(g, \boldsymbol{f})$.

We denote the signature of a real quadratic form q by $\mathrm{Sign}(q)$.

Theorem 2.4 ([2, Thm. 4.100]). *Let $\boldsymbol{f} = (f_1, \ldots, f_p) \subset \mathbb{K}[\boldsymbol{x}]$ be as above and $g \in \mathbb{K}[\boldsymbol{x}]$. Then,* $\mathrm{Sign}(\mathrm{Herm}(\boldsymbol{f}, g)) = \mathrm{TaQ}(g, \boldsymbol{f})$.

Hence, Tarski-queries are given by signatures of Hermite matrices. From $\mathrm{TaQ}(1, \boldsymbol{f})$ $\mathrm{TaQ}(g, \boldsymbol{f})$ and $\mathrm{TaQ}(g^2, \boldsymbol{f})$, one can compute the number of real roots of $\boldsymbol{f}$ that satisfy a given sign condition for g. We define $c(g \diamond 0)$ for $\diamond \in \{<, =, >\}$ as $\sharp\{x \mid \boldsymbol{f}(x) = 0 \wedge g(x) \diamond 0\}$. We have the following invertible system

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} c(g = 0) \\ c(g > 0) \\ c(g < 0) \end{bmatrix} = \begin{bmatrix} \mathrm{TaQ}(1, \boldsymbol{f}) \\ \mathrm{TaQ}(g, \boldsymbol{f}) \\ \mathrm{TaQ}(g^2, \boldsymbol{f}) \end{bmatrix}. \qquad (2)$$

Theorem 2.5 ([15, Thm. 1.9]). *Let M be a symmetric matrix in $\mathbb{R}^{m \times m}$ and for $0 \leq i \leq m$ let M_i denote its i-th leading principal minor. We assume that $M_i \neq 0$ for all $0 \leq i \leq m$. Then we have*

$$\mathrm{Sign}(M) = m - 2\,\mathrm{Var}(M_0, M_1, \ldots, M_m),$$

where Var *stands for the number of sign variations in the sequence.*

3 PARAMETRIC HERMITE MATRICES

3.1 Basic construction and properties

Let $\boldsymbol{f} = (f_1, \ldots, f_p) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ such that $\boldsymbol{f}$ satisfies Assumption A and $g \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$. We take as a base field $\mathbb{K}$ the rational function field $\mathbb{Q}(\boldsymbol{y})$. By [21, Lem. 4], as $\boldsymbol{f}$ satisfies Assumption A, the ideal $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ generated by $\boldsymbol{f}$ in $\mathbb{K}[\boldsymbol{x}]$ is zero-dimensional. Hence one can define Hermite's quadratic form $\mathrm{Herm}(\boldsymbol{f}, g)$ and compute a *parametric* Hermite matrix $\mathcal{H}_g \in \mathbb{K}^{\delta \times \delta}$ representing $\mathrm{Herm}(\boldsymbol{f}, g)$ (once a basis B of $\mathcal{A}_{\mathbb{K}}$ is fixed). We start by making explicit how these can be computed and next prove some *nice* specialization properties of these matrices. We follow and extend the approach in [21].

Gröbner basis and monomial basis. We denote $\mathtt{grevlex}(\boldsymbol{x})$ for the graded reverse lexicographical ordering (*grevlex*) among the variables $\boldsymbol{x}$ (with $x_1 \succ \cdots \succ x_n$) and $\mathtt{grevlex}(\boldsymbol{x}) \succ \mathtt{grevlex}(\boldsymbol{y})$ (with $y_1 \succ \cdots \succ y_t$) for the elimination ordering. For $p \in \mathbb{C}(\boldsymbol{y})[\boldsymbol{x}]$, $\mathrm{lc}_{\boldsymbol{x}}(p)$ (resp. $\mathrm{lm}_{\boldsymbol{x}}(p)$) denotes the leading coefficient (resp. monomial) of p for the ordering $\mathtt{grevlex}(\boldsymbol{x})$. We let $\mathscr{G}$ be the reduced Gröbner basis of $\langle \boldsymbol{f} \rangle \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ w.r.t. this elimination ordering. By [21, Lem. 6], $\mathscr{G}$ is also a Gröbner basis of $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ w.r.t. $\mathtt{grevlex}(\boldsymbol{x})$. Hence the set $\mathscr{B}$ of all monomials in $\boldsymbol{x}$ that are not reducible by the leading monomials of $\mathscr{G}$ (w.r.t. $\mathtt{grevlex}(\boldsymbol{x})$) is finite since $\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ is zero-dimensional. It forms a basis of $\mathcal{A}_{\mathbb{K}}$. We define $\mathcal{H}_g$ as the parametric Hermite matrix associated to $(\boldsymbol{f}, g)$ w.r.t. the basis $\mathscr{B}$.

Algorithm for computing Hermite matrices. In [21], an algorithm is described to compute the parametric Hermite matrix $\mathcal{H}_1$. Actually this does not only compute the matrix $\mathcal{H}_1$ but also the family of matrices $(M_b)_{b \in \mathscr{B}}$ such that M_b is the matrix of the multiplication map L_b w.r.t. the basis $\mathscr{B}$. We explain now how we can compute $\mathcal{H}_g$ from $\mathcal{H}_1$. We first compute $\overline{g}$ the normal form of g by the Gröbner basis $\mathscr{G}$ (w.r.t. $\mathtt{grevlex}(\boldsymbol{x})$ and $\mathbb{K}$ as a base field), namely $\overline{g} = \sum_{b \in \mathscr{B}} c_b b$, with $c_b \in \mathbb{Q}(\boldsymbol{y})$. Then we have $M_g = \sum_{b \in \mathscr{B}} c_b M_b$, where M_g denotes the matrix of the multiplication by g in the basis $\mathscr{B}$. By Proposition 2.2, we obtain $\mathcal{H}_g = \mathcal{H}_1 \cdot M_g$.

Specialization properties. We prove now specialization properties of these parametric Hermite matrices. The Gröbner basis $\mathscr{G}$ is a subset of $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$, thus for all $p \in \mathscr{G}$, $\mathrm{lc}_{\boldsymbol{x}}(p) \in \mathbb{Q}[\boldsymbol{y}]$. We denote by $V(\mathrm{lc}_{\boldsymbol{x}}(p))$ its vanishing set in $\mathbb{C}^t$. We consider the following algebraic set $\mathcal{W}_\infty \subseteq \mathbb{C}^t$:

$$\mathcal{W}_\infty := \bigcup_{p \in \mathscr{G}} V(\mathrm{lc}_{\boldsymbol{x}}(p)). \qquad (3)$$

Proposition 3.1. *For all $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$, the specialization $\mathcal{H}_g(\eta)$ coincides with the Hermite matrix $\mathcal{H}_g^\eta$ associated to $(\boldsymbol{f}(\eta, \cdot), g(\eta, \cdot))$ w.r.t. the basis $\mathscr{B}$.*

Proof. Let $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$. By [21, Lem. 9] which is a consequence of [17, Thm. 3.1], the specialization $\mathscr{G}(\eta, \cdot) := \{p(\eta, \cdot) \mid p \in \mathscr{G}\}$ is a Gröbner basis of the ideal $\langle \boldsymbol{f}(\eta, \cdot) \rangle \subseteq \mathbb{C}[\boldsymbol{x}]$ w.r.t. the ordering $\mathtt{grevlex}(\boldsymbol{x})$. Since $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$, the leading coefficient $\mathrm{lc}_{\boldsymbol{x}}(p)$ does not vanish at η for all $p \in \mathscr{G}$. Thus, the set of leading monomials of $\mathscr{G}$ in the variables $\boldsymbol{x}$ w.r.t. $\mathtt{grevlex}(\boldsymbol{x})$ is exactly the set of leading monomials of $\mathscr{G}(\eta, \cdot)$ w.r.t. $\mathtt{grevlex}(\boldsymbol{x})$. Therefore, the finite set $\mathscr{B}$ is also the set of monomials in $\boldsymbol{x}$ that are not reducible by $\mathscr{G}(\eta, \cdot)$. Hence $\mathscr{B}$ is a basis of the quotient ring $\mathbb{C}[\boldsymbol{x}]/\langle \boldsymbol{f}(\eta, \cdot) \rangle$. So, $\langle \boldsymbol{f}(\eta, \cdot) \rangle$ is zero-dimensional and one can define $\mathcal{H}_g^\eta$ as the Hermite matrix associated to $(\boldsymbol{f}(\eta, \cdot), g(\eta, \cdot))$ w.r.t. the basis $\mathscr{B}$.

Moreover, the specialization property for the Gröbner basis $\mathscr{G}$ implies that when dividing some polynomial w.r.t. $\mathscr{G}$, none of the denominators which appear vanish at $\eta \in \mathbb{C}^t$. Hence, given $h \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ and its normal form $\overline{h}$ w.r.t. $\mathscr{G}$ (computed with $\mathbb{K}$ as a base field and w.r.t. $\mathtt{grevlex}(\boldsymbol{x})$), for any $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$, $\overline{h}(\eta, \cdot)$ coincides with the normal form of $h(\eta, \cdot)$ w.r.t. $\mathscr{G}(\eta, \cdot)$. This implies that $\mathcal{H}_g(\eta) = \mathcal{H}_g^\eta$. $\square$

Corollary 3.2. *For all $\eta \in \mathbb{C}^t \setminus \mathcal{W}_\infty$, the signature of $\mathcal{H}_g(\eta)$ is the Tarski-query of $g(\eta, \cdot)$ for the zero-dimensional system $\boldsymbol{f}(\eta, \cdot)$.*

Proof. By Proposition 3.1, $\mathcal{H}_g(\eta)$ is a Hermite matrix associated to $(\boldsymbol{f}(\eta, \cdot), g(\eta, \cdot))$. The result follows from Theorem 2.4 . $\square$

Note that $\mathcal{W}_\infty$ does not depend on g. One can compute the number of real roots of the specialized system $\boldsymbol{f}(\eta, \cdot)$ satisfying some sign condition for g by computing the signatures of three parametric Hermite matrices evaluated in η and inverting the system (2).

3.2 Degree bounds

We bound the degrees of the entries of the parametric Hermite matrix $\mathcal{H}_g$ under some assumptions that we make explicit below. We start by recalling the definition of a regular sequence.

Definition 3.3 (Regular sequence). *Let $(f_1, \dots, f_p) \subset \mathbb{K}[\boldsymbol{x}]$ with $p \le n$ be a homogeneous polynomial sequence. We say that $(f_1, \dots, f_p)$ is a* homogeneous regular sequence *if for all $1 \le i \le p$, f_i is not a zero-divisor in $\mathbb{K}[\boldsymbol{x}]/\langle f_1, \dots, f_{i-1}\rangle$.*

A polynomial sequence $(f_1, \dots, f_p) \subset \mathbb{K}[\boldsymbol{x}]$ is called an affine regular sequence *if $(f_1^H, \dots, f_p^H)$ is a homogeneous regular sequence, where for a polynomial $q \in \mathbb{K}[\boldsymbol{x}]$, q^H denotes the homogeneous component of largest degree of q.*

First we bound the degrees of the entries of the matrix $\mathcal{H}_g$. For $p \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ we denote by $\deg(p)$ the total degree of p and $\deg_{\boldsymbol{x}}(p)$ (resp. $\deg_{\boldsymbol{y}}(p)$) the degree of p w.r.t. $\boldsymbol{x}$ (resp. $\boldsymbol{y}$). Let $d := \max_{1 \le i \le p} \deg(f_i)$. We consider the reduced Gröbner basis $\mathscr{G}$ as above and the associated monomial basis $\mathscr{B}$ of monomials in $\boldsymbol{x}$ of the finite dimensional vector space $\mathcal{A}_{\mathbb{K}}$. The quotient ring $\mathcal{A}_{\mathbb{K}}$ has dimension δ. Note that by the regularity assumption, the codimension of the ideal generated by $f_1, \dots, f_p$ is p if this ideal is not $\langle 1 \rangle$. Hence, combined with Assumption A, this forces $p = n$ and by Bézout's inequality, we have $\delta \le d^n$. We recall below Assumption B.

For any $p \in \mathscr{G}$, we have $\deg p = \deg_{\boldsymbol{x}} p$.

By [21, Prop. 20], Assumption B holds for *generic* sequences $\boldsymbol{f}$.

Lemma 3.4. *Under Assumption B, $\deg_{\boldsymbol{y}}(\mathrm{lc}_{\boldsymbol{x}}(p)) = 0$ for all $p \in \mathscr{G}$.*

Proof. Let $p \in \mathscr{G}$, by definition of the ordering $\texttt{grevlex}(\boldsymbol{x}) \succ \texttt{grevlex}(\boldsymbol{y})$, $\mathrm{lc}_{\boldsymbol{x}}(p)$ is obtained from a term τ in p s.t. $\deg_{\boldsymbol{x}}(\tau) = \deg_{\boldsymbol{x}}(p)$. By Assumption B, $\deg_{\boldsymbol{x}}(p) = \deg(p)$, so $\deg_{\boldsymbol{y}}(\tau) = 0$. □

Lemma 3.5. *If Assumption B holds, then for any $q \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$, the normal form $\overline{q}$ of q w.r.t. $\mathscr{G}$ lies in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ and $\deg(\overline{q}) \le \deg(q)$.*

Proof. Let $q \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$, $\overline{q}$ is the remainder of successive divisions of q by polynomials in $\mathscr{G}$. As Assumption B holds, by Lemma 3.4, those divisions do not introduce any denominator. So, every term appearing during these reductions are polynomials in $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$. By Assumption B, for any $p \in \mathscr{G}$, the total degree of every term of p is bounded by $\deg_{\boldsymbol{x}}(p) = \deg(\mathrm{lm}_{\boldsymbol{x}}(p))$ by Lemma 3.4. Thus, a division of q by p involves only terms of total degree $\deg(q)$. Therefore, during the normal form reduction of q by $\mathscr{G}$, only terms of degree at most $\deg(q)$ will appear. Hence $\deg(\overline{q}) \le \deg(q)$. □

We prove now degree bounds on the entries of L_g and $\mathcal{H}_g$.

Lemma 3.6. *Under Assumption B, let $g \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ and let us denote by $(g_{i,j})_{1 \le i,j \le \delta}$ the matrix of L_g in the basis $\mathscr{B}$. Then, for all $1 \le i, j \le \delta$, $g_{i,j} \in \mathbb{Q}[\boldsymbol{y}]$ and $\deg(g_{i,j}) \le \deg(g) + \deg(b_j) - \deg(b_i)$.*

Proof. We have for all $1 \le j \le \delta$, $\overline{gb_j} = \sum_{i=1}^{\delta} g_{i,j} b_i$ and $g_{i,j} \in \mathbb{Q}[\boldsymbol{y}]$ by Lemma 3.5. Also, $\deg(\overline{gb_j}) = \max \deg(g_{i,j} b_i)$ because $g_{i,j} \in \mathbb{Q}[\boldsymbol{y}]$ and the b_i's are distinct monomials in $\boldsymbol{x}$. In particular, for all $1 \le i \le \delta$, $\deg(g_{i,j} b_i) = \deg(g_{i,j}) + \deg(b_i) \le \deg(\overline{gb_j}) \le \deg(gb_j) \le \deg(g) + \deg(b_j)$ by Lemma 3.5. The result follows. □

Proposition 3.7. *Under Assumption B, let $g \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ and let us denote by $(h_{i,j})_{1 \le i,j \le \delta}$ the Hermite matrix $\mathcal{H}_g$ associated to $(\boldsymbol{f}, g)$ in the basis $\mathscr{B}$. Then, for all $1 \le i, j \le \delta$, $h_{i,j} \in \mathbb{Q}[\boldsymbol{y}]$ and*

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

As a direct consequence, the degree of a minor of $\mathcal{H}_g$ defined by the rows $(r_1, \dots, r_k)$ and the columns $(c_1, \dots, c_k)$ is bounded by

$$k \deg(g) + \sum_{i=1}^{k} (\deg(b_{r_i}) + \deg(b_{c_i})).$$

Hence, the determinant of $\mathcal{H}_g$ has degree bounded by $\delta \deg(g) + 2 \sum_{i=1}^{\delta} \deg(b_i)$ and $\delta \le d^n$.

Proof. We have $h_{i,j} = \mathrm{Tr}(L_{gb_ib_j})$. Let $C = (c_{k,\ell})_{1 \le k, \ell \le \delta}$ denote the entries of the matrix of $L_{gb_ib_j}$ w.r.t. $\mathscr{B}$. By Lemma 3.6, as $gb_ib_j \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$, $C \in \mathbb{Q}[\boldsymbol{y}]^{\delta \times \delta}$. So, $h_{i,j} = \mathrm{Tr}(C) = \sum_{k=1}^{\delta} c_{k,k} \in \mathbb{Q}[\boldsymbol{y}]$. By Lemma 3.6, $\deg(h_{i,j}) \le \max_k \deg(c_{k,k}) \le \max_k \deg(gb_ib_j)$. Therefore, $\deg(h_{i,j}) \le \deg(g) + \deg(b_i) + \deg(b_j)$.

The degree bound for the minors of $\mathcal{H}_g$ is clear by expanding the expression for determinants. □

Corollary 3.8. *Assume that $\boldsymbol{f}$ is an affine regular sequence satisfying B. For $g \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$, the degree of any minor of $\mathcal{H}_g$ is bounded by $(\deg(g) + n(d-1))d^n$.*

Proof. Since $\boldsymbol{f}$ is an affine regular sequence, one can apply [21, Lem. 23]. Hence, the highest degree among the elements of $\mathscr{B}$ is bounded by $n(d-1)$ and it holds that $2 \sum_{i=1}^{\delta} \deg(b_i) \le n(d-1)d^n$. Substituting these degree bounds on the b_i's in the ones of Proposition 3.7 ends the proof. □

4 ALGORITHM

Let $\boldsymbol{Q} = (Q_1, \dots, Q_s) \subset \mathbb{Q}[\boldsymbol{X}]$ for $\boldsymbol{X} = (X_1, \dots, X_k)$. Let $\mathcal{Z}$ be a subset of $\mathbb{R}^k$. We say that an element $\sigma \in \{0, 1, -1\}^s$ is a sign condition for $\boldsymbol{Q}$. A sign condition σ for $\boldsymbol{Q}$ is said to be realizable over $\mathcal{Z}$ if the following set is nonempty

$$\mathrm{Reali}(\sigma, \mathcal{Z}) := \{x \in \mathcal{Z} \mid \bigwedge_{i=1}^{s} \mathrm{sign}(Q_i(x)) = \sigma(i)\}.$$

We consider the set $\mathrm{SIGN}(\boldsymbol{Q}, \mathcal{Z}) \subseteq \{0, 1, -1\}^s$ of realizable sign conditions for $\boldsymbol{Q}$ over $\mathcal{Z}$.

Let $\boldsymbol{f}$ and $\boldsymbol{g}$ be an instance of Problem 1. We are interested in the set of sign conditions $\mathrm{SIGN}(\boldsymbol{g}, \mathcal{V}_{\mathbb{R}})$. We describe an algorithm for the determination of the realizable sign conditions for $\boldsymbol{g}$ over the real solutions of $\boldsymbol{f} = 0$ when $\boldsymbol{f}$ satisfies Assumption A. This algorithm does not recover the whole set $\mathrm{SIGN}(\boldsymbol{g}, \mathcal{V}_{\mathbb{R}})$, but only the set of realizable conditions for $\boldsymbol{g}$ over $\mathcal{V}_{\mathbb{R}} \cap \mathcal{W}$ where $\mathcal{W}$ is a nonempty Zariski open subset of $\mathbb{C}^{t+n}$. It means that we potentially miss some elements of $\mathrm{SIGN}(\boldsymbol{g}, \mathcal{V}_{\mathbb{R}})$ but they can only occur for $(\boldsymbol{y}, \boldsymbol{x})$ lying in a Zariski closed set. Also, as a by-product our algorithm enables us to compute a valid solution to Problem 1 for $(\boldsymbol{f}, \boldsymbol{g})$.

This algorithm is a variant of [2, Chap. 10] for determining the sign conditions realized by a family of polynomials on a finite set of points in $\mathbb{R}^k$ using Tarski-queries. Tarski-queries are expressed as signatures of parametric Hermite matrices as in Corollary 3.2. We also use sample points algorithms as in [21, 26]. In the case where $\boldsymbol{g}$ is empty, this algorithm coincides with the one in [21].

4.1 Sign determination on a finite set of points

We are given a family of polynomials $\boldsymbol{Q} = (Q_1(\boldsymbol{X}), \dots, Q_s(\boldsymbol{X})) \subset \mathbb{Q}[\boldsymbol{X}]$ with $\boldsymbol{X} = (X_1, \dots, X_k)$ and an *implicit* finite set of points Z in $\mathbb{R}^k$ of size r. By implicit we mean that we have no explicit description for the points in Z. Typically, the set Z designates the roots of the system $\boldsymbol{f}(\eta, \cdot) = 0$ with η in the space of parameters and $\boldsymbol{Q}$ is the family $\boldsymbol{g}(\eta, \cdot)$. For now we assume that we have access to a black-box for computing the Tarski-queries $\mathrm{TaQ}(Q, Z)$ for any $Q \in \mathbb{Q}[\boldsymbol{X}]$. We aim at computing $\mathrm{SIGN}(\boldsymbol{Q}, Z)$.

For a sign condition $\sigma \in \{0, 1, -1\}^s$ for $\boldsymbol{Q}$, define $c(\sigma, Z) := \sharp\,\mathrm{Reali}(\sigma, Z)$ and, for $\alpha \in \{0, 1, 2\}^s$, denote $\boldsymbol{Q}^\alpha := \prod_{i=1}^s Q_i^{\alpha(i)}$, and $\sigma^\alpha := \prod_{i=1}^s \sigma(i)^{\alpha(i)}$. One can notice that on $\mathrm{Reali}(\sigma, Z)$, the sign of $\boldsymbol{Q}^\alpha$ is fixed and equal to σ^α.

We also order $\{0, 1, -1\}^s$ with the lexicographic order induced by $0 < 1 < -1$ and $\{0, 1, 2\}^s$ with the lexicographic order induced by $0 < 1 < 2$. Let $\Sigma = \{\sigma_1, \dots, \sigma_p\} \subset \{0, 1, -1\}^s$ with $\sigma_1 <_{\mathrm{lex}} \cdots <_{\mathrm{lex}} \sigma_p$, we denote by $c(\Sigma, Z)$ the column vector $(c(\sigma_1, Z), \dots, c(\sigma_p, Z))^t$. Similarly, let $A = \{\alpha_1, \dots, \alpha_m\} \subset \{0, 1, 2\}^s$ with $\alpha_1 <_{\mathrm{lex}} \cdots <_{\mathrm{lex}} \alpha_m$, we denote by $\mathrm{TaQ}(\boldsymbol{Q}^A, Z)$ the column vector $(\mathrm{TaQ}(\boldsymbol{Q}^{\alpha_1}, Z), \dots, \mathrm{TaQ}(\boldsymbol{Q}^{\alpha_m}, Z))^t$.

We define the matrix of signs of A on Σ as the $m \times p$ matrix $\mathrm{Mat}(A, \Sigma)$ whose entry (i, j) is $\sigma_j^{\alpha_i}$.

Proposition 4.1 ([2, Prop. 10.59]). *If $\mathrm{SIGN}(\boldsymbol{Q}, Z) \subseteq \Sigma$, then it holds that $\mathrm{Mat}(A, \Sigma) \cdot c(\Sigma, Z) = \mathrm{TaQ}(\boldsymbol{Q}^A, Z)$.*

Hence, when $\mathrm{Mat}(A, \Sigma)$ is invertible, one can determine $c(\Sigma, Z)$ and thus $\mathrm{SIGN}(\boldsymbol{Q}, Z) = \{\sigma \in \Sigma \mid c(\sigma, Z) > 0\}$ from $\mathrm{TaQ}(\boldsymbol{Q}^A, Z)$ by linear system solving. In this case, we say that the set A is adapted to Σ for sign determination. If one chooses $\Sigma = \{0, 1, -1\}^s$ to be the whole set of possible sign conditions for $\boldsymbol{Q}$, the only adapted set to Σ is $A = \{0, 1, 2\}^s$ as we need $\mathrm{Mat}(A, \Sigma)$ to be square. In this case $\mathrm{Mat}(A, \Sigma)$ is invertible [2, Prop. 10.60]. However, we need to compute 3^s Tarski-queries to perform sign determination. Yet the number of realizable sign conditions is bounded by the number r of elements in Z and often $r \ll 3^s$. So when $\Sigma = \{0, 1, -1\}^s$, many entries in $c(\Sigma, Z)$ are equal to 0. To avoid to compute an exponential number of Tarski-queries, we want to avoid unrealizable sign conditions. To do so, we use the incremental approach of [2, Sec. 10.3]. Let $\boldsymbol{Q}_i := (Q_{s-i+1}, \dots, Q_s)$ be the last i polynomials in $\boldsymbol{Q}$. At step i, we compute $\mathrm{SIGN}(\boldsymbol{Q}_i, Z)$ the realizable sign conditions for $\boldsymbol{Q}_i$, for i from 1 to s, so that we get rid of the empty sign conditions at each step of the computation.

First for any $\Sigma \subseteq \{0, 1, -1\}^s$, we explain how to construct a set $A \subseteq \{0, 1, 2\}^s$ that is adapted to Σ. For $\sigma = (\sigma(1), \dots, \sigma(s)) \in \{0, 1, -1\}^s$, we denote by σ' the vector obtained by removing the first coordinate of σ, *i.e.* $\sigma' := (\sigma(2), \dots, \sigma(s)) \in \{0, 1, -1\}^{s-1}$.

Definition 4.2. *For $\Sigma \subseteq \{0, 1, -1\}^s$, we define $\Sigma'_1 := \{\sigma' \mid \sigma \in \Sigma\}$, and the subsets $\Sigma'_2, \Sigma'_3 \subseteq \Sigma'_1$ such that Σ'_2 (resp. Σ'_3) contains the elements of Σ'_1 that can be extended to an element of Σ in at least two different ways (resp. exactly three different ways).*

Definition 4.3. *Let $\Sigma \subseteq \{0, 1, -1\}^s$, we define $\mathrm{Ada}(\Sigma) \in \{0, 1, 2\}^s$ by induction on $s \geq 1$ as follows:*

- *if $s = 1$, let $h \in \{1, 2, 3\}$ be the size of Σ, and set $\mathrm{Ada}(\Sigma) = \{0, \dots, h-1\}$;*
- *if $s > 1$, $\mathrm{Ada}(\Sigma) = 0 \times \mathrm{Ada}(\Sigma'_1) \cup 1 \times \mathrm{Ada}(\Sigma'_2) \cup 2 \times \mathrm{Ada}(\Sigma'_3)$.*

```
Algorithm 1: One step of sign determination
Input  : $\boldsymbol{Q} = \{Q\} \cup \boldsymbol{Q}'$, the sets $\Sigma := \mathrm{SIGN}(\boldsymbol{Q}', Z)$ and
         $\mathrm{Ada}(\Sigma)$, the associated matrix of signs
         $\mathrm{Mat}(\mathrm{Ada}(\Sigma), \Sigma)$
Output : The sets $\mathrm{SIGN}(\boldsymbol{Q}, Z)$, $\mathrm{Ada}(\mathrm{SIGN}(\boldsymbol{Q}, Z))$ and the
         associated matrix of signs
Compute $S := \mathrm{SIGN}(Q, Z)$ from the Tarski-queries
  $\mathrm{TaQ}(1, Z), \mathrm{TaQ}(Q, Z), \mathrm{TaQ}(Q^2, Z)$ by solving (2). $S$
  corresponds to the nonzero entry of the solution
Deduce $A := \mathrm{Ada}(S)$ from Definition 4.3
Compute the vector $T := \mathrm{TaQ}(\boldsymbol{Q}^{A \times \mathrm{Ada}(\Sigma)}, Z)$
$M \leftarrow \mathrm{Mat}(A \times \mathrm{Ada}(\Sigma), S \times \Sigma) = \mathrm{Mat}(A, S) \otimes \mathrm{Mat}(\mathrm{Ada}(\Sigma), \Sigma)$
Compute $c := c(S \times \Sigma, Z)$ by solving $M \cdot c = T$
Deduce $\mathrm{SIGN}(\boldsymbol{Q}, Z)$ # given by the nonzero entries in c
Delete in $M$ the columns whose index is not in $\mathrm{SIGN}(\boldsymbol{Q}, Z)$
Deduce $\mathrm{Ada}(\mathrm{SIGN}(\boldsymbol{Q}, Z))$ from the row rank profile of $M$
  and delete the other rows.
```

Proposition 4.4. *[2, Prop. 10.65] The set $\mathrm{Ada}(\Sigma)$ is adapted to Σ for sign determination.*

Now suppose that for $1 \leq i < s$, we have built $\mathrm{SIGN}(\boldsymbol{Q}_i, Z)$ and $\mathrm{Ada}(\mathrm{SIGN}(\boldsymbol{Q}_i, Z))$, we explain how we can compute $\mathrm{SIGN}(\boldsymbol{Q}_{i+1}, Z)$ and $\mathrm{Ada}(\mathrm{SIGN}(\boldsymbol{Q}_{i+1}, Z))$. It is based on the two following lemmas.

Lemma 4.5. *Let $s_1, s_2 \geq 0$, and $A_1 \subseteq \{0, 1, 2\}^{s_1}$, $A_2 \subseteq \{0, 1, 2\}^{s_2}$, $\Sigma_1 \subseteq \{0, 1, -1\}^{s_1}$, $\Sigma_2 \subseteq \{0, 1, -1\}^{s_2}$. The matrix of signs of $A_1 \times A_2$ on $\Sigma_1 \times \Sigma_2$ is $\mathrm{Mat}(A_1 \times A_2, \Sigma_1 \times \Sigma_2) = \mathrm{Mat}(A_1, \Sigma_1) \otimes \mathrm{Mat}(A_2, \Sigma_2)$. As a consequence, if A_1 is adapted to Σ_1 and A_2 is adapted to Σ_2 then $A_1 \times A_2$ is adapted to $\Sigma_1 \times \Sigma_2$.*

Proof. Let $\alpha = (\alpha_1, \alpha_2) \in A_1 \times A_2$ and $\sigma = (\sigma_1, \sigma_2) \in \Sigma_1 \times \Sigma_2$. By definition, we have $\sigma^\alpha = \sigma_1^{\alpha_1} \cdot \sigma_2^{\alpha_2}$. Since rows and columns of matrices of signs are ordered with the lexicographic orderings induced by $0 < 1 < 2$ for the rows and $0 < 1 < -1$ for the columns, the result holds. □

Lemma 4.6 (See [2, Lem. 10.66]). *Let $\Sigma \subseteq \Gamma \subseteq \{0, 1, -1\}^s$ and $p = \sharp\Sigma$. The matrix $\mathrm{Mat}(\mathrm{Ada}(\Sigma), \Sigma)$ is the matrix obtained by extracting the first p linearly independent rows of $\mathrm{Mat}(\mathrm{Ada}(\Gamma), \Sigma)$.*

The computation of $\mathrm{SIGN}(\boldsymbol{Q}_{i+1}, Z)$ and $\mathrm{Ada}(\mathrm{SIGN}(\boldsymbol{Q}_{i+1}, Z))$ is described in Algorithm 1. After s iterations of this algorithm we get $\mathrm{SIGN}(\boldsymbol{Q}, Z)$. This is [2, Alg. 10.11].

4.2 General sign determination

We design an algorithm based on Algorithm 1 to solve Problem 1.

Let $\boldsymbol{f} = (f_1, \dots, f_p) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ such that $\boldsymbol{f}$ satisfies Assumption A and let $\boldsymbol{g} = (g_1, \dots, g_s) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ define the inequalities of our input system. As before, let $\mathscr{G}$ be the reduced Gröbner basis of $\langle \boldsymbol{f} \rangle$ w.r.t. the ordering $\mathtt{grevlex}(\boldsymbol{x}) \succ \mathtt{grevlex}(\boldsymbol{y})$. We also denote by $\mathbb{K}$ the field $\mathbb{Q}(\boldsymbol{y})$ and $\mathscr{B} \subset \mathbb{Q}[\boldsymbol{x}]$ is the basis of $\mathcal{A}_{\mathbb{K}} := \mathbb{K}[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle_{\mathbb{K}}$ derived from $\mathscr{G}$ of dimension δ.

Let $g \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$, $\mathcal{H}_g \in \mathbb{K}^{\delta \times \delta}$ denotes the Hermite matrix associated to $(\boldsymbol{f}, g)$ in $\mathscr{B}$. We consider as in (3), the algebraic set $\mathcal{W}_\infty = \cup_{p \in \mathscr{G}} V(\mathrm{lc}_{\boldsymbol{x}}(p)) \subset \mathbb{C}^t$.

Lemma 4.7. *Let r denotes the rank of $\mathcal{H}_g$. There exists a Zariski dense subset $\mathcal{U}_g$ of $\mathrm{GL}_\delta(\mathbb{C})$ such that for $U \in \mathcal{U}_g$, the first r leading principal minors of $\mathcal{H}_g^U := U^t \mathcal{H}_g U$ are not identically zero.*

Proof. The matrix $\mathcal{H}_g$ has rank r so there exists $\eta \in \mathbb{R}^t \setminus \mathcal{W}_\infty$ such that the evaluation $\mathcal{H}_g(\eta)$ is a matrix of rank r. Moreover, for all $U \in \mathrm{GL}_\delta(\mathbb{C})$, $\mathcal{H}_g^U(\eta) = U^t \mathcal{H}_g(\eta) U$. We show that there exists a Zariski dense subset $\mathcal{U}_g$ such that for all $U \in \mathcal{U}_g$, the first r leading principal minors of $\mathcal{H}_g^U(\eta)$ are nonzero. This would imply that the first r leading principal minors of $\mathcal{H}_g^U$ are not identically zero.

For $1 \leq j \leq r$, let us denote by $\mathcal{M}_j$ the set of all $j \times j$ minors of $\mathcal{H}_g(\eta)$. We consider the matrix $U := (\mathfrak{u}_{i,j})_{1 \leq i,j \leq \delta}$ where $\mathfrak{u} = (\mathfrak{u}_{i,j})$ are new indeterminates. Then, the j-th leading principal minor $M_j(\mathfrak{u})$ of the matrix $\mathcal{H}_g^U(\eta)$ can be written as

$$M_j(\mathfrak{u}) = \sum_{m \in \mathcal{M}_j} u_m \cdot m,$$

where the u_m's are elements of $\mathbb{Q}[\mathfrak{u}]$. As $\mathcal{H}_g(\eta)$ is a real symmetric matrix of rank r there exists a matrix $Q \in \mathrm{GL}_\delta(\mathbb{R})$ such that

$$\mathcal{H}_g^Q(\eta) = Q^t \mathcal{H}_g(\eta) Q = \begin{bmatrix} \Delta & 0 \\ 0 & 0 \end{bmatrix},$$

where Δ is a diagonal matrix of size r with nonzero real entries on its diagonal. Hence the evaluation of $\mathfrak{u}$ at the entries of Q gives $M_j(\mathfrak{u})$ a nonzero value. So we conclude that $M_j(\mathfrak{u})$ is not identically zero.

Finally, let $\mathcal{U}_j$ be the nonempty Zariski open subset of $\mathrm{GL}_\delta(\mathbb{C})$ defined as the non-vanishing set of $M_j(\mathfrak{u})$. We define $\mathcal{U}_g$ as the intersection of $\mathcal{U}_j$ for $1 \leq j \leq r$, and for $U \in \mathcal{U}_g$, none of the first r leading principal minors of $\mathcal{H}_g^U(\eta)$ is zero. Thus, none of the first r leading principal minors of $\mathcal{H}_g^U$ is identically zero. □

Lemma 4.8. *Let S be a symmetric matrix in $\mathbb{R}^{\delta \times \delta}$ of rank r and let S_i be its i-th leading principal minor for $0 \leq i \leq \delta$. We assume that $S_i \neq 0$ for $i \leq r$. Then, the signature of S equals $r - 2v$ where v is the number of sign variations in $S_0, \ldots, S_r$.*

Proof. We have

$$S = \begin{bmatrix} \widetilde{S} & V^t \\ V & W \end{bmatrix} = \begin{bmatrix} I_r & 0 \\ V\widetilde{S}^{-1} & I_{\delta-r} \end{bmatrix} \underbrace{\begin{bmatrix} \widetilde{S} & 0 \\ 0 & W - V\widetilde{S}^{-1}V^t \end{bmatrix}}_{R} \begin{bmatrix} I_r & \widetilde{S}^{-1}V^t \\ 0 & I_{\delta-r\cdot} \end{bmatrix}.$$

Thus S and R have the same signature. Since $\det(\widetilde{S}) = S_r \neq 0$, we have $\mathrm{rk}(\widetilde{S}) = r = \mathrm{rk}(S) = \mathrm{rk}(R)$. Therefore, $W - V\widetilde{S}^{-1}V^t = 0$ and $\mathrm{Sign}(R) = \mathrm{Sign}(\widetilde{S})$. By Theorem 2.5, $\mathrm{Sign}(\widetilde{S}) = r - 2v$. □

We use the previous lemmas as follows. Assume that after picking randomly a matrix $U \in \mathrm{GL}_\delta(\mathbb{C})$, the first r leading principal minors of $\mathcal{H}_g^U := U^t \cdot \mathcal{H}_g \cdot U$ are not identically zero, with r the rank of $\mathcal{H}_g$. Then over a connected component of the semi-algebraic set defined by the complementary of $\mathcal{W}_\infty$ and the non-vanishing set of these minors, the sign of each leading principal minor is invariant. Consequently the Tarski-query $\mathrm{TaQ}(\boldsymbol{f}(\eta, \cdot), g(\eta, \cdot))$ is invariant when η ranges over this connected component. Then by sampling at least one point in each connected component using the algorithm in [21] originating from [26], we are able to recover all the sign conditions satisfied by a family of polynomials $\boldsymbol{g}$ on a dense subset of $\mathcal{V}_\mathbb{R}$ the real algebraic set defined by $\boldsymbol{f} = 0$.

Algorithm 2 for solving Problem 1 uses the subroutines:

- **FirstHermiteMatrix** follows from Algorithm 1 in [21]. It takes as input a polynomial sequence $\boldsymbol{f}$ that satisfies Assumption A and outputs a Gröbner basis $\mathscr{G}$ of $\langle \boldsymbol{f} \rangle$ for the ordering $\mathtt{grevlex}(\boldsymbol{x}) \succ \mathtt{grevlex}(\boldsymbol{y})$, a monomial basis $\mathscr{B}$ of $\mathcal{A}_\mathbb{K}$ derived from $\mathscr{G}$, the family of multiplication matrices $(M_b)_{b \in \mathscr{B}}$ in $\mathscr{B}$, a polynomial $w_\infty \in \mathbb{Q}[\boldsymbol{y}]$ whose vanishing set is $\mathcal{W}_\infty$ defined in (3), and the Hermite matrix $\mathcal{H}_1$ associated to $(\boldsymbol{f}, 1)$ in $\mathscr{B}$.
- **LeadPrincMinors** returns the list of the numerators of the nonzero leading principal minors of a matrix with entries in $\mathbb{Q}(\boldsymbol{y})$.
- **SamplePoints** that takes as input a sequence of polynomials $(h_1, \ldots, h_\ell) \subset \mathbb{Q}[\boldsymbol{y}]$ and sample a finite set of points that meets every connected component of the semi-algebraic set defined by $h_1 \neq 0, \ldots, h_\ell \neq 0$.

For a family of polynomials $(Q_1, \ldots, Q_\ell) \subset \mathbb{Q}[\boldsymbol{y}]$ and $\eta \in \mathbb{R}^t$ the sign pattern of $(Q_i(\eta))_{1 \leq i \leq \ell}$ is the semi-algebraic formula Φ below

$$\Phi := \bigwedge_{i=1}^{\ell} \mathrm{sign}(Q_i) = \mathrm{sign}(Q_i(\eta)). \tag{4}$$

Theorem 4.9 (Correction). *Assume that $\boldsymbol{f}$ satisfies Assumption A. Let $\boldsymbol{g} = (g_1, \ldots, g_s)$ be a polynomial sequence. There exists a Zariski dense subset $\mathcal{U}$ of $\mathrm{GL}_\delta(\mathbb{C})$ such that if U is sampled in $\mathcal{U} \cap \mathbb{Q}^{\delta \times \delta}$, Algorithm 2 outputs a set Σ that is equal to $\mathrm{SIGN}(\boldsymbol{g}, \mathcal{V}_\mathbb{R} \cap \pi^{-1}(\mathcal{W}))$ where $\mathcal{V}_\mathbb{R}$ is the real algebraic set defined by $\boldsymbol{f}$ and $\mathcal{W}$ is a nonempty Zariski open subset of $\mathbb{C}^t$; and a solution to Problem 1 for $(\boldsymbol{f}, \boldsymbol{g})$.*

Proof. For $1 \leq i \leq s$, let Σ_i be the value of Σ and Ada_i the value of Ada after the i-th iteration of the loop in line 5. We also define $\Sigma_0 := \emptyset$ and $\boldsymbol{g}_0 := \emptyset$.

We prove the following loop invariant: for all $0 \leq i \leq s$, there exists a Zariski dense subset $\mathcal{U}_i$ of $\mathrm{GL}_\delta(\mathbb{C})$ s.t. if U was sampled in $\mathcal{U}_i \cap \mathbb{Q}^{\delta \times \delta}$, then $\Sigma_i = \mathrm{SIGN}(\boldsymbol{g}_i, \mathcal{V}_\mathbb{R} \cap \pi^{-1}(\mathcal{W}_i))$ where $\mathcal{W}_i$ is the nonempty Zariski open subset in $\mathbb{C}^t$ defined as the non-vanishing locus of w_∞ and the polynomials in the set Minors obtained after performing the for loop starting at line 9.

This is true when entering the loop as $\Sigma_0 = \emptyset = \mathrm{SIGN}(\emptyset, \mathcal{V}_\mathbb{R})$.

Now suppose that the result holds for $0 \leq i - 1 < s$. Let $\Sigma^* := \{0, 1, -1\} \times \Sigma_{i-1}$ and $\mathrm{Ada}^* := \{0, 1, 2\} \times \mathrm{Ada}_{i-1}$. By Lemma 4.7, for each $\alpha \in \mathrm{Ada}^*$ there exists a Zariski dense subset $\mathcal{U}_\alpha$ of $\mathrm{GL}_\delta(\mathbb{C})$ such that if $U \in \mathcal{U}_\alpha$, the first rk_α (see line 10) leading principal minors of $U^t \cdot \mathcal{H}_{\boldsymbol{g}_i^\alpha} \cdot U$ are not identically 0. Let $\mathcal{U}_i := \mathcal{U}_{i-1} \cap \bigcap_{\alpha \in \mathrm{Ada}^*} \mathcal{U}_\alpha$. It is a Zariski dense subset of $\mathrm{GL}_\delta(\mathbb{C})$ and we further suppose that U was sampled in $\mathcal{U}_i \cap \mathbb{Q}^{\delta \times \delta}$. In particular $U \in \mathcal{U}_{i-1}$, so by the induction hypothesis, $\Sigma_{i-1} = \mathrm{SIGN}(\boldsymbol{g}_{i-1}, \mathcal{V}_\mathbb{R} \cap \pi^{-1}(\mathcal{W}_{i-1}))$. Note that $\mathcal{W}_i$ is nonempty since all its defining polynomials are not identically 0 and $\mathcal{W}_i \subseteq \mathcal{W}_{i-1}$ as the set Minors can only increase along the iterations. We now show that $\Sigma_i = \mathrm{SIGN}(\boldsymbol{g}_i, \mathcal{V}_\mathbb{R} \cap \pi^{-1}(\mathcal{W}_i))$. Let $\mathcal{R}$ be the semi-algebraic set defined as the real trace of $\mathcal{W}_i$. Then the signs of the first rk_α leading principal minors of $U^t \cdot \mathcal{H}_{\boldsymbol{g}_i^\alpha}(\eta) \cdot U$ are invariant when η ranges over a connected component C of $\mathcal{R}$. By Lemma 4.8, the vector $T_\eta := (\mathrm{Sign}(\mathcal{H}_{\boldsymbol{g}_i^\alpha}(\eta)))_{\alpha \in \mathrm{Ada}^*}$ is invariant when η varies over C. However, the set L defined at line 14 contains

```
Algorithm 2: Classification
  Input :
      – A polynomial sequence $\boldsymbol{f} = (f_1, \ldots, f_p) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ such
        that $\boldsymbol{f}$ satisfies Assumption A
      – A polynomial sequence $\boldsymbol{g} = (g_1, \ldots, g_s) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$
  Output:
      – A set $\Sigma \subseteq \{0, 1, -1\}^s$ of sign conditions satisfied by $\boldsymbol{g}$ on the
        real algebraic set defined by $\boldsymbol{f}$
      – The description of a collection of semi-algebraic sets $\mathcal{T}_i$
        solving Problem 1
1  $\mathcal{H}_1, w_\infty, \mathscr{G}, \mathscr{B}, (M_b)_{b\in\mathscr{B}} \leftarrow$ FirstHermiteMatrix($\boldsymbol{f}$)
2  Choose randomly a matrix $U \in \mathbb{Q}^{\delta\times\delta}$
3  $\Sigma \leftarrow \emptyset$, Ada $\leftarrow \emptyset$, $M \leftarrow \mathrm{Mat}(\mathrm{Ada}, \Sigma)$
4  Minors $\leftarrow \emptyset$
5  for $i$ from 1 to $s$ do
6      $\boldsymbol{g}_i \leftarrow (g_{s-i+1}, \ldots, g_s)$
7      $\Sigma \leftarrow \{0, 1, -1\} \times \Sigma$, Ada $\leftarrow \{0, 1, 2\} \times$ Ada,
8      $M \leftarrow \mathrm{Mat}(\mathrm{Ada}, \Sigma) = \mathrm{Mat}(\{0, 1, 2\}, \{0, 1, -1\}) \otimes M$
9      for $\alpha \in$ Ada do
10         Compute $\mathcal{H}_{\boldsymbol{g}_i^\alpha}$ using the algorithm of Section 3.1
             and let $\mathrm{rk}_\alpha$ be its rank
11         $(h_1^\alpha, \ldots, h_{\mathrm{rk}_\alpha}^\alpha) \leftarrow$ LeadPrincMinors($U^t \cdot \mathcal{H}_{\boldsymbol{g}_i^\alpha} \cdot U$)
12         Minors $\leftarrow$ Minors $\cup \{h_1^\alpha, \ldots, h_{\mathrm{rk}_\alpha}^\alpha\}$
13     end
14     $L \leftarrow$ SamplePoints($w_\infty \neq 0 \wedge$ Minors $\neq 0$)
15     for $\eta \in L$ do
16         $T_\eta \leftarrow \left(\mathrm{Sign}(\mathcal{H}_{\boldsymbol{g}_i^\alpha}(\eta))\right)_{\alpha\in\mathrm{Ada}}$
17         Solve $M \cdot c_\eta = T_\eta$ to compute $c_\eta$
18         Deduce $\Sigma_\eta$ corresponding to nonzero entries in $c_\eta$
19     end
20     $\Sigma \leftarrow \bigcup_{\eta\in L} \Sigma_\eta$
21     Delete in $M$ columns whose index is not in $\Sigma$
22     Deduce Ada = Ada($\Sigma$) from the rank row profile of $M$
         and delete the other rows
23 end
24 for $\eta \in L$ do
25     $\Phi_\eta \leftarrow$ Sign pattern of $(h_j^\alpha(\eta))$ for $\alpha \in$ Ada and
         $1 \leq j \leq \mathrm{rk}_\alpha$ as in (4)
26     $r_\eta \leftarrow$ entry of $c_\eta$ corresponding to
         $(1, 1, \ldots, 1) \in \{0, 1, -1\}^s$
27 end
28 return $\Sigma$, $(\Phi_\eta \wedge w_\infty \neq 0 \wedge \text{Minors} \neq 0, \eta, r_\eta)_{\eta\in L}$
```

at least one point in each connected component of $\mathcal{R}$. So we have $\{T_\eta \mid \eta \in \mathcal{R}\} = \{T_\eta \mid \eta \in L\}$. Moreover, by the induction hypothesis, for all $\eta \in \mathcal{R}$, we have $\mathrm{SIGN}(\boldsymbol{g}_{i-1}, \mathcal{V}_\mathbb{R} \cap \pi^{-1}(\eta)) \subseteq \Sigma_{i-1}$ since $\eta \in \mathcal{W}_{i-1}$. Thus for all $\eta \in \mathcal{R}$, we have

$$\Sigma_\eta := \mathrm{SIGN}(\boldsymbol{g}_i, \mathcal{V}_\mathbb{R} \cap \pi^{-1}(\eta)) \subseteq \{0, 1, -1\} \times \Sigma_{i-1} =: \Sigma^*.$$

As a consequence of Proposition 4.1, Σ_η corresponds to the nonzero entries of $c_\eta := \mathrm{Mat}(\Sigma^*, \mathrm{Ada}^*)^{-1} \cdot T_\eta = M^{-1} \cdot T_\eta$. Since M does not depend on η, it holds that Σ_η is invariant over a connected component of $\mathcal{R}$. Finally,

$$\begin{aligned}\mathrm{SIGN}(\boldsymbol{g}_i, \mathcal{V}_\mathbb{R} \cap \pi^{-1}(\mathcal{W}_i)) &= \mathrm{SIGN}(\boldsymbol{g}_i, \mathcal{V}_\mathbb{R} \cap \pi^{-1}(\mathcal{R})) \\ &= \bigcup_{\eta\in\mathcal{R}} \Sigma_\eta = \bigcup_{\eta\in L} \Sigma_\eta = \Sigma_i.\end{aligned}$$

Hence Algorithm 2 outputs a set Σ describing all the sign conditions realised by $\boldsymbol{g}$ on $\mathcal{V}_\mathbb{R} \cap \pi^{-1}(\mathcal{W})$ for $\mathcal{W}$ a nonempty Zariski open subset of $\mathbb{C}^t$. Finally, we show that the output of Algorithm 2: $(\Phi_\eta \wedge w_\infty \neq 0 \wedge \text{Minors} \neq 0, \eta, r_\eta)_{\eta\in L}$ is a solution for Problem 1. For $\eta \in L$, let $\mathcal{T}_\eta$ be the semi-algebraic set defined by $\Phi_\eta \wedge w_\infty \neq 0 \wedge \text{Minors} \neq 0$. By construction, $c_{\eta'}$ is invariant when η' varies over $\mathcal{T}_\eta$ and its first entry equals r_η that is exactly $\sharp\mathcal{V}_\mathbb{R} \cap \pi^{-1}(\eta')$. The union of the sets $\mathcal{T}_\eta$ is $\mathbb{R}^t \setminus \mathcal{W}$; it is dense in $\mathbb{R}^t$. □

4.3 Complexity analysis

Further, we use the following notation for integers a, b, c:

$$\mathscr{T}_{a,b,c} = \binom{a+b+c}{a} \text{ and } \mathscr{M}_{a,b} = \binom{a+b}{a}.$$

Note that one can evaluate a multivariate polynomial of degree at most D in k variables within $O(\mathscr{M}_{D,k})$ arithmetic operations.

Let $\boldsymbol{f} = (f_1, \ldots, f_p) \subseteq \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ be a regular sequence satisfying Assumptions A and B and $\boldsymbol{g} = (g_1, \ldots, g_s) \subseteq \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ a polynomial sequence. Let d be a bound on the degree of the polynomials in $\boldsymbol{f}$ and $\boldsymbol{g}$. We further assume that n, t and d are at least 2 as we are dealing with asymptotics. Let $2 < \omega \leq 3$ be an admissible exponent for matrix multiplication. We also denote $\lambda := n(d-1)$.

We prove that the arithmetic cost of each loop iteration in Algorithm 2 is dominated by the computation of the sample points at line 14. By [21, Prop. 26], the cost in terms of arithmetic operations in $\mathbb{Q}$ of the call to **FirstHermitematrix** at line 1 is at most

$$\widetilde{O}\left(\mathscr{M}_{t,2\lambda}\left(n\mathscr{T}_{d,t,n} + n^{\omega+1}d^{\omega n+1} + d^{(\omega+1)n}\right)\right). \tag{5}$$

Note that at loop iteration i the newly computed Hermite matrices are of the form $\mathcal{H} \cdot L_{g_i}, \mathcal{H} \cdot L_{g_i}^2$, where $\mathcal{H}$ is a Hermite matrix that has already been computed at the previous iteration and L_{g_i} is the matrix of the multiplication by g_i w.r.t. the basis $\mathscr{B}$ in $\mathcal{A}_\mathbb{K}$. So, each Hermite matrix is computed by multiplying a known Hermite matrix by one matrix of multiplication L_{g_i} for $1 \leq i \leq s$.

Lemma 4.10. *Under the above assumptions, let g be one of the g_i's, one can compute the matrix of multiplication L_g w.r.t. basis $\mathscr{B}$ within*

$$\widetilde{O}\left(\mathscr{T}_{t,d,\lambda}\left(\mathscr{T}_{d,t,n} + \mathscr{M}_{n,d}d^{\omega n} + n^{\omega+1}d^{\omega n+1}\right)\right)$$

arithmetic operations in $\mathbb{Q}$.

Proof. Let δ be the size of the Hermite matrix L_g. We already observed that $\delta \leq d^n$. We compute L_g by evaluation and interpolation using the multivariate interpolation algorithm of [6]. Because $\boldsymbol{f}$ satisfies Assumption B and is regular, by Lemma 3.6 and [21, Lem. 23], the matrix L_g has polynomial entries in $\boldsymbol{y}$ of degree at most $d + \lambda$. Thus we need $\mathscr{T}_{t,d,\lambda}$ interpolation points $\eta \in \mathbb{Q}^t$.

First we bound the cost of computing $L_g(\eta)$ for $\eta \in \mathbb{Q}^t$. We start by computing all the matrices $L_{x_i}(\eta)$. This is done in time $O(dn^{\omega+1}\delta^\omega) = O(n^{\omega+1}d^{\omega n+1})$ using [11, Algo. 4]. Then we evaluate g at η in time $O\left(\mathscr{T}_{d,t,n}\right)$. We write $g(\eta, \boldsymbol{x}) = \sum_m c_m m$ where $c_m \in \mathbb{Q}$ and m ranges over the set of monomials in $\boldsymbol{x}$ of degree at most d. There are $\mathscr{M}_{n,d}$ such monomials. We compute all the matrices $L_m(\eta)$ using $O(\mathscr{M}_{n,d}d^{\omega n})$ arithmetic operations by multiplying appropriately the matrices $L_{x_i}(\eta)$. Then, we compute $L_g(\eta) = \sum_m c_m L_m(\eta)$ in time $O(d^{2n}\mathscr{M}_{n,d})$. All in all, computing $L_g(\eta)$ uses $O\left(\mathscr{T}_{d,t,n} + \mathscr{M}_{n,d}d^{\omega n} + n^{\omega+1}d^{\omega n+1}\right)$ arithmetic operations in $\mathbb{Q}$. Hence, the whole evaluation step has an arithmetic cost lying in

$$O\left(\mathscr{T}_{t,d,\lambda}\left(\mathscr{T}_{d,t,n} + \mathscr{M}_{n,d}d^{\omega n} + n^{\omega+1}d^{\omega n+1}\right)\right).$$

Finally, we interpolate δ^2 entries which are polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree at most $d+\lambda$. So using multivariate interpolation [6], this is done in time $O\left(\delta^2\mathscr{T}_{t,d,\lambda}\log^2\mathscr{T}_{t,d,\lambda}\log\log\mathscr{T}_{t,d,\lambda}\right)$. Summing the cost of the two steps together ends the proof. □

Proposition 4.11. *Suppose that $\boldsymbol{f} = (f_1, \ldots, f_p) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ is a regular sequence satisfying Assumptions A and B. Then any parametric Hermite matrix $\mathcal{H}_g$ occurring in Algorithm 2 with $g \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ of degree d_g can be computed within*

$$\widetilde{O}\left(\mathscr{T}_{t,d_g,2\lambda}\left(d^{2n}\mathscr{T}_{t,d_g,2\lambda} + d^{\omega n}\right)\right) \tag{6}$$

arithmetic operations in $\mathbb{Q}$. Moreover, any minor of $\mathcal{H}_g$ can be computed using

$$\widetilde{O}\left(\mathscr{M}_{t,(d_g+\lambda)d^n}\left(d^{2n}\mathscr{T}_{t,d_g,2\lambda} + d^{\omega n}\right)\right) \tag{7}$$

arithmetic operations in $\mathbb{Q}$.

Proof. Again let $\delta \leq d^n$ be the size of the Hermite matrix $\mathcal{H}_g$. We write $g = g'g_i$ so that $\mathcal{H}_g = \mathcal{H}_{g'} \cdot L_{g_i}$ for some $1 \leq i \leq s$ and $\mathcal{H}_{g'}$ a parametric Hermite matrix that is already known. By Lemma 3.6 and Proposition 3.7, the matrices $\mathcal{H}_g, \mathcal{H}_{g'}$ and L_{g_i} have entries in $\mathbb{Q}[\boldsymbol{y}]$. Moreover, by [21, Lem. 23] the largest degree among the entries of $\mathcal{H}_g$ and $\mathcal{H}_{g'}$ is bounded by $\Lambda := d_g + 2\lambda$ and L_{g_i} has all its entries of degree at most $d+\lambda$. We compute the evaluations $\mathcal{H}_g(\eta) = \mathcal{H}_{g'}(\eta)\cdot L_{g_i}(\eta)$ for $\mathscr{M}_{t,\Lambda}$ distinct points $\eta \in \mathbb{Q}^t$, and then we interpolate the matrix $\mathcal{H}_g$ using the algorithm of [6].

Let $\eta \in \mathbb{Q}^t$. We first estimate the cost of computing $L_{g_i}(\eta)$. It is the evaluation of δ^2 polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree at most $d+\lambda$. So its cost is in $O\left(\mathscr{T}_{t,d,\lambda}\delta^2\right)$ arithmetic operations in $\mathbb{Q}$.

Similarly, we estimate the cost for computing $\mathcal{H}_{g'}(\eta)$. We obtain $O\left(\mathscr{M}_{t,\Lambda}\delta^2\right)$ arithmetic operations in $\mathbb{Q}$.

Finally, we need to compute the matrix product $\mathcal{H}_{g'}(\eta)L_{g_i}(\eta)$ and this is done in time $O(\delta^\omega)$. Notice that $\lambda - d = n(d-1) - d = nd - n - d \geq 0$, as $n \geq 2$ and $d \geq 2$. So $d + \lambda \leq \Lambda$. Summing up every step together we obtain that the evaluation $\mathcal{H}_g(\eta)$ can be computed within $O\left(\delta^2\mathscr{M}_{t,\Lambda} + \delta^\omega\right)$ arithmetic operations in $\mathbb{Q}$. Since there are $\mathscr{M}_{t,\Lambda}$ evaluation points, the whole evaluation step uses

$$O\left(\mathscr{M}_{t,\Lambda}\left(d^{2n}\mathscr{M}_{t,\Lambda} + d^{\omega n}\right)\right)$$

arithmetic operations in $\mathbb{Q}$ at most. Finally, we interpolate δ^2 entries which are polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree at most Λ. Using [6], the complexity of this step lies in $O\left(\delta^2\mathscr{M}_{t,\Lambda}\log^2\mathscr{M}_{t,\Lambda}\log\log\mathscr{M}_{t,\Lambda}\right)$. Summing up these costs, we obtain the claimed complexity for $\mathcal{H}_g$.

To compute the minors, we again use an evaluation-interpolation scheme. Any minor of $\mathcal{H}_g$ has degree at most $(d_g+\lambda)d^n$ by Corollary 3.8, so we need $\mathscr{M}_{t,(d_g+\lambda)d^n}$ interpolation points. Each evaluation of the matrix costs $O\left(\delta^2\mathscr{M}_{t,\Lambda}\right)$ and the computation of the minors lies in $O(\delta^\omega)$. We deduce the bound as before. □

One shows that the cost for computing the minors of $\mathcal{H}_g$ dominates the cost for computing the matrix $\mathcal{H}_g$. First note that

$$\mathscr{M}_{n,d} = \frac{(d+n)\ldots(d+1)}{n!} = d^n\prod_{k=1}^{n}\left(\frac{1}{d}+\frac{1}{k}\right) \leq 2d^n,$$

since $\frac{1}{d}+1 \leq 2$ and $\frac{1}{d}+\frac{1}{k} \leq 1$ for $k \geq 2$. Then, the cost in Lemma 4.10 is bounded by the cost (5) of **FirstHermiteMatrix**. In [21, Sec. 6.2], it is shown that (5) is bounded by $\widetilde{O}\left(\mathscr{M}_{t,\lambda d^n}\mathscr{M}_{t,2\lambda}d^{2n}\right)$. Thus the cost for computing L_{g_i} is bounded by (7). In addition, it holds that (6) is bounded by (7). Hence we can conclude that computing the minors dominates the cost of computing the matrices.

Now let us bound the cost of computing the set of sample points at Line 14. In Algorithm 2, we compute parametric Hermite matrices $\mathcal{H}_{\boldsymbol{g}^\alpha}$, with $\boldsymbol{g}^\alpha = \prod g_i^{\alpha_i}$ with $\alpha \in \{0,1,2\}^s$. So, the degree of g is bounded by $2ds$. Hence, the degree of any minor in Minors is bounded by $\mathfrak{D} := (2ds+\lambda)d^n$. Let r_i be the size of Σ at the end of iteration i of the loop. By [1], we have

$$r_i \leq r := \binom{s}{t}4^{t+1}d(2d-1)^{n+t-1}.$$

At iteration i, we compute at most $2r$ new Hermite matrices, so we add at most $2\delta r$ new minors in the set Minors. Let M_i be the size of the set Minors after the loop iteration i. We have $M_i \leq 2\delta ir \leq 2\delta sr$. So we call the routine **SamplePoints** with at most $2d^n sr$ polynomials, because as $\boldsymbol{f}$ satisfies Assumption B, we can omit $w_\infty = 1$. By [21, Thm. 2], the set of sample points L contains at most $(4d^n sr\mathfrak{D})^t$ points and this set can be computed using

$$\widetilde{O}\left(\mathscr{M}_{t,\mathfrak{D}}(2d^n sr)^{t+1}2^{3t}\mathfrak{D}^{2t+1}\right) \tag{8}$$

arithmetic operations in $\mathbb{Q}$. We can now prove Theorem 1.1.

Proof of Theorem 1.1. The sequence $\boldsymbol{f}$ is regular and satisfies both Assumptions A and B. At each iteration of Algorithm 2, the call to **SamplePoints** has a cost bounded by (8). We also compute at most $2r$ new Hermite matrices and their $\delta \leq d^n$ leading principal minors. By Proposition 4.11, this can be done using

$$\widetilde{O}\left(d^n r\mathscr{M}_{t,\mathfrak{D}}\left(d^{2n}\mathscr{T}_{t,2sd,2\lambda} + d^{\omega n}\right)\right)$$

arithmetic operations. Since $\mathscr{T}_{t,2sd,2\lambda} \in O\left(\mathfrak{D}^t\right)$, the above estimate is bounded by (8). Next, we have to evaluate the signatures of at most $3r$ Hermite matrices for every points $\eta \in L$. This is done by evaluating the sign patterns of the minors. There are at most $3\delta r$ minors of degree at most $\mathfrak{D}$ to evaluate at at most $(4d^n sr\mathfrak{D})^t$ points. This is done within $O\left(d^n r(4d^n sr\mathfrak{D})^t\mathscr{M}_{t,\mathfrak{D}}\right)$ arithmetic operations in $\mathbb{Q}$ and this is bounded by (8). The linear algebra to solve the linear systems $M \cdot c_\eta = T_\eta$ or to compute the rank row profile of M has a negligible cost in front of the evaluations of the minors. Finally we sum the costs for each of the s iterations and substitute the values of $\lambda, r, \mathfrak{D}$ to get the complexity estimate. The algorithm outputs $\sharp L \leq (4d^n sr\mathfrak{D})^t$ formulas. Each formula contains $O(d^n sr)$ minors of degree at most $\mathfrak{D}$. This completes the proof. □

5 PRACTICAL EXPERIMENTS

We report here on the practical behaviour of our algorithm and compare it with existing Maple packages based on other methods for solving parametric semi-algebraic systems. In Algorithm 2, we need to compute sample points per connected components of the non-vanishing set of leading principal minors of several Hermite matrices. Once we have computed these sample points, the semi-algebraic conditions for the classification are derived from the sign patterns of the minors on these points. However when facing practical problems, calling the **SamplePoints** routine with this number of minors is often the bottleneck of Algorithm 2. If we assume that for each inequality g_i with $1 \leq i \leq s$, the Hermite matrix $\mathcal{H}_{g_i}$ is nonsingular, one can get better timings in practice with the following approach:

- Compute a set $\{\eta_1, \ldots, \eta_\ell\}$ of sample points in the non-vanishing set of the determinants of $(\mathcal{H}_1, \mathcal{H}_{g_1}, \ldots, \mathcal{H}_{g_s})$. For $1 \leq i \leq \ell$, perform sign determination to obtain r_i the number of solutions of the specialized system $(\boldsymbol{f}(\eta_i, \cdot), \boldsymbol{g}(\eta_i, \cdot))$. One can show that we obtain all the possible number of solutions that the input system can admit.
- Next in order to get semi-algebraic conditions, compute the 3^s Hermite matrices $\mathcal{H}_{\boldsymbol{g}^\alpha}$ for all $\alpha \in \{0, 1, 2\}^s$ and all their leading principal minors. From each sign pattern τ on this family of minors, the signatures of the Hermite matrices are determined and one can associate $0 \leq r_\tau \leq \delta$ the number of solutions of the input system. Finally we derive a classification from the sign patterns τ such that $r_\tau \in \{r_1, \ldots, r_\ell\}$.

Notice that we get a classification with semi-algebraic formulas that contain clauses that may be infeasible. Yet we only need one call to the **SamplePoints** routine with $s + 1$ polynomials in input.

The timings are given in hours (h.), minutes (m.) and seconds (s.) and the computations have been performed on a PC Intel (R) Xeon (R) Gold 6244 CPU 3.6GHz with 1.5Tb of RAM. In our implementation, we compute Hermite matrices using FGb package [12] for Gröbner basis computation. For the sample points routine, we use RAGlib [25]. In Table 1, we analyse the costs on dense *generic* inputs, *i.e.* the input polynomials $(f_1, \ldots, f_n)$ and $(g_1, \ldots, g_s) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ are dense and randomly chosen among polynomials of degree d. We collect results for various values of (n, t, s, d). We focus on the timings for computing all the Hermite matrices (**hm**), all their leading principal minors (**min**). We also report in column **det** the timings for computing only the $(s + 1)$ matrices $(\mathcal{H}_1, \mathcal{H}_{g_1}, \ldots, \mathcal{H}_{g_s})$ and their determinants; and for computing sample points (column **sp**) in the non-vanishing locus of these determinants. We compare our algorithm with the Maple packages RootFinding[Parametric] [14] (the column RF) and RegularChains[ParametricSystemTools] [27].

In the column RF, we give the timings for the command DiscriminantVariety (**dv**) that computes a set of polynomials defining a discriminant variety $\mathcal{D}$ of the input system. For generic systems, the output of DiscriminantVariety coincides with the irreducible factors of the determinants of $(\mathcal{H}_1, \ldots, \mathcal{H}_{g_s})$ and the border polynomials returned by the command BorderPolynomial (**bp**) contains these polynomials. We also collect the results for the command CellDecomposition (**cad**) that outputs semi-algebraic formulas by computing an open CAD for $\mathbb{R}^t \setminus \mathcal{D}$.

				Hermite				RF		
n	t	s	d	**hm**	**min**	**det**	**sp**	**dv**	**cad**	**bp**
2	2	2	2	0.15 s	0.4 s	0.1 s	5 s	0.14 s	2 s	0.11 s
2	2	3	2	0.7 s	2 s	0.1 s	10 s	0.9 s	10 s	1 s
3	2	1	2	0.5 s	9 s	0.4 s	33 s	10 m	11 m	7 m
3	2	2	2	3 s	1 m	0.4 s	57 s	10 m	13 m	14 m
2	3	2	2	0.3 s	4 s	0.1 s	18m	0.7 s	>50 h	0.2 s
3	3	1	2	1 s	4 m	6 s	>50 h	>50 h	>50 h	>50 h
2	2	1	3	0.9 s	30 s	0.8 s	3m	52 m	57 m	47 s
2	2	2	3	5 s	5 m	1 s	6m	57 m	1h 16 m	2 m

Table 1: Generic dense system

The column **det** has to be compared with the two columns **dv** and **bp** as they are three different approaches to compute polynomials that defines the boundary of semi-algebraic sets over which the number of solutions of the input system is invariant.

We observe that our method outperforms DiscrimantVariety and BorderPolynomial. With our approach based on the minors of the Hermite matrices, we are not only able to solve the classification problem for systems faster by several orders of magnitude than what can be achieved with CellDecomposition (**cad**) and the command RealRootClassification of the RegularChains[ParametricSystemTools] library. We can also tackle problems that were previously out of reach.

Perspective-Three-Point Problem (P3P). We now consider a system coming from the P3P problem and apply our algorithm to find a classification. The problem consists in determining the position of a camera given the relative spatial location of 3 control points. As in [13], we want to compute a classification of the real solutions of the following system:

$$\begin{cases} 1 & = A^2 + B^2 - ABu \\ t & = B^2 + C^2 - BCv \\ x & = A^2 + C^2 - ACw \end{cases} \quad \text{with} \quad A > 0, B > 0, C > 0, \qquad \text{(P3P)}$$

subject to the following constraints: $x, t > 0$, $-2 < u, v, w < 2$, where A, B, C are the *variables* and x, t, u, v, w are *parameters*.

In [13], a special case of (P3P) is studied where $t = 1$. This restriction corresponds to the case where the three controls points form an isosceles triangle. In this case, a discriminant variety $\mathcal{D}$ for the system is computed in [13]. Sample points in the semi-algebraic set $\mathbb{R}^4 \setminus \mathcal{D}$ in order to deduce all the possible number of solutions of (P3P) in the isosceles case are computed using RAGlib but this is not sufficient to obtain semi-algebraic conditions that prescribe the number of real solutions to the input parametric system.

With our method, we are able to derive these semi-algebraic descriptions for each possible number of solutions from the signs of the leading principal minors of parametric Hermite matrices. In less than one hour, we compute all the minors and sample points in $\mathbb{R}^4 \setminus \mathcal{D}$ whence we obtain a complete classification in the isosceles case.

We also studied the general case. The system (P3P) has 3 variables and 5 parameters. We compute the first Hermite matrix $\mathcal{H}_1$ and the ones corresponding to each inequality $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_C$ and their determinants in a few seconds. This gives polynomials defining a discriminant variety of the system (P3P). Already this first step was out of reach using the Maple commands DiscriminantVariety or BorderPolynomial. Next we are able to compute the leading principal minors of all Hermite matrices of the form $\mathcal{H}_{A^{\alpha_1}B^{\alpha_2}C^{\alpha_3}}$ with $(\alpha_1, \alpha_2, \alpha_3) \in \{0, 1, 2\}^3$ and get semi-algebraic conditions for a classification. One further step would be to sample points outside the discriminant variety to get all the possible number of solutions of the system (P3P).

REFERENCES

[1] S. Basu, R. Pollack, and M.-F. Roy. On the betti numbers of sign conditions. *Proceedings of the American Mathematical Society*, 133(4):965–974, 2005.

[2] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, second edition, 2006.

[3] M. Ben-Or, D. Kozen, and J. Reif. The complexity of elementary algebra and geometry. In *Proceedings of the sixteenth annual ACM symposium on Theory of computing*, pages 457–464, 1984.

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

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

[6] J. F. Canny, E. Kaltofen, and L. Yagati. Solving systems of nonlinear polynomial equations faster. In *Proceedings of the ACM-SIGSAM 1989 international symposium on Symbolic and algebraic computation*, pages 121–128, 1989.

[7] R. Chen. Geometric fiber classification of morphisms and a geometric approach to cylindrical algebraic decomposition. *arXiv preprint arXiv:2311.10515*, 2023.

[8] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975)*, volume Vol. 33 of *Lecture Notes in Comput. Sci.*, pages 134–183. Springer, Berlin-New York, 1975.

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

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

[11] J. Faugère, P. Gaudry, L. Huot, and G. Renault. Sub-cubic change of ordering for gröbner basis: a probabilistic approach. In K. Nabeshima, K. Nagasaka, F. Winkler, and Á. Szántó, editors, *International Symposium on Symbolic and Algebraic Computation, ISSAC '14, Kobe, Japan, July 23-25, 2014*, pages 170–177. ACM, 2014.

[12] J.-C. Faugère. Fgb: a library for computing gröbner bases. In *International Congress on Mathematical Software*, pages 84–87. Springer, 2010.

[13] J.-C. Faugère, G. Moroz, F. Rouillier, and M. Safey El Din. 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*, pages 79–86, 2008.

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

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

[16] C. Hermite. Extrait d'une lettre de Mr. Ch. Hermite de Paris à Mr. Borchardt de Berlin sur le nombre des racines d'une équation algébrique comprises entre des limites données. *J. Reine Angew. Math.*, 52:39–51, 1856.

[17] M. Kalkbrener. On the stability of Gröbner bases under specializations. *J. Symbolic Comput.*, 24(1):51–58, 1997.

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

[19] H. P. Le, D. Manevich, and D. Plaumann. Computing totally real hyperplane sections and linear series on algebraic curves. *Le Matematiche*, 77(1):119–141, June 2022.

[20] H. P. Le and M. Safey El Din. Faster one block quantifier elimination for regular polynomial systems of equations. In *ISSAC '21—Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation*, pages 265–272. ACM, New York, [2021] ©2021.

[21] H. P. Le and M. Safey El Din. Solving parametric systems of polynomial equations over the reals through Hermite matrices. *J. Symbolic Comput.*, 112:25–61, 2022.

[22] S. Liang, D. J. Jeffrey, and M. M. Maza. The complete root classification of a parametric polynomial on an interval. In *Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, pages 189–196, 2008.

[23] G. Moroz. Complexity of the resolution of parametric systems of polynomial equations and inequations. In *Proceedings of the 2006 international symposium on Symbolic and algebraic computation*, pages 246–253, 2006.

[24] L. D. G. Puente, E. Gross, H. A. Harrington, M. Johnston, N. Meshkat, M. P. Millán, and A. Shiu. Absolute concentration robustness: Algebra and geometry, 2023.

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

[26] M. Safey El Din and E. Schost. Polar varieties and computation of one point in each connected component of a smooth algebraic set. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 224–231. ACM, New York, 2003.

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

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

[29] L. Yang and Z. Zeng. Equi-cevaline points on triangles. In *Computer Mathematics: Proceedings of the Fourth Asian Symposium (ASCM 2000)*, page 130. World Scientific Publishing Company Incorporated, 2000.