Faster One Block Quantifier Elimination for Regular Polynomial Systems of Equations

Huu Phuoc Le, Mohab Safey El Din

Faster one block quantifier elimination for regular polynomial systems of equations

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

May 5, 2021

Abstract

Quantifier elimination over the reals is a central problem in computational real algebraic geometry, polynomial system solving and symbolic computation. Given a semi-algebraic formula (whose atoms are polynomial constraints) with quantifiers on some variables, it consists in computing a logically equivalent formula involving only unquantified variables. When there is no alternation of quantifiers, one has a *one block* quantifier elimination problem.

This paper studies a variant of the one block quantifier elimination in which we compute an almost equivalent formula of the input. We design a new probabilistic efficient algorithm for solving this variant when the input is a system of polynomial equations satisfying some regularity assumptions. When the input is generic, involves s polynomials of degree bounded by D with n quantified variables and t unquantified ones, we prove that this algorithm outputs semi-algebraic formulas of degree bounded by $\mathcal{D}$ using $O^{\sim}\Big((n-s+1)\, 8^t\, \mathcal{D}^{3t+2}\, \binom{t+\mathcal{D}}{t}\Big)$ arithmetic operations in the ground field where $\mathcal{D} := 2(n+s)\, D^s(D-1)^{n-s+1}\, \binom{n}{s}$. In practice, it allows us to solve quantifier elimination problems which are out of reach of the state-of-the-art (up to 8 variables).

Keywords Quantifier elimination; Effective real algebraic geometry; Polynomial system solving

1 Introduction

Problem statement. Let $\boldsymbol{f} = (f_1, \dots, f_s) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ with $\boldsymbol{x} = (x_1, \dots, x_n)$ and $\boldsymbol{y} = (y_1, \dots, y_t)$. We aim at solving the following quantifier elimination problem over the reals

$$\exists (x_1, \dots, x_n) \in \mathbb{R}^n \quad f_1(\boldsymbol{x}, \boldsymbol{y}) = \dots = f_s(\boldsymbol{x}, \boldsymbol{y}) = 0.$$

This consists in computing a logically equivalent *quantifier-free* semi-algebraic formula $\Phi(\boldsymbol{y})$, i.e. Φ is a finite disjunction of conjonctions of polynomial constraints in $\mathbb{Q}[\boldsymbol{y}]$ which is true if and only if the input quantified formula is true. The $\boldsymbol{x}$ variables are called *quantified* variables and the $\boldsymbol{y}$ variables are called *parameters*.

Let π be the projection $(\boldsymbol{x}, \boldsymbol{y}) \mapsto \boldsymbol{y}$. Note that, geometrically, Φ describes the *projection* on the $\boldsymbol{y}$-space of the real algebraic set $\mathcal{V}_{\mathbb{R}} \subset \mathbb{R}^t \times \mathbb{R}^n$ defined by simultaneous vanishing of the f_i's. In this paper, we focus on solving a variant of the classical one block quantifier elimination, which computes a semi-algebraic formula which defines a dense subset of the interior of $\pi(\mathcal{V}_{\mathbb{R}})$.

Example 1. *Consider the toy example $x^2 + y^2 = 1$. Its projection on the y coordinate is described by the quantifier-free formula $(y \geq -1) \wedge (y \leq 1)$ while for our variant quantifier elimination problem, an admissible output is $(y > -1) \wedge (y < 1)$.*

Except for proving theorems, this is sufficient for most of applications of quantifier elimination in engineering sciences or computing sciences where either the output formula only needs to define a sufficiently large subset of the $\pi(\mathcal{V}_{\mathbb{R}})$ or is evaluated with parameters's values which are subject to numerical noise.

Prior works. The real quantifier elimination is a fundamental problem in mathematical logic and computational real algebraic geometry. It naturally arises in many problems in diverse application areas. The works of Tarski and Seidenberg [39, 32] imply that the projection of any semi-algebraic set is also semi-algebraic and give an algorithm, which is however not elementary recursive, to compute this projection. The Cylindrical Algebraic Decomposition (CAD) [8] is the first effective algorithm for this problem whose complexity is doubly exponential in the number of indeterminates [11]. Since then, there have been extensive researches on developing this domain. We can name the CAD variants with improved projections [24, 19, 25, 6] or the partial CAD [9]. Following the idea of [17] that exploits the block structure, [28, 3] introduced algorithms of only doubly exponential complexity in the order of quantifiers (number of blocks). For one-block quantifier elimination, the arithmetic complexity and the degree of polynomials in the output of these algorithms are of order $s^{n+1}D^{O(nt)}$ where D is the bound on the degree of input polynomials (see [4, Algo 14.6]). However, obtaining efficient implementations of these algorithms remains challenging. We also cite here some other works in real quantifier elimination [41, 38, 40, 7, 36] and applications to other fields [23, 1, 37].

In spite of this tremendous progress, many important applications stay out of reach of the state-of-the-art of the classic quantifier elimination. This motivates the researches on its variants. Generic quantifier elimination, in which the input and output formulas are equivalent for only almost every parameter, is studied in [12, 33]. A practically efficient algorithm is presented in [20, 21] for the same problem but under some assumptions on the input. The variant studied in this paper is a particular instance of the one in [20, 21].

Main results. In this paper, we consider the input $\boldsymbol{f} = (f_1, \ldots, f_s)$ satisfying the assumptions below.

Assumption A.

- *The ideal of $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ generated by $\boldsymbol{f}$ is radical.*
- *The algebraic set $\mathcal{V} \subset \mathbb{C}^{t+n}$ of $\boldsymbol{f}$ is equi-dimensional of dimension $d + t$. Its singular locus has dimension at most $t - 1$.*

Assumption B. *The Zariski closure $\overline{\pi(\mathcal{V})}$ of $\pi(\mathcal{V})$ is the whole parameter space $\mathbb{C}^t$ and $\pi(\mathcal{V}_{\mathbb{R}})$ is not of zero-measure in $\mathbb{R}^t$.*

The first result of the paper is a new probabilistic algorithm for solving the aforementioned variant of the quantifier elimination on such an input $\boldsymbol{f}$. Our algorithm applies the algorithm of [30] to the system $\boldsymbol{f}$ considering $\mathbb{Q}(\boldsymbol{y})$ as the based field. This allows to reduce our problem to zero-dimensional polynomial systems in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$. Next, we compute semi-algebraic formulas that describe approximate projections of these systems on the $\boldsymbol{y}$-space through the algorithm of [22]. This algorithm relies on a parametric variant of Hermite matrices for real root counting [27, 18]. A similar outline is also presented in [40, 13], in which the author computes an expensive comprehensive Gröbner bases [42] to analyze all cases before applying the real root counting algorithm of [27]. The relaxation of the output allows us to replace this exhaustive computation by the real root finding algorithm of [30].

Our second goal is to analyze the complexity of this new algorithm. For generic inputs, we bound the degree of the outputs and establish an arithmetic complexity which depends on this bound. The precise notion of genericity is as follows.

Let $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_{\le D} = \{p \in \mathbb{C}[\boldsymbol{x}, \boldsymbol{y}] \mid \deg(p) \le D\}$. A property P is said to be generic over $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_D^s$ if and only if there exists a non-empty Zariski open subset $\mathscr{P} \subset \mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_D^s$ such that the property P holds for every $\boldsymbol{f} \in \mathscr{P}$.

Our complexity result is then stated below. The notation $O\tilde{~}(g)$ means $O(g \log^\kappa(g))$ for some $\kappa > 0$.

Theorem 1. *Let $\mathcal{D} = 2(n+s)\, D^s (D-1)^{n-s+1} \binom{n}{s}$. There exists a non-empty Zariski open subset $\mathscr{F}$ of $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_{\le D}^s$ and a probabilistic algorithm such that, for every $\boldsymbol{f} \in \mathscr{F}$, this algorithm, in case of success, computes a semi-algebraic formula Φ defining a dense subset of the interior of $\pi(V(\boldsymbol{f}) \cap \mathbb{R}^{t+n})$ within*

$$O\tilde{~}\Big((n-s+1)\, 8^t\, \mathcal{D}^{3t+2} \tbinom{t+\mathcal{D}}{t}\Big)$$

arithmetic operations in $\mathbb{Q}$ and Φ involves only polynomials in $\mathbb{Q}[\boldsymbol{y}]$ of degree at most $\mathcal{D}$.

Even though our complexity result has the same order as the one given in [4, Algo 14.6], we obtain explicit degree bounds on the output formulas and make explicit the hidden constant in the O notation in the exponent.

On the practical aspect, our implementation in MAPLE of this algorithm outperforms real quantifier elimination functions in MAPLE and MATHEMATICA. It allows us to solve examples, both generic and non-generic, that are out of reach of these softwares (up to 8 indeterminates). These timings are reported in Section 6.

Structure of the paper. In Section 2, we start by recalling some basic notions. In Section 3, we resume the algorithm for real root finding of [30]. Also in the same section, we prove some auxiliary results in order to apply this algorithm parametrically. Next, we dedicate Section 4 for the description of our algorithm for solving the targeted problem and proving its correctness. The complexity of this algorithm is analyzed in Section 5. Finally, we report on some experimental results in Section 6.

2 Preliminaries

Algebraic sets and critical points. Let $\mathbb{F}$ be a subfield of $\mathbb{C}$ and $F \subset \mathbb{F}[x_1, \ldots, x_n]$. The algebraic subset of $\mathbb{C}^n$ at which the elements of F vanish is denoted by $V(F)$. 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 $\mathcal{V}$. The singular locus of $\mathcal{V}$ is denoted by $\mathrm{sing}(\mathcal{V})$. Given any subset $\mathcal{S}$ of $\mathbb{C}^n$, we denote by $\overline{\mathcal{S}}$ the Zariski closure of $\mathcal{S}$, i.e., the smallest algebraic set containing $\mathcal{S}$. An algebraic set $\mathcal{V}$ is equi-dimensional if its irreducible components share the same dimension.

A map φ between two algebraic sets $\mathcal{V} \subset \mathbb{C}^n$ and $\mathcal{W} \subset \mathbb{C}^i$ is a polynomial map if there exist $\varphi_1, \ldots, \varphi_i \in \mathbb{C}[x_1, \ldots, x_n]$ such that $\varphi(\eta) = (\varphi_1(\eta), \ldots, \varphi_i(\eta))$ for $\eta \in \mathcal{V}$. Let $\mathcal{V} \subset \mathbb{C}^n$ be an equi-dimensional algebraic set. We denote by $\mathrm{crit}(\varphi, \mathcal{V})$ the set of critical points of the restriction of φ to the non-singular locus of $\mathcal{V}$. If c is the codimension of $\mathcal{V}$ and $(f_1, \ldots, f_s)$ generates the ideal $I(\mathcal{V})$, the subset of $\mathcal{V}$ at which the Jacobian matrix associated to $(f_1, \ldots, f_s, \varphi_1, \ldots, \varphi_i)$ has rank less than or equal to c is the union of $\mathrm{crit}(\varphi, \mathcal{V})$ and $\mathrm{sing}(\mathcal{V})$ (see, e.g., [31, Subsection 3.1]). Further we denote by $\mathrm{jac}(f_1, \ldots, f_s, \varphi_1, \ldots, \varphi_i)$ this Jacobian matrix.

Gröbner bases and zero-dimensional ideals. Let $\mathbb{F}$ be a field and $\overline{\mathbb{F}}$ be its algebraic closure. We fix an admissible monomial order $\succ$ (see [10, Sec. 2.2]) over $\mathbb{F}[\boldsymbol{x}]$ where $\boldsymbol{x} = (x_1, \ldots, x_n)$. For $p \in \mathbb{F}[\boldsymbol{x}]$, the leading monomial of p with respect to $\succ$ is denoted by $\mathrm{lm}_\succ(p)$.

A Gröbner basis G of an ideal $I \subset \mathbb{F}[\boldsymbol{x}]$ w.r.t. the order $\succ$ is a finite 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 $p \in \mathbb{F}[\boldsymbol{x}]$, the remainder of the division of p by G using the order $\succ$ is uniquely defined and is called the *normal form* of p w.r.t. G. A polynomial p is reduced by G if p equals to its normal form w.r.t 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. When this holds, by [10, Sec. 5.3, Theorem 6], the quotient ring $\mathbb{F}[\boldsymbol{x}]/I$ is a $\mathbb{F}$-vector space of finite dimension. The dimension of this vector space is also called the algebraic degree of I; it coincides with the number of points of $V(I)$ counted with multiplicities [4, Sec. 4.5]. For any Gröbner basis of I, the set of monomials in $\boldsymbol{x}$ which are irreducible by G forms a monomial basis, denoted by 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 $\mathbb{F}$.

Properness & Noether normalization. A map $\varphi : V \mapsto \mathbb{C}^i$ is proper at $\beta \in \mathbb{C}^i$ if there exists a neighborhood $\mathcal{O}$ of β such that $\varphi^{-1}(\overline{\mathcal{O}})$ is compact, where $\overline{\mathcal{O}}$ denotes the closure of $\mathcal{O}$ in the Euclidean topology. If φ is proper everywhere on its image, we say that the map φ is proper. The properness is strongly related to the following notion of Noether normalization.

Let $\mathbb{F}$ be a field and I be an ideal of $\mathbb{F}[x_1, \ldots, x_n]$. The variables $(x_{i+1}, \ldots, x_n)$ are in Noether position w.r.t. I if their canonical images in the quotient algebra $\mathbb{F}[x_1, \ldots, x_n]/I$ are algebraic integers over $\mathbb{F}[x_1, \ldots, x_i]$ and $\mathbb{F}[x_1, \ldots, x_i] \cap I = \langle 0 \rangle$. Once $\mathbb{F} = \mathbb{C}$ and the variables $(x_{i+1}, \ldots, x_n)$ is in Noether position w.r.t. I, the projection of $V(I)$ on $(x_1, \ldots, x_i)$ is proper.

Change of variables. Given a field $\mathbb{F}$, we denote by $\mathrm{GL}(n, \mathbb{F})$ the set of invertible matrices of size $n \times n$ with entries in $\mathbb{F}$. Let $p \in \mathbb{F}[\boldsymbol{x}]$ be a polynomial. For any $A \in \mathrm{GL}(n, \mathbb{F})$, we denote by p^A the polynomial $p(A \cdot \boldsymbol{x}) \in \mathbb{F}[\boldsymbol{x}]$. For any algebraic set $V \subset \overline{\mathbb{F}}^n$, V^A denotes the algebraic set $\{A^{-1} \cdot \boldsymbol{x} \mid \boldsymbol{x} \in V\}$.

For two blocks of indeterminates $\boldsymbol{x}$ and $\boldsymbol{y}$, we consider frequently the matrices that act only on the variables $\boldsymbol{x}$ and leave $\boldsymbol{y}$ invariant. Those matrices form a subset denoted by $\mathrm{GL}(n, t, \mathbb{F})$ of $\mathrm{GL}(n + t, \mathbb{F})$.

3 Algorithm for real root finding

3.1 The S^2 algorithm

Now, we recall the algorithm in [30], which we refer to as the S^2 algorithm, for computing at least one point per connected component of a smooth real algebraic set.

Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ be a polynomial sequence in $\mathbb{R}[x_1, \ldots, x_n]$. For $1 \le i \le d$, let ϕ_i be the projection $(x_1, \ldots, x_n) \to (x_1, \ldots, x_i)$.

When $\boldsymbol{f}$ defines a smooth equi-dimensional algebraic set $\mathcal{V} \subset \mathbb{C}^n$ and generates a radical ideal, one can build a polynomial system using appropriate minors of $\mathrm{jac}(\boldsymbol{f})$ to define $\mathrm{crit}(\phi_i, \mathcal{V})$. Note that the critical loci are nested

$$\mathrm{crit}(\phi_1, \mathcal{V}) \subset \mathrm{crit}(\phi_2, \mathcal{V}) \subset \cdots \mathrm{crit}(\phi_d, \mathcal{V}) \subset \mathrm{crit}(\phi_{d+1}, \mathcal{V}) = \mathcal{V}.$$

Note also that in *generic* coordinates $\mathrm{crit}(\phi_i, \mathcal{V})$ has expected dimension $i - 1$. The algorithm in [30] then exploits stronger properties of these critical loci under some genericity assumption on the coordinate system (which are satisfied through a generic linear change of coordinates).

Proposition 2. *[30, Theorem 2] Assume that $\boldsymbol{f}$ defines a smooth equi-dimensional algebraic set and generates a radical ideal.*

Then, there exists a non-empty Zariski open set $\mathscr{A}_{\boldsymbol{f}} \in \mathrm{GL}(n, \mathbb{C})$ such that for $A \in \mathscr{A}_{\boldsymbol{f}}$ the following holds:

- *the restriction of ϕ_{i-1} to $\mathrm{crit}(\phi_i, \mathcal{V}^A)$ is proper;*
- *the set $\mathrm{crit}(\phi_i, \mathcal{V}^A)$ is either empty or of dimension $i - 1$ for $1 \le i \le d + 1$.*

The first item in Proposition 2 implies the second one. The index in the notation $\mathscr{A}_{\boldsymbol{f}}$ indicates that the non-empty Zariski open set depends on $\boldsymbol{f}$. Algorithm S^2 considers fibers of the above critical loci with the convention $\pi_0 : \boldsymbol{x} \to \bullet$. Proposition 2 is the cornerstone of the S^2 algorithm which can be derived from the following one.

Proposition 3. *[30, Theorem 2] Assume that $\boldsymbol{f}$ defines a smooth equi-dimensional algebraic set and generates a radical ideal.*

For $A \in \mathscr{A}_{\boldsymbol{f}} \cap \mathrm{GL}(n, \mathbb{Q})$ as defined in Proposition 2 and $\alpha = (\alpha_1, \dots, \alpha_d) \in \mathbb{R}^d$, the union of the sets

$$\mathrm{crit}(\phi_i, \mathcal{V}^A) \cap \phi_{i-1}^{-1}((\alpha_1, \dots, \alpha_{i-1})), \quad 1 \leq i \leq d+1$$

is finite and meets all connected components of $\mathcal{V} \cap \mathbb{R}^n$.

Example 4. *Let $\mathcal{V}$ be the smooth surface defined by $x_1^2 - x_2^2 - x_3^2 = 1$. The Jacobian matrix $\mathrm{jac}_{\boldsymbol{x}}(\boldsymbol{f})$ writes simply $(2x_1, -2x_2, -2x_3)$. It turns out that the identity matrix lies in the set $\mathscr{A}$ defined in Proposition 2. Taking $\alpha = (0, 0)$, we obtain 3 zero-dimensional systems:*

- $\mathrm{crit}(\phi_1, \mathcal{V})$*:* $\{-2x_2, -2x_3, x_1^2 - x_2^2 - x_3^2 - 1\}$,
- $\mathrm{crit}(\phi_2, \mathcal{V}) \cap \phi_1^{-1}(\mathbf{0})$*:* $\{-2x_3, x_1^2 - x_2^2 - x_3^2 - 1, x_1\}$,
- $\mathcal{V} \cap \phi_2^{-1}(\mathbf{0})$*:* $\{x_1^2 - x_2^2 - x_3^2 - 1, x_1, x_2\}$.

The first system admits two real solutions $(1, 0, 0)$ and $(-1, 0, 0)$. The other systems do not have any real solution. The two points $(1, 0, 0)$ and $(-1, 0, 0)$ intersect the two connected components of $\mathcal{V}$.

Of course, on general examples, one would need to perform a randomly chosen linear change of variables but this example illustrates already how S^2 works.

3.2 Parametric variant of S^2

We present now a parametric variant of S^2. We let $\boldsymbol{f} = (f_1, \dots, f_s) \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ where $\boldsymbol{y} = (y_1, \dots, y_t)$ are considered as parameters and $\boldsymbol{x} = (x_1, \dots, x_n)$ are variables. The algebraic set defined by $\boldsymbol{f}$ is denoted by $\mathcal{V} \subset \mathbb{C}^t \times \mathbb{C}^n$. Let π denote the projection $(\boldsymbol{x}, \boldsymbol{y}) \mapsto \boldsymbol{y}$ and π_i denote the projection $(\boldsymbol{y}, \boldsymbol{x}) \mapsto (\boldsymbol{y}, x_1, \dots, x_i)$.

Considering $\mathbb{Q}(\boldsymbol{y})$ as the ground field, the parametric variant of S^2 computes on the input $\boldsymbol{f}$ a list of finite subsets of $\mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$, each of which generates a zero-dimensional ideal of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$. These subsets are basically $\boldsymbol{f}^A \cup \Delta_i^A \cup \{x_1 - \alpha_1, \dots, x_{i-1} - \alpha_{i-1}\}$, where (A, α) is randomly chosen in $\mathrm{GL}(n, t, \mathbb{Q}) \times \mathbb{Q}^n$ and Δ_i^A is the set of all $(n-d)$-minors of the Jacobian matrix of $\boldsymbol{f}^A$ w.r.t. $x_i, \dots, x_n$.

The rest of this subsection is devoted to the auxiliary results that allow us to use the S^2 algorithm parametrically as above.

Lemma 5. *When Assumptions (A) and (B) hold, there exists a non-empty Zariski open subset $\mathscr{B}$ of $\mathbb{C}^t$ such that for every $\eta \in \mathscr{B}$, the specialization $\boldsymbol{f}(\eta, \cdot)$ of $\boldsymbol{f}$ at η generates a radical equi-dimensional ideal whose algebraic set is either empty or has dimension d.*

Proof. Under Assumption (B), by the fiber dimension theorem [34, Theorem 1.25], there exists a non-empty Zariski open subset $\mathscr{B}'$ of $\mathbb{C}^t$ such that $\pi^{-1}(\eta) \cap \mathcal{V}$ is an algebraic set of dimension d.

Let $\mathcal{W}$ denote the set of points of $\mathcal{V}$ at which the Jacobian matrix $\mathrm{jac}_{\boldsymbol{x}}(\boldsymbol{f})$ of $\boldsymbol{f}$ w.r.t. $\boldsymbol{x}$ has rank at most $n - d - 1$. We note that $\mathcal{W} = \mathrm{crit}(\pi, \mathcal{V}) \cup \mathrm{sing}(\mathcal{V})$.

The algebraic version of Sard's theorem [31, Proposition B2] implies that $\pi(\mathrm{crit}(\pi, \mathcal{V}))$ is contained in a proper Zariski closed subset of $\mathbb{C}^t$. On the other hand, as Assumptions (A) hold, the dimension of $\pi\,(\mathrm{sing}(\mathcal{V}))$ is less than t. Thus, it is also contained in a proper Zariski closed subset of $\mathbb{C}^t$.

Hence, the Zariski closure of $\pi(\mathcal{W})$ is a proper Zariski closed subset of $\mathbb{C}^t$. Let $\mathscr{B}$ be the intersection of the complement in $\mathbb{C}^t$ of this Zariski closure with $\mathscr{B}'$. For $\eta \in \mathscr{B}$, the set

$$\{\boldsymbol{x} \in \mathbb{C}^n \mid \boldsymbol{f}(\eta, \boldsymbol{x}) = 0, \mathrm{rank}\ \ \mathrm{jac}_{\boldsymbol{x}}(\boldsymbol{f})(\eta) < n - d\}$$

is empty. Since the dimension of $\pi^{-1}(\eta) \cap \mathcal{V}$ is d and the Jacobian matrix $\mathrm{jac}_{\boldsymbol{x}}(\boldsymbol{f})(\eta, \cdot)$ of $\boldsymbol{f}(\eta, \cdot)$ w.r.t. the variables $\boldsymbol{x}$ is of rank $n - d$ for every $(\eta, \boldsymbol{x}) \in \mathcal{V} \cap \pi^{-1}(\eta)$, the ideal $\boldsymbol{f}(\eta, \cdot)$ is radical and defines a smooth and equi-dimensional set of dimension d by Jacobian criterion [14, Theorem 16.19]. $\square$

Lemma 5 shows that when specializing $\boldsymbol{y} = (y_1, \ldots, y_t)$ to a generic point $\eta \in \mathscr{B} \cap \mathbb{R}^t$ in $\boldsymbol{f}$, one obtains a sequence of polynomials $\boldsymbol{f}(\eta, \cdot)$ which satisfies the assumptions of Proposition 2. One could then apply Algorithm S^2 to $\boldsymbol{f}(\eta, \cdot)$ to grab sample points per connected components in the real algebraic set it defines. However, proceeding this way would lead us to use a linear change of variables encoded by a matrix A which depends on η. The result below shows that one can choose one generic change of variables, once for all, that will be valid for most of parameters' values.

Proposition 6. *Assume that Assumptions (A) and (B) hold. There exists a non-empty Zariski open subset $\mathscr{O}$ of $\mathrm{GL}(n, t, \mathbb{C})$ such that for every $A \in \mathscr{O} \cap \mathrm{GL}(n, t, \mathbb{Q})$ the following holds.*

There exists a non-empty Zariski open subset $\mathscr{Y}_A$ of $\mathbb{C}^t$ such that $\mathscr{Y}_A$ is a subset of the non-empty Zariski open set $\mathscr{B}$ in Lemma 5 and A lies in the non-empty Zariski open set $\mathscr{A}_{\boldsymbol{f}(\eta,.)}$ defined in Proposition 2 for every $\eta \in \mathscr{Y}_A$.

Proof. Let $\overline{\mathbb{C}(\boldsymbol{y})}$ denote the algebraic closure of $\mathbb{C}(\boldsymbol{y})$. We consider $\overline{\mathbb{C}(\boldsymbol{y})}$ as the coefficient field. The proof of [30, Theorem 1] is purely algebraic and then is valid over the based field $\overline{\mathbb{C}(\boldsymbol{y})}$. Hence, there exists a non-empty Zariski open subset $\tilde{\mathscr{O}}$ of $\mathrm{GL}(n, t, \overline{\mathbb{C}(\boldsymbol{y})})$ such that for $A \in \tilde{\mathscr{O}} \cap \mathrm{GL}(n, t, \mathbb{Q})$, the variables $(x_1, \ldots, x_{i-1})$ is in Noether position w.r.t. the ideal in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ generated by $\boldsymbol{f}^A + \Delta_i^A$ for $1 \leq i \leq d + 1$ where Δ_i^A is the set of maximal minors of the truncated Jacobian matrix of $\mathrm{jac}(\boldsymbol{f}^A)$ with all the partial derivatives w.r.t. $\boldsymbol{y}$ and x_j for $1 \leq j \leq i$ being removed (hence these minors are the ones defining $\mathrm{crit}(\pi_i, \mathcal{V}) \cup \mathrm{sing}(\mathcal{V})$).

This is equivalent to the following. For $1 \leq i \leq d + 1$, $i \leq j \leq n$, there exist the polynomials $p_{i,j} \in \mathbb{Q}(\boldsymbol{y})[x_1, \ldots, x_{i-1}, x_j]$ such that each $p_{i,j}$ lies in the ideal of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ generated by $\boldsymbol{f}^A \cup \Delta_i^A$ and it is monic when considering x_j as the only variable (with the coefficients in $\mathbb{Q}(\boldsymbol{y})[x_1, \ldots, x_{i-1}]$).

The denominators of $p_{i,j}$ are then polynomials in $\mathbb{Q}[\boldsymbol{y}]$. We choose $\mathscr{Y}_A$ to be the intersection of the non-empty Zariski open set $\mathscr{B}$ defined in Lemma 5 and the non-empty Zariski open set defined by the non-vanishing of all the denominators appeared in the $p_{i,j}$'s. Thus, for $\eta \notin \mathscr{Y}_A$, $p_{i,j}(\eta, \cdot) \in \mathbb{Q}[x_1, \ldots, x_{i-1}, x_j]$ is monic in x_j. Consequently, $(x_i, \ldots, x_n)$ is in Noether position w.r.t. the ideal of $\mathbb{C}[\boldsymbol{x}]$ generated by $\boldsymbol{f}^A(\eta, \cdot) \cup \Delta_i^A(\eta, \cdot)$. Finally, taking $\mathscr{O} = \tilde{\mathscr{O}} \cap \mathrm{GL}(n, t, \mathbb{C})$, the conclusion follows. $\square$

4 One-block quantifier elimination algorithm

4.1 Description

In this subsection, we describe our algorithm for solving our variant of the quantifier elimination problem. The input is a polynomial sequence $\boldsymbol{f} = (f_1, \ldots, f_s) \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ satisfying Assumptions (A) and (B). Further, we denote by $Z(\Psi)$ the zero set of any semi-algebraic formula Ψ, i.e., $Z(\Psi) = \{\boldsymbol{y} \in \mathbb{R}^t \mid \Psi(\boldsymbol{y}) \text{ is true}\}$.

By Assumptions (A) and (B), the fiber dimension theorem [34, Theorem 1.25] implies that there exists a non-empty Zariski open subset of $\mathbb{C}^t$ such that $\pi^{-1}(\eta)$ has dimension d. The idea is to apply the parametric variant of S^2 with $\mathbb{Q}(\boldsymbol{y})$ as a ground field.

More precisely, we start by picking randomly (A, α) in $\mathrm{GL}(n, t, \mathbb{Q}) \times \mathbb{Q}^n$ and apply the change of variables $\boldsymbol{x} \mapsto A \cdot \boldsymbol{x}$ to the input $\boldsymbol{f}$ to obtain a new sequence $\boldsymbol{f}^A$. As A acts only on $\boldsymbol{x}$, $\pi(V(\boldsymbol{f}^A) \cap \mathbb{R}^{n+t}) =$

$\pi(\mathcal{V}_\mathbb{R})$. Hence, a quantifier-free formula that solves our problem for $\boldsymbol{f}^A$ is also a solution of the same problem for $\boldsymbol{f}$.

Let $\mathrm{jac}_{\boldsymbol{x}}(\boldsymbol{f}^A)$ be the Jacobian matrix of $\boldsymbol{f}^A$ w.r.t. the variables $\boldsymbol{x} = (x_1, \dots, x_n)$. We denote by $J_1, \dots, J_n$ the columns of $\mathrm{jac}_{\boldsymbol{x}}(\boldsymbol{f}^A)$ respectively. For $1 \le i \le d$, let $W_i^{A,\alpha}$ be the union of $\boldsymbol{f}^A$, all the $(n-d)$-minors of the matrix consisting of the columns $J_{i+1}, \dots, J_n$ and $\{x_1 - \alpha_1, \dots, x_{i-1} - \alpha_{i-1}\}$. In particular, $W_{d+1}^{A,\alpha}$ denotes $\boldsymbol{f}^A \cup \{x_1 - \alpha_1, \dots, x_d - \alpha_d\}$.

We prove later in Lemma 8 that, for generic (A, α), the ideals of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ generated by $W_i^{A,\alpha}$ are radical and zero-dimensional.

We now solve the quantifier elimination problem for each of the polynomial sets $W_i^{A,\alpha}$. For this step, we refer to a subroutine called RealRootClassification that takes as input a polynomial sequence $F \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ such that the ideal of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ generated by F is radical and zero-dimensional and computes a quantifier-free formula Φ_F in $\boldsymbol{y}$ such that $Z(\Phi_F)$ is dense in the interior of $\pi(V(F) \cap \mathbb{R}^{n+t})$. For this task, we refer to the algorithm of [22]. We will explain the essential details of this subroutine later in Subsection 4.2.

Calling the subroutine RealRootClassification on the inputs $W_i^{A,\alpha}$ gives us the lists of semi-algebraic formulas Φ_i. Finally, we return $\Phi = \vee_{i=1}^{d+1} \Phi_i$ as the output of our algorithm.

We summarize the whole discussion above in the following pseudo-code, where we call to two additional subroutines below:

- GenericDimension which takes the sequence $\boldsymbol{f}$ and computes the dimension of the ideal generated by $\boldsymbol{f}$ in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$.
- $(n-d)$ Minors which takes as input a matrix M whose coefficients are in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ and computes all of its $(n-d)$-minors.

Algorithm 1: One-block quantifier elimination

Input: $\boldsymbol{f} \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ satisfying Assumptions (A) and (B).
Output: A formula Φ s.t $Z(\Phi)$ is dense in the interior of $\pi(\mathcal{V}_\mathbb{R})$.

Choose randomly $(A, \alpha) \in \mathrm{GL}(n, \mathbb{Q}) \times \mathbb{Q}^n$
$\boldsymbol{f}^A \leftarrow \boldsymbol{f}(A \cdot \boldsymbol{x})$
$[J_1, \dots, J_n] \leftarrow \mathrm{jac}_{\boldsymbol{x}}(\boldsymbol{f}^A)$
$d \leftarrow$ GenericDimension$(\boldsymbol{f}^A)$
for $1 \le i \le d+1$ **do**
  $W_i^{A,\alpha} \leftarrow (n-d)$ Minors$([J_{i+1}, \dots, J_n]) \cup \{\boldsymbol{f}^A, x_1 - \alpha_1, \dots, x_{i-1} - \alpha_{i-1}\}$
  $\Phi_i \leftarrow$ RealRootClassification$(W_i^{A,\alpha})$
return $\Phi \leftarrow \vee_{i=1}^{d+1} \Phi_i$

4.2 Real root classification

Now we explain the general ideas of the algorithm presented in [22] that is used in the RealRootClassification subroutine.

Let $F \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ be a polynomial sequence such that the ideal $\langle F \rangle$ generated by F in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ is radical and zero-dimensional.

For such an input F, RealRootClassification computes a semi-algebraic formula Φ_F and a polynomial $w_\infty \in \mathbb{Q}[\boldsymbol{y}]$ that satisfies:

- $Z(\Phi_F) \subset \pi(V(F) \cap \mathbb{R}^{n+t})$,

- $Z(\Phi_F) \setminus V(w_\infty) = \pi(V(F) \cap \mathbb{R}^{n+t}) \setminus V(w_\infty)$.

The algorithm in [22] is based on constructing a symmetric matrix H_F with entries in $\mathbb{Q}(\boldsymbol{y})$ associated to F. This matrix is basically a parametric version of the classical Hermite matrix for the ideal $\langle F \rangle$ (see, e.g., [4, Chap. 4]), which provides the number of distinct real/complex solutions of the system $F(\eta, \cdot)$ through the signature/rank of the specialization of H_F at η [22, Corollary 17].

Let G_F be the reduced Gröbner basis of the ideal in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ generated by F w.r.t. the $\mathrm{grevlex}(\boldsymbol{x}) \succ \mathrm{grevlex}(\boldsymbol{y})$ order. We consider the leading coefficients of the elements of G_F in variables $\boldsymbol{x}$ w.r.t. the $\mathrm{grevlex}(\boldsymbol{x})$ order, which are polynomials in $\mathbb{Q}[\boldsymbol{y}]$. Then, w_∞ is taken as the square-free part of the product of these leading coefficients. The polynomial w_∞ defines an algebraic set of $\boldsymbol{y}$-space over which the matrix H_F does not have good specialization property (see [22, Proposition 16]).

Next, we choose randomly a matrix $Q \in \mathrm{GL}(\delta, \mathbb{Q})$. As the entries of H_F lie in $\mathbb{Q}(\boldsymbol{y})$, so do the leading principal minors $M_1, \ldots, M_\delta$ of $Q^T \cdot H_F \cdot Q$. Let $m_1, \ldots, m_\delta$ be the numerators of those minors, which are in $\mathbb{Q}[\boldsymbol{y}]$. A sufficiently generic matrix Q ensures that none of the m_i's is identically zero, hence allowing us to determine the signature of H_F according to the signs of the m_i's. We then compute a finite set of points L of $\mathbb{Q}^t$ that intersects every connected component of the semi-algebraic set defined by $\wedge_{i=1}^{\delta}(m_i \neq 0) \wedge (w_\infty \neq 0)$. Over those connected components, the polynomials m_i are sign-invariant. Since the signature of $H_F(\eta)$ can be deduced from the signs of the $m_i(\eta)$, the number of real solutions of $F(\eta, \cdot)$ is also invariant when η varies in each connected component.

Let $L_0 = \{\eta \in L \mid F(\eta, \cdot) \text{ admits at least one real solution}\}$ and

$$\Phi_F = (\vee_{\eta \in L_0}(\mathrm{sign}\ (M_1(\eta)) \wedge \ldots \wedge \mathrm{sign}\ (M_\delta(\eta)))) \wedge w_\infty \neq 0.$$

Then Φ_F is an admissible output of RealRootClassification for F. The correctness of this algorithm is proven in [22, Proposition 28].

In the pseudo-code below, we introduce the subroutines

- HermiteMatrix which takes as input a polynomial sequence $F \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ such that the ideal $\langle F \rangle \subset \mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ is zero-dimensional and computes the parametric Hermite matrix associated to F w.r.t. the $\mathrm{grevlex}(\boldsymbol{x})$ order.
  The description of this subroutine is given in [22, Algo. 2].
- PrincipalMinors computes the leading principal minors of the matrix $Q^T \cdot H_F \cdot Q$.
- SamplePoints which takes as input a polynomial sequence $m_1, \ldots, m_\delta, w_\infty \in \mathbb{Q}[\boldsymbol{y}]$ and computes a finite set of points that intersects every connected component of the semi-algebraic set defined by $\wedge_{i=1}^{\delta} m_i \neq 0 \wedge w_\infty \neq 0$.
  We describe such a subroutine in [22, Sec. 3].
- Signature which evaluates the signature of a symmetric matrix of entries in $\mathbb{Q}$.

We end this subsection by an example to illustrate our algorithm.

Example 7. *We consider the polynomial $f = x_1^2 + y_1 x_2^2 + y_2 x_2 + y_3$. Let $\Delta = y_2^2 - 4y_1 y_3$. The projection of $V(f) \cap \mathbb{R}^5$ on (y_1, y_2, y_3) is*

$$(\Delta \geq 0 \wedge\ y_1 > 0) \vee (y_1 < 0) \vee (y_1 = 0 \wedge ((y_2 \neq 0) \vee (y_2 = 0 \wedge y_3 \leq 0)))\,.$$

Applying the parametric variant of S^2 for $A = I_3$ and $\alpha = (0, 0)$, we obtain 2 systems $W_1 = \{2y_1 x_2 + y_2, f\}$ and $W_2 = \{f, x_1\}$. Next, we call RealRootClassification *on these systems, choosing $Q = I_2$ to simplify the calculation. We obtain then $w_{1,\infty} = w_{2,\infty} = y_1$ and the Hermite matrices:*

$$H_1 = \begin{pmatrix} 2 & 0 \\ 0 & -2y_3 + y_2^2/(2y_1) \end{pmatrix}, \quad H_2 = \begin{pmatrix} 2 & -y_2/y_1 \\ -y_2/y_1 & (-2y_1 y_3 + y_2^2)/y_1^2 \end{pmatrix}.$$

Algorithm 2: RealRootClassification

Input: A polynomial sequence $F \subset \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$ such that the ideal of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ generated by F is radical and zero-dimensional.

Output: A formula $\Phi_F \wedge (w_\infty \neq 0)$.

```
H_F, w_∞ ← HermiteMatrix(F)
Choose randomly Q ∈ GL(δ, ℚ) // δ is the size of H_F
(M_1, ..., M_δ) ← PrincipalMinors(Q^T · H_F · Q)
(m_1, ..., m_δ) ← Numerators(M_1, ..., M_δ)
L ← SamplePoints((∧_{i=1}^δ m_i ≠ 0) ∧ w_∞ ≠ 0)
for η ∈ L do
    if Signature(H_F(η)) ≠ 0 then
        σ ← (sign M_1(η), ..., sign M_δ(η))
        Φ_F ← Φ_F ∨ ((sign M_1, ..., sign M_δ) = σ)
return Φ_F ∧ (w_∞ ≠ 0)
```

The sequences of leading principal minors are respectively $[2, \Delta/y_1]$ *and* $[2, \Delta/y_1^2]$*. We compute then* 4 *points representing* 4 *connected components of the semi-algebraic set defined by* $y_1 \neq 0 \wedge \ \Delta \neq 0$*:*

$$(1, 1/8, 0), (-1, 1/8, 0), (1, 1/8, 1/128), (-1, 1/8, -1/128).$$

The matrix H_2 *has non-zero signature over the first and second points, which both lead to the sign condition* $\Delta > 0 \wedge y_1^2 > 0$*. Thus, we have*

$$\Phi_2 = (\Delta > 0 \wedge y_1^2 > 0) \wedge (y_1 \neq 0).$$

For H_1*, non-zero signatures are satisfied at the first and fourth points. Evaluating the sign of* Δ *and* y_1 *at those points gives*

$$\Phi_1 = ((\Delta > 0 \wedge \ y_1 > 0) \vee (\Delta < 0 \wedge \ y_1 < 0)) \wedge (y_1 \neq 0).$$

The final output is therefore $\Phi = \Phi_1 \vee \Phi_2$*, which is equivalent to*

$$\begin{aligned}\Phi &= (\Delta > 0 \wedge y_1 > 0) \vee (\Delta < 0 \wedge y_1 < 0) \vee (\Delta > 0 \wedge y_1 \neq 0)\\ &= (\Delta > 0 \wedge y_1 > 0) \vee (\Delta \neq 0 \wedge y_1 < 0).\end{aligned}$$

It is straight-forward to see that $Z(\Phi)$ *is a dense subset of* $\pi\left(V(f) \cap \mathbb{R}^5\right)$*.*

4.3 Correctness of Algorithm 1

We start by proving that the polynomial sequences $W_i^{A,\alpha}$ satisfy the assumptions required by RealRootClassification.

Lemma 8. *Assume that Assumptions (A) and (B) hold. Let* $\mathscr{O}$ *be the Zariski open subset of* $\mathrm{GL}(n, t, \mathbb{C})$ *defined in Proposition 6 and* $A \in \mathscr{O} \cap \mathrm{GL}(n, t, \mathbb{Q})$*. There exists a non-empty Zariski open subset* $\mathscr{X}$ *of* $\mathbb{C}^d$ *such that for* $\alpha \in \mathscr{X} \cap \mathbb{Q}^d$*, the ideal of* $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ *generated by* $W_i^{A,\alpha}$ *is radical and either empty or zero-dimensional.*

Proof. By Proposition 6, the algebraic set defined by $W_i^{A,\alpha}(\eta, \cdot)$ is finite when η varies over a non-empty Zariski open subset $\mathscr{Y}_A$ of $\mathbb{C}^t$. Thus, the ideal of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ generated by $W_i^{A,\alpha}$ is zero-dimensional. Now we prove that the ideal generated by $W_i^{A,\alpha}$ is radical.

Let $M_1^A, \dots, M_\ell^A$ be the $(n-d)$ minors of the Jacobian matrix J associated to $\boldsymbol{f}^A$ when considering only the partial derivatives w.r.t. $x_{i+1}, \dots, x_n$. Recall that $W_i^{A,\alpha}$ is the union of $\boldsymbol{f}^A$ with the $M_1^A, \dots, M_\ell^A$ with $x_1 - \alpha_1, \dots, x_{i-1} - \alpha_{i-1}$. Further, we denote by ${W'}_i^A \subset \mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ the ideal generated by $\boldsymbol{f}^A, M_1^A, \dots, M_\ell^A$.

The idea is to follow [31, Definitions 3.2 and 3.3] where *charts* and *atlases* are defined for algebraic sets defined by the vanishing of $\boldsymbol{f}^A$ and $M_1^A, \dots, M_\ell^A$.

Let m be a $(n-d-1)$ minor of J. Without loss of generality we assume that it is the upper left such minor and let $M_1^A, \dots, M_{d-(i-1)}^A$ be the $(n-d)$ minors of J obtained by completing m with the $n-d$-th line of J and the missing column. We denote by $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]_m$ the localized ring where divisions by powers of m are allowed.

By [31, Lemma B.12] there exists a non-empty Zariski open set $\mathscr{O}'_{m,n-d}$ such that for $A \in \mathrm{GL}(n,t,\mathbb{C})$, the localization of the ideal generated by $f_1^A, \dots, f_{n-d}^A, M_1^A, \dots, M_{d-(i-1)}^A$ in the ring $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]_m$ is radical and coincides with the localization of ${W'}_i^A$ in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]_m$. By [31, Prop. 3.4], there exists a non-empty Zariski open set $\mathscr{O}'' \subset \mathrm{GL}(n,t,\mathbb{C})$ such that for $A \in \mathscr{O}''$, any irreducible component of the algebraic set defined by ${W'}_i^A$ contains a point at which a $(n-d-1)$ minor of J does not vanish. This implies that any primary component ${W'}_i^A$ whose associated algebraic set contains such a point is radical and then prime.

Now define Ω as the intersection of $\mathscr{O}$ (defined in Proposition 6), all non-empty Zariski open sets $\mathscr{O}'_{m,k}$ and $\mathscr{O}''$. Hence, we then deduce that ${W'}_i^A$ generates a radical ideal.

It remains to prove that there exists a non-empty Zariski open set $\mathscr{X}_i \subset \mathbb{C}^{i-1}$ such that for $\alpha = (\alpha_1, \dots, \alpha_{i-1}) \in \mathscr{X}_i$, $\langle {W'}_i^A \rangle + \langle x_1 - \alpha_1, \dots, x_{i-1} - \alpha_{i-1} \rangle$ is radical in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$. Note that choosing α outside the set of critical values of π_i restricted to the algebraic set defined by ${W'}_i^A$ in $\overline{\mathbb{Q}(\boldsymbol{y})}^n$ is enough. By Sard's theorem, this set of critical values is contained in the vanishing set of a non-zero polynomial $\nu \in \mathbb{Q}[\boldsymbol{y}][\boldsymbol{x}]$. Now note that it suffices to define $\mathscr{X}_i$ as the complement of the vanishing set of the coefficients of ν when it is seen in $\mathbb{Q}[\boldsymbol{x}][\boldsymbol{y}]$ and $\mathscr{X} = \cap_{i=1}^{d+1} \mathscr{X}_i$. $\square$

We prove the correctness of Algorithm 1 in Proposition 9 below.

Proposition 9. *Assume that Assumptions* (A) *and* (B) *hold. Let $\mathscr{O} \subset \mathrm{GL}(n,t,\mathbb{C})$ and $\mathscr{X} \subset \mathbb{C}^d$ be defined respectively in Proposition 6 and Lemma 8. Then for $A \in \mathscr{O} \cap \mathrm{GL}(n,t,\mathbb{Q})$ and $\alpha \in \mathscr{X} \cap \mathbb{Q}^d$, the formula Φ computed by Algorithm 1 defines a dense subset of the interior of $\pi(\mathcal{V}_\mathbb{R})$.*

Proof. By Lemma 8, $W_i^{A,\alpha}$ satisfies the assumptions of RealRootClassification. Thus, the calls of RealRootClassification on $W_i^{A,\alpha}$ are valid and return the formulas Φ_i and the polynomials $w_{i,\infty}$. As A acts only on $\boldsymbol{x}$, $\pi(\mathcal{V}_\mathbb{R}^A) = \pi(\mathcal{V}_\mathbb{R})$. Thus,

$$Z(\Phi_i) \subset \pi(V(W_i^{A,\alpha}) \cap \mathbb{R}^{n+t}) \subset \pi(\mathcal{V}_\mathbb{R}^A) = \pi(\mathcal{V}_\mathbb{R}).$$

Therefore, $Z(\Phi) = \cup_{i=1}^{d+1} Z(\Phi_i) \subset \pi(\mathcal{V}_\mathbb{R})$.

By the description of Φ_i, for $1 \leq i \leq d+1$,

$$Z(\Phi_i) \setminus V(w_{i,\infty}) = \pi(V(W_i^{A,\alpha}) \cap \mathbb{R}^{n+t}) \setminus V(w_{i,\infty}).$$

Let $\mathscr{Y}_A$ be the non-empty Zariski open subset of $\mathbb{C}^t$ in Proposition 6 ($\mathscr{Y}_A$ depends on the matrix A). We denote

$$\mathcal{W} = \cup_{i=1}^{d+1} V(w_{i,\infty}) \cup (\mathbb{C}^t \setminus \mathscr{Y}_A).$$

We will show that, for $\eta \in \pi(\mathcal{V}_\mathbb{R}^A) \setminus \mathcal{W}$, $\eta \in Z(\Phi)$.

Since $\eta \in \pi(\mathcal{V}_{\mathbb{R}}^A)$, $V(\boldsymbol{f}^A(\eta,\cdot)) \cap \mathbb{R}^n$ is not empty. On the other hand, as $\eta \in \mathcal{Y}_A$, $\boldsymbol{f}^A(\eta,\cdot)$ generates a radical equi-dimensional ideal whose algebraic set is either empty or smooth of dimension d. By Proposition 3, $V(\boldsymbol{f}^A(\eta,\cdot)) \cap \mathbb{R}^n$ is not empty if and only if $\cup_{i=1}^{d+1} V(W_i^{A,\alpha}(\eta) \cap \mathbb{R}^n)$ is not empty either. We deduce that $\eta \in \cup_{i=1}^{d+1} \pi(V(W_i^{A,\alpha}) \cap \mathbb{R}^{n+t}) \setminus \mathcal{W}$. We have that

$$\begin{aligned}&\cup_{i=1}^{d+1} \pi(V(W_i^{A,\alpha}) \cap \mathbb{R}^{n+t}) \setminus \mathcal{W} = \cup_{i=1}^{d+1} (\pi(V(W_i^{A,\alpha}) \cap \mathbb{R}^{n+t}) \setminus \mathcal{W})\\ &= \cup_{i=1}^{d+1} (Z(\Phi_i) \setminus \mathcal{W}) = (\cup_{i=1}^{d+1} Z(\Phi_i)) \setminus \mathcal{W}.\end{aligned}$$

Therefore, $Z(\Phi) \setminus \mathcal{W} = \pi(\mathcal{V}_{\mathbb{R}}) \setminus \mathcal{W}$ and $\pi(\mathcal{V}_{\mathbb{R}}) \setminus Z(\Phi)$ is of measure zero in $\mathbb{R}^t$. By Assumption (B), we conclude that $Z(\Phi)$ is a dense subset of the interior of $\pi(\mathcal{V}_{\mathbb{R}})$. ☐

5 Complexity analysis

We now estimate the arithmetic complexity of Algorithm 1 once $A \in \mathscr{O} \cap \mathrm{GL}(n, t, \mathbb{Q})$ and $\alpha \in \mathscr{X} \cap \mathbb{Q}^n$ as in Proposition 6 are found from a random choice. In this section, the input $\boldsymbol{f}$ forms a regular sequence of $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ (then, $s = n - d$) satisfying Assumptions (A) and (B). As the calls to RealRootClassification on the systems $W_i^{A,\alpha}$ are the most costly parts of our algorithm, we focus on estimating their complexities. To this end, we introduce the following assumption.

Assumption C. *Let $F \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ and G be the reduced Gröbner basis of F w.r.t. the $\mathrm{grevlex}(\boldsymbol{x}) \succ \mathrm{grevlex}(\boldsymbol{y})$ order. Then F is said to satisfy Assumption (C) if and only if for any $g \in G$, the total degree of g in both $\boldsymbol{x}$ and $\boldsymbol{y}$ equals the degree of g w.r.t. only $\boldsymbol{x}$.*

In [22, Lemma 13], it is proven that, on an input F satisfying Assumption (C), the polynomial w_∞ in RealRootClassification is simply 1 and the entries of the Hermite matrix H_F are in $\mathbb{Q}[\boldsymbol{y}]$. Therefore, the SamplePoints subroutine is called on the sequence of leading principal minors of the parametric Hermite matrices. Again, with Assumption (C), the degree of these leading principal minors can be bounded (see [22, Lemma 32]). Therefore, one obtains the complexity bound for RealRootClassification for such F.

Back to our problem, we will establish a degree bound for the polynomials given into SamplePoints. Some notations that will be used further are introduced below.

Let D be a bound of the total degree of elements of $\boldsymbol{f}$. The zero-dimensional ideal of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$ generated by $W_i^{A,\alpha}$ is denoted by $\langle W_i^{A,\alpha} \rangle$. The quotient ring $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle W_i^{A,\alpha} \rangle$ is a finite dimensional $\mathbb{Q}(\boldsymbol{y})$-vector space. Let G_i be the reduced Gröbner basis of the ideal of $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ generated by $W_i^{A,\alpha}$ w.r.t. $\mathrm{grevlex}(\boldsymbol{x}) \succ \mathrm{grevlex}(\boldsymbol{y})$ and B_i be the monomial basis of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle W_i^{A,\alpha} \rangle$ constructed using G_i as described in Section 2.

We begin with the following lemma.

Lemma 10. *When Assumption (C) holds for $W_i^{A,\alpha}$, any leading principal minor of the matrix H_i has degree bounded by $2\sum_{b \in B_i} \deg(b)$.*

Proof. The proof can be deduced from [22, Lemma 13, Proposition 31, Lemma 32]. It is mainly based on the control of degrees appearing in the normal form computation in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle W_i^{A,\alpha} \rangle$. ☐

It remains to estimate the sum $\sum_{b \in B_i} \deg(b)$. A bound is obtained by simply taking the product of the highest degree appeared in B_i and its cardinality. As the Hilbert series of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle W_i^{A,\alpha} \rangle$ when $\boldsymbol{f}$ is a generic system are known (see, e.g., [16, 35]), explicit bounds of these quantities are easily obtained.

Lemma 11. *Let B_i be defined as above. There exists a non-empty Zariski open subset $\mathscr{Q}$ of $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]_{\le D}^s$ such that, for $\boldsymbol{f} \in \mathscr{Q}$, the following inequality holds for $1 \le i \le d+1$:*

$$\textstyle\sum_{b \in B_i} \deg_{\boldsymbol{x}}(b) \le (n + s - i)\, D^s (D-1)^{n-i-s+2} \binom{n-i+1}{s}.$$

Proof. By [26, Theorem 2.2], there exists a non-empty Zariski open subset $\mathscr{Q}_{1,1} \subset \mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]^s_{\le D}$ such that when $\boldsymbol{f} \in \mathscr{Q}_{1,1}$, the algebraic degree of $\langle W_1^{A,\alpha} \rangle$, which is also the cardinality of B_1, is bounded by

$$D^s \sum_{k=0}^{n-s} \binom{k+s-1}{s-1} (D-1)^k \le D^s (D-1)^{n-s} \binom{n}{s}.$$

On the other hand, by [35, Corollary 3.2], there exists a non-empty Zariski subset $\mathscr{Q}_{1,2} \subset \mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]^s_{\le D}$ such that for $\boldsymbol{f} \in \mathscr{Q}_{1,2}$, the witness degree, i.e., the highest degree appeared in the reduced Gröbner basis of $W_1^{A,\alpha}$ w.r.t. $\mathrm{grevlex}(\boldsymbol{x})$, is bounded by $(n+s-1)D - 2n + 2$. Thus, the highest degree in B_1 is bounded by $(n+s-1)D - 2n + 1$. Thus, let $\mathscr{Q}_1 = \mathscr{Q}_{1,1} \cap \mathscr{Q}_{1,2}$ and, for $\boldsymbol{f} \in \mathscr{Q}_1$, we obtain

$$\sum_{b \in B_1} \deg(b) \le (n+s-1)\, D^s (D-1)^{n-s+1} \binom{n}{s}.$$

We note that, for $1 \le i \le d$, the system $W_i^{A,\alpha}$ can also be interpreted as the system defining the critical locus of the projection $(x_i, \dots, x_n) \mapsto x_i$ restricted to $V\left(\boldsymbol{f}^A(\alpha_1, \dots, \alpha_{i-1}, x_i, \dots, x_n)\right)$. Therefore, by replacing n by $n - i + 1$ in the above bound, we deduce that, for $1 \le i \le d$, there exists a non-empty Zariski open subset $\mathscr{Q}_i \subset \mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]^s_{\le D}$ such that

$$\sum_{b \in B_i} \deg(b) \le (n+s-i)\, D^s (D-1)^{n-i-s+2} \binom{n-i+1}{s}.$$

For the particular case $i = d+1$, the cardinality of B_{d+1} is bounded by D^s and the highest degree in B_{d+1} is bounded by $s(D-1)$. Therefore, the bound also holds for $i = d+1$.

By taking $\mathscr{Q} = \cap_{i=1}^{d+1} \mathscr{Q}_i$, we conclude the proof. □

Further, we denote $\mathcal{D} = 2(n+s-1)D^s(D-1)^{n-s+1}\binom{n}{s}$. We prove now that Assumption (C) holds generically then finish the proof of Theorem 1 stated in Section 1.

Proposition 12. *There exists a non-empty Zariski open subset $\mathscr{P} \subset \mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]^s_{\le D}$ such that, for every $\boldsymbol{f} \in \mathscr{P}$, there exists a non-empty Zariski open subset $\mathscr{K}_{\boldsymbol{f}} \subset \mathrm{GL}(n, t, \mathbb{C}) \times \mathbb{C}^n$ such that for $(A, \alpha) \in \mathscr{K}_{\boldsymbol{f}}$, Assumption (C) holds for every system $W_i^{A,\alpha}$.*

Proof. Let y_{t+1} be a new variable and ${}^h\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]_D$ denote the set of homogeneous polynomials in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]$ of degree D. For any polynomial $F \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$, we denote by ${}^hF \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]$ the homogenization of F w.r.t. all the variables $(\boldsymbol{x}, \boldsymbol{y})$, that means ${}^hF = y_{t+1}^{\deg(p)} \cdot F\left(\frac{x_1}{y_{t+1}}, \dots, \frac{x_n}{y_{t+1}}, \frac{y_1}{y_{t+1}}, \dots, \frac{y_t}{y_{t+1}}\right)$ for each $p \in F$. Further, $\langle {}^hF \rangle_h$ denotes the ideal of $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]$ generated by ${}^hF$.

We consider the following property (C1): The leading terms appearing in the reduced Gröbner basis of $\langle {}^hF \rangle_h$ w.r.t. $\mathrm{grevlex}(\boldsymbol{x} \succ \boldsymbol{y} \succ y_{t+1})$ do not involve any of the variables $y_1, \dots, y_{t+1}$. In the proof of [22, Prop. 30], it is proven that the property (C1) implies Assumption (C).

Following the proof of [2, Prop. 7], if y_{j+1} is not a zero-divisor of the quotient ring $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]/\langle {}^hF, y_1, \dots, y_j \rangle_h$ for every $0 \le j \le t$, then F satisfies the property (C1). This property means that $(y_1, \dots, y_{t+1})$ forms a regular sequence in the quotient ring $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]/\langle {}^hF \rangle_h$. We name this property as (C2).

From the proof of [35, Lemma 2.1, Lemma 2.2] and [14, Proposition 18.13], there exists a dense Zariski open subset $\mathscr{P}_1 \subset \mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]^s_{\le D}$ such that for $\boldsymbol{f} \in \mathscr{P}_1$, there exists a dense Zariski open subset $\mathscr{K}_{\boldsymbol{f},1} \subset \mathrm{GL}(n, t, \mathbb{C}) \times \mathbb{C}^n$ such that for $(A, \alpha) \in \mathscr{K}_{\boldsymbol{f},1}$, the quotient ring $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]/\langle {}^hW_1^{A,\alpha} \rangle_h$ is a Cohen-Macaulay ring of dimension $t+1$ and the ideal $\langle {}^hW_1^{A,\alpha}, y_1, \dots, y_{t+1} \rangle_h$ has dimension 0. By the unmixedness theorem [14, Corollary 18.14], $(y_1, \dots, y_{t+1})$ is a regular sequence over $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}, y_{t+1}]/\langle {}^hW_1^{A,\alpha} \rangle_h$. Thus, $W_1^{A,\alpha}$ satisfies the property (C2) and Assumption (C) holds.

Similar for $2 \leq i \leq d+1$, we obtain dense Zariski subsets $\mathscr{P}_i \subset \mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]^s_{\leq D}$ and $\mathscr{K}_{\boldsymbol{f},i} \subset \mathrm{GL}(n,t,\mathbb{C}) \times \mathbb{C}^n$ for each $\boldsymbol{f} \in \mathscr{P}_i$. Taking $\mathscr{P} = \cap_{i=1}^{d+1} \mathscr{P}_i$, and for $\boldsymbol{f} \in \mathscr{P}$, $\mathscr{K} = \cap_{i=1}^{d+1} \mathscr{K}_{\boldsymbol{f},i}$, we conclude the proof. □

Proof of Theorem 1. It is well-known that Assumptions (A) and (B) are generic. Also, the set of regular sequences is also dense in $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]^s_{\leq D}$. Thus, there exists a non-empty Zariski open subset $\mathscr{R} \subset \mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]^s_{\leq D}$ such that for any $\boldsymbol{f} \in \mathscr{R}$, $\boldsymbol{f}$ forms a regular sequence satisfying Assumptions (A) and (B). Recall that $d+t$ is the dimension of $V(\boldsymbol{f})$. As $\boldsymbol{f}$ forms a regular sequence in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$, $d = n - s$.

Algorithm 1 consists of $(d+1)$ calls to RealRootClassification with inputs $W_i^{A,\alpha}$ respectively. Let $\mathscr{P}$ be the non-empty Zariski open set in Proposition 12 and $\mathscr{Q} = \mathscr{P} \cap \mathscr{R}$. Then, for $\boldsymbol{f} \in \mathscr{Q}$, SamplePoints is called on the list of leading principal minors, which lie in $\mathbb{Q}[\boldsymbol{y}]$ of degree bounded by $\mathcal{D}$. The number of principal minors is equal to the dimension of the quotient ring $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle W_i^{A,\alpha} \rangle$, which is also bounded by $\mathcal{D}$.

Thus, by applying [22, Theorem 2], each call to RealRootClassification on the systems $W_i^{A,\alpha}$ costs at most $O\tilde{~}\left(8^t\, \mathcal{D}^{3t+2} \binom{t+\mathcal{D}}{t}\right)$ arithmetic operations in $\mathbb{Q}$. In total, the arithmetic complexity of Algorithm 1 is bounded by $O\tilde{~}\left((n-s+1)\, 8^t\, \mathcal{D}^{3t+2} \binom{t+\mathcal{D}}{t}\right)$. □

6 Experiments

We compare the practical behavior of Algorithm 1 with QuantifierElimination (MAPLE's RegularChains) and Resolve (MATHEMATICA) on an Intel(R) Xeon(R) Gold 6244 3.60GHz machine of 754GB RAM. The timings are given in seconds (s.), minutes (m.) and hours (h.). The symbol ∞ means that the computation is stopped after 72 hours without getting the result. We use our MAPLE implementation for Hermite matrices, in which FGB package [15] is used for Gröbner bases computation. The computation of sample points of semi-algebraic sets is done using RAGLIB library [29] which employs `msolve` library [5] for zero-dimensional system solving.

For RealRootClassification, we use the following notations:

- HM: timings of computing Hermite matrices and their minors.
- SP: total timings of computing the sample points.
- SIZE: the largest size of the Hermite matrices.
- DEG: the highest degree appeared in the output formulas.

We start with random dense systems. Fixing the total degree $D = 2$, we run our algorithm for various t, n and s. In Table 1, SamplePoints accounts for the major part of the timings of RealRootClassification. While our algorithm can tackle these examples, neither MAPLE nor MATHEMATICA finish after 72 (h.). The theoretical degree bound agrees with the practical observations. This agrees with our complexity result. On smaller problems, we observed that formulas output by MAPLE and MATHEMATICA have way larger degrees than the ones we output. Hence, these implementations, based on Cylindrical Algebraic Decomposition, suffer from its doubly exponential complexity while our implementation takes advantage of the singly exponential complexity of our algorithm.

Table 2 shows the timings for sparse systems. Each polynomial is generated with $D = 2$ and has $2n$ terms. Even Assumption (C) is not satisfied, our algorithm still applies. Thanks to the sparsity, the size and degree of the matrices in our algorithm are smaller than in the dense cases. Thus, the computation of our algorithm here is faster than in Table 1 while these examples are out of reach of MAPLE and MATHEMATICA.

Finally, Table 3 give the timings for structured systems. We separate the variables $\boldsymbol{x}$ into blocks of total degree 1; $[i, n-i]$ means that the degree in $[x_1, \ldots, x_i]$ and $[x_{i+1}, \ldots, x_n]$ are respectively 1.

t	n	s	HM	SP	SIZE	DEG	MAPLE	MATHEMATICA
2	3	2	.2 s.	3 s.	8	24	∞	∞
2	4	2	9 s.	1 m.	12	40	∞	∞
2	5	2	2 m.	15 m.	16	56	∞	∞
2	6	2	20 m.	2.5 h.	20	72	∞	∞
2	7	2	1.5 h.	6 h.	24	88	∞	∞
3	3	2	6 s.	1 m.	8	24	∞	∞
3	4	2	5 m.	15 m.	12	40	∞	∞
3	5	2	2 h.	5 h.	16	56	∞	∞
3	6	2	8 h.	16 h.	20	72	∞	∞
4	3	2	40 s.	30 m.	8	24	∞	∞
4	4	2	6 h.	40 h.	12	40	∞	∞
5	3	2	5 m.	14 h.	8	24	∞	∞

Table 1: Generic systems with $D = 2$

t	n	s	HM	SP	SIZE	DEG	MAPLE	MATHEMATICA
3	3	2	3 s.	37 s.	7	22	∞	∞
3	4	2	2 m.	10 m.	9	34	∞	∞
3	5	2	2 m.	10 m.	9	32	∞	∞
4	3	2	20 s.	20 m.	7	22	∞	∞
4	4	2	15 s.	18 m.	5	20	∞	∞

Table 2: Sparse systems with $D = 2$

Here, entries of the Hermite matrices have non-trivial denominators with high degree. Computation those matrices takes the major part. However, our algorithm still outperforms the two other software.

t	n	s	Block	HM	SP	SIZE	DEG	MAPLE	MATHEMATICA
3	3	2	$[1, 2]$	5 s.	45 s.	4	20	∞	∞
3	4	2	$[2, 2]$	4 m.	1 m.	8	32	∞	∞
3	5	2	$[2, 3]$	2 h.	9 m.	8	40	∞	∞
3	6	2	$[3, 3]$	30 h.	45 m.	14	60	∞	∞

Table 3: Structured systems

References

[1] Hirokazu Anai and Volker Weispfenning. Reach set computations using real quantifier elimination. In *Hybrid Systems: Computation and Control*, pages 63–76. Springer Berlin Heidelberg, 2001.

[2] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of the F5 Gröbner basis algorithm. *J. Symb. Comput.*, 70:49–70, 2015.

[3] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43(6):1002–1045, November 1996.

[4] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry*. Springer-Verlag, Berlin, Heidelberg, 2006.

[5] Jérémy Berthomieu, Christian Eder, and Mohab Safey El Din. msolve: A Library for Solving Polynomial Systems. Preprint, February 2021.

[6] Christopher W. Brown. Improved projection for Cylindrical Algebraic Decomposition. *J. Symb. Comput.*, 32(5):447 – 465, 2001.

[7] Christopher W. Brown and Christian Gross. Efficient preprocessing methods for quantifier elimination. In *Computer Algebra in Scientific Computing*, pages 89–100, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

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

[9] George E. Collins and Hoon Hong. Partial Cylindrical Algebraic Decomposition for quantifier elimination. *J. Symb. Comput.*, 12(3):299 – 328, 1991.

[10] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, (Undergraduate Texts in Mathematics)*. Springer-Verlag, Berlin, Heidelberg, 2007.

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

[12] Andreas Dolzmann, Thomas Sturm, and Volker Weispfenning. A new approach for automatic theorem proving in real geometry. *J. Autom. Reason.*, 21(3):357–380, December 1998.

[13] Andreas Dolzomann and Lorenz A. Gilch. Generic hermitian quantifier elimination. In Bruno Buchberger and John Campbell, editors, *Artificial Intelligence and Symbolic Computation*, pages 80–93, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[14] David Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995.

[15] Jean-Charles Faugère. FGb: A Library for Computing Gröbner Bases. In *Mathematical Software - ICMS 2010*, volume 6327 of *Lecture Notes in Computer Science*, pages 84–87. Springer Berlin / Heidelberg, 2010.

[16] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. On the complexity of the generalized minrank problem. *J. Symb. Comput.*, 55:30 – 58, 2013.

[17] D. Yu Grigor'ev. Complexity of deciding Tarski algebra. *J. Symb. Comput.*, 5(1–2):65–108, February 1988.

[18] Charles Hermite. 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, 1856.

[19] Hoon Hong. An improvement of the projection operator in Cylindrical Algebraic Decomposition. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC '90, page 261–264, New York, NY, USA, 1990. Association for Computing Machinery.

[20] Hoon Hong and Mohab Safey El Din. Variant real quantifier elimination: Algorithm and application. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, ISSAC '09, page 183–190, New York, NY, USA, 2009. Association for Computing Machinery.

[21] Hoon Hong and Mohab Safey El Din. Variant quantifier elimination. *J. Symb. Comput.*, 47(7):883 – 901, 2012. International Symposium on Symbolic and Algebraic Computation (ISSAC 2009).

[22] Huu Phuoc Le and Mohab Safey El Din. Solving parametric systems of polynomial equations over the reals through Hermite matrices. Preprint, November 2020.

[23] Richard Liska and Stanly L. Steinberg. Applying Quantifier Elimination to Stability Analysis of Difference Schemes. *The Computer Journal*, 36(5):497–503, 01 1993.

[24] Scott McCallum. An improved projection operation for Cylindrical Algebraic Decomposition of three-dimensional space. *J. Symb. Comput.*, 5:141 – 161, 1988.

[25] Scott McCallum. On projection in CAD-based quantifier elimination with equational constraint. In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation*, ISSAC '99, page 145–149, New York, NY, USA, 1999. Association for Computing Machinery.

[26] Jiawang Nie and Kristian Ranestad. Algebraic degree of polynomial optimization. *SIAM J. on Optimization*, 20(1):485–502, April 2009.

[27] P. Pedersen, Marie-Françoise Roy, and Aviva Szpirglas. Counting real zeros in the multivariate case. In Frédéric Eyssette and André Galligo, editors, *Computational Algebraic Geometry*, pages 203–224, Boston, MA, 1993. Birkhäuser Boston.

[28] James Renegar. On the computational complexity and geometry of the first-order theory of the reals. Part III: Quantifier elimination. *J. Symb. Comput.*, 13(3):329–352, March 1992.

[29] Mohab Safey El Din. Real alebraic geometry library, RAGlib (version 3.4), 2017.

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

[31] Mohab Safey El Din and Éric Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM*, 63(6):48:1–48:37, January 2017.

[32] A. Seidenberg. A new decision method for elementary algebra. *Annals of Mathematics*, 60(2):365–374, 1954.

[33] Andreas Seidl and Thomas Sturm. A generic projection operator for partial cylindrical algebraic decomposition. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, ISSAC '03, page 240–247, New York, NY, USA, 2003. Association for Computing Machinery.

[34] Igor R. Shafarevich. *Basic Algebraic Geometry 1: Varieties in Projective Space*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[35] Pierre-Jean Spaenlehauer. On the complexity of computing critical points with Gröbner bases. *SIAM Journal on Optimization*, 24:1382–1401, 07 2014.

[36] Adam W. Strzeboński. Cylindrical Algebraic Decomposition using validated numerics. *J. Symb. Comput*, 41(9):1021 – 1038, 2006.

[37] Thomas Sturm and Ashish Tiwari. Verification and synthesis using real quantifier elimination. In *Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, ISSAC '11, page 329–336, New York, NY, USA, 2011. Association for Computing Machinery.

[38] Thomas Sturm and Volker Weispfenning. Computational geometry problems in REDLOG. In *Selected Papers from the International Workshop on Automated Deduction in Geometry*, page 58–86, Berlin, Heidelberg, 1996. Springer-Verlag.

[39] Alfred Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, 1951.

[40] V. Weispfenning. A new approach to quantifier elimination for real algebra. In *Quantifier Elimination and Cylindrical Algebraic Decomposition*, pages 376–392, Vienna, 1998. Springer Vienna.

[41] Volker Weispfenning. The complexity of linear problems in fields. *J. Symb. Comput.*, 5(1):3–27, 1988.

[42] Volker Weispfenning. Comprehensive gröbner bases. *Journal of Symbolic Computation*, 14(1):1–29, 1992.