

Faster One Block Quantifier Elimination for Regular Polynomial Systems of Equations

Huu Phuoc Le

Sorbonne Université, CNRS, LIP6, Équipe PolSys
F-75252, Paris Cedex 05, France
huu-phuoc.le@lip6.fr

Mohab Safey El Din

Sorbonne Université, CNRS, LIP6, Équipe PolSys
F-75252, Paris Cedex 05, France
mohab.safey@lip6.fr

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 $O\left((n-s+1)8^t \mathcal{D}^{3t+2} \binom{t+\mathcal{D}}{t}\right)$ 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).

CCS CONCEPTS

• Computing methodologies → Symbolic and algebraic algorithms; Equation and inequality solving algorithms; • Theory of computation → Computational geometry.

KEYWORDS

Quantifier elimination; Effective real algebraic geometry; Polynomial system solving

Huu Phuoc Le and Mohab Safey El Din are supported by the ANR grants ANR-18-CE33-0011 Sesame, and ANR-19-CE40-0018 De Rerum Natura, the joint ANR-FWF ANR-19-CE48-0015 ECARP project and the European Union’s Horizon 2020 research and innovative training network program under the Marie Skłodowska-Curie grant agreement N° 813211 (POEMA).

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ISSAC '21, July 18–23, 2021, Virtual Event, Russian Federation.

© 2021 Association for Computing Machinery.

ACM ISBN 978-1-4503-8382-0/21/07...\$15.00

<https://doi.org/10.1145/3452143.3465546>

ACM Reference Format:

Huu Phuoc Le and Mohab Safey El Din. 2021. Faster One Block Quantifier Elimination for Regular Polynomial Systems of Equations. In Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation (ISSAC '21), July 18–23, 2021, Virtual Event, Russian Federation. ACM, New York, NY, USA, 10 pages. <https://doi.org/10.1145/3452143.3465546>

1 INTRODUCTION

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

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

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

Let π be the projection $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{y}$. Note that, geometrically, Φ describes the projection on the \mathbf{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 [32, 39] 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 [6, 19, 24, 25] or the partial CAD [9]. Following the idea of [17] that exploits the block structure, [3, 28] 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 [7, 36, 38, 40, 42] and applications to other fields [1, 23, 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 $f = (f_1, \dots, f_s)$ satisfying the assumptions below.

Assumption A.

- The ideal of $\mathbb{Q}[\mathbf{x}, \mathbf{y}]$ generated by f is radical.
- The algebraic set $\mathcal{V} \subset \mathbb{C}^{t+n}$ of 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 f . Our algorithm applies the algorithm of [30] to the system f considering $\mathbb{Q}(\mathbf{y})$ as the based field. This allows to reduce our problem to zero-dimensional polynomial systems in $\mathbb{Q}(\mathbf{y})[\mathbf{x}]$. Next, we compute semi-algebraic formulas that describe approximate projections of these systems on the \mathbf{y} -space through the algorithm of [22]. This algorithm relies on a parametric variant of Hermite matrices for real root counting [18, 27]. A similar outline is also presented in [13, 42], in which the author computes an expensive comprehensive Gröbner bases [41] 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 $\mathbb{C}[\mathbf{x}, \mathbf{y}]_{\leq D} = \{p \in \mathbb{C}[\mathbf{x}, \mathbf{y}] \mid \deg(p) \leq D\}$. A property P is said to be generic over $\mathbb{C}[\mathbf{x}, \mathbf{y}]_D^s$ if and only if there exists

a non-empty Zariski open subset $\mathcal{P} \subset \mathbb{C}[\mathbf{x}, \mathbf{y}]_D^s$ such that the property P holds for every $f \in \mathcal{P}$.

Our complexity result is then stated below. The notation $O \sim(g)$ 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 \mathcal{F} of $\mathbb{C}[\mathbf{x}, \mathbf{y}]_{\leq D}^s$ and a probabilistic algorithm such that, for every $f \in \mathcal{F}$, this algorithm, in case of success, computes a semi-algebraic formula Φ defining a dense subset of the interior of $\pi(V(f) \cap \mathbb{R}^{t+n})$ within

$$O \sim \left((n-s+1) 8^t \mathcal{D}^{3t+2} \binom{t+\mathcal{D}}{t} \right)$$

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

Even though our complexity result has the same order as the one of [4, Algo 14.6], we obtain explicitly the degree bounds on the output formulas and the 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 $F \subset \mathbb{F}[x_1, \dots, x_n]$. 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 $I(\mathcal{V}) \subset \mathbb{C}[x_1, \dots, x_n]$ the radical ideal associated to \mathcal{V} . The singular locus of \mathcal{V} is denoted by $\text{sing}(\mathcal{V})$. 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 $\varphi_1, \dots, \varphi_i \in \mathbb{C}[x_1, \dots, x_n]$ such that $\varphi(\eta) = (\varphi_1(\eta), \dots, \varphi_i(\eta))$ for $\eta \in \mathcal{V}$. Let $\mathcal{V} \subset \mathbb{C}^n$ be an equi-dimensional algebraic set. We denote by $\text{crit}(\varphi, \mathcal{V})$ 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, \dots, f_s) generates the ideal $I(\mathcal{V})$, the subset of \mathcal{V} at which the Jacobian matrix $\text{jac}(f_1, \dots, f_s, \varphi_1, \dots, \varphi_i)$ of $(f_1, \dots, f_s, \varphi_1, \dots, \varphi_i)$ has rank less than or equal to c is the union of $\text{crit}(\varphi, \mathcal{V})$ and $\text{sing}(\mathcal{V})$ (see, e.g., [31, Subsection 3.1]).

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 $>$ (see [10, Sec. 2.2]) over $\mathbb{F}[\mathbf{x}]$ where $\mathbf{x} = (x_1, \dots, x_n)$. For $p \in \mathbb{F}[\mathbf{x}]$, the leading monomial of p with respect to $>$ is denoted by $\text{lm}_>(p)$.

A Gröbner basis G of an ideal $I \subset \mathbb{F}[\mathbf{x}]$ w.r.t. the order $>$ is a finite generating set of I such that the set of leading monomials $\{\text{lm}_>(g) \mid g \in G\}$ generates $\langle \text{lm}_>(p) \mid p \in I \rangle$. For $p \in \mathbb{F}[\mathbf{x}]$, the remainder of the division of p by G using the order $>$ 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 $\mathbb{F}[\mathbf{x}]/I$ 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 \mathbf{x} which are irreducible by G forms a monomial basis, denoted by B , of this vector space. For $p \in \mathbb{F}[\mathbf{x}]$, the normal form of p by G can be interpreted as its image in $\mathbb{F}[\mathbf{x}]/I$ and is a \mathbb{F} -linear combination of elements of B .

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

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

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

3 ALGORITHM FOR REAL ROOT FINDING

3.1 The S^2 algorithm

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

Let $\mathbf{f} = (f_1, \dots, f_s)$ be a polynomial sequence in $\mathbb{R}[x_1, \dots, x_n]$. For $1 \leq i \leq d$, let ϕ_i be the projection $(x_1, \dots, x_n) \rightarrow (x_1, \dots, x_i)$. When \mathbf{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 $\text{jac}(\mathbf{f})$ to define

$\text{crit}(\phi_i, \mathcal{V})$. Note that the critical loci are nested

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

Note also that in generic coordinates $\text{crit}(\phi_i, \mathcal{V})$ 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 \mathbf{f} defines a smooth equi-dimensional algebraic set and generates a radical ideal.

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

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

The first item in Proposition 2 implies the second one. The index in the notation $\mathcal{A}_{\mathbf{f}}$ indicates that the non-empty Zariski open set depends on \mathbf{f} . Algorithm S^2 considers fibers of the above critical loci with the convention $\pi_0 : \mathbf{x} \rightarrow \bullet$. 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 \mathbf{f} defines a smooth equi-dimensional algebraic set and generates a radical ideal.

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

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

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 $\text{jac}(\mathbf{f})$ writes simply $(2x_1, -2x_2, -2x_3)$. It turns out that the identity matrix lies in the set \mathcal{A} defined in Proposition 2. Taking $\alpha = (0, 0)$, we obtain 3 zero-dimensional systems:

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

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

Considering $\mathbb{Q}(\mathbf{y})$ as the ground field, the parametric variant of S^2 computes on the input \mathbf{f} a list of finite subsets of $\mathbb{Q}(\mathbf{y})[\mathbf{x}]$, each of which generates a zero-dimensional ideal of $\mathbb{Q}(\mathbf{y})[\mathbf{x}]$. These subsets are basically $f^A \cup \Delta_i^A \cup \{x_1 - \alpha_1, \dots, x_{i-1} - \alpha_{i-1}\}$, where (A, α) is randomly chosen in $\text{GL}(n, t, \mathbb{Q}) \times \mathbb{Q}^n$ and Δ_i^A is the set of all $(n-d)$ -minors of the Jacobian matrix of 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 \mathcal{B} of \mathbb{C}^t such that for every $\eta \in \mathcal{B}$, the specialization $f(\eta, \cdot)$ of \mathbf{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 \mathcal{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 $\text{jac}_{\mathbf{x}}(\mathbf{f})$ of \mathbf{f} w.r.t. \mathbf{x} has rank at most $n-d-1$. We note that $\mathcal{W} = \text{crit}(\pi, \mathcal{V}) \cup \text{sing}(\mathcal{V})$. The algebraic version of Sard's theorem [31, Proposition B2] implies that $\pi(\text{crit}(\pi, \mathcal{V}))$ is contained in a proper Zariski closed subset of \mathbb{C}^t . On the other hand, as Assumptions (A) hold, the dimension of $\pi(\text{sing}(\mathcal{V}))$ 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 \mathcal{B} be the intersection of the complement in \mathbb{C}^t of this Zariski closure with \mathcal{B}' . For $\eta \in \mathcal{B}$, the set

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

is empty. Since the dimension of $\pi^{-1}(\eta) \cap \mathcal{V}$ is d and the Jacobian matrix $\text{jac}_{\mathbf{x}}(\mathbf{f})(\eta, \cdot)$ of $f(\eta, \cdot)$ w.r.t. the variables \mathbf{x} is of rank $n-d$ for every $(\eta, \mathbf{x}) \in \mathcal{V} \cap \pi^{-1}(\eta)$, the ideal $f(\eta, \cdot)$ 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 $\mathbf{y} = (y_1, \dots, y_t)$ to a generic point $\eta \in \mathcal{B} \cap \mathbb{R}^t$ in \mathbf{f} , one obtains $f(\eta, \cdot)$ satisfying the assumptions of Proposition 2. One could then apply Algorithm S^2 to $f(\eta, \cdot)$ to grab sample points in the real algebraic set it defines. However, proceeding this way would lead us to use a change of variables encoded by a matrix A depending on η . The result below shows that choosing one generic change of variables will be valid for most of parameters' values.

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

There exists a dense Zariski open subset \mathcal{A}_A of \mathbb{C}^t such that \mathcal{A}_A is a subset of the Zariski open set \mathcal{B} in Lemma 5 and A lies in the Zariski open set $\mathcal{A}_f(\eta, \cdot)$ defined in Proposition 2 for every $\eta \in \mathcal{A}_A$.

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

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

The denominators of $p_{i,j}$ are then polynomials in $\mathbb{Q}(\mathbf{y})$. We choose \mathcal{A}_A to be the intersection of the non-empty Zariski open set \mathcal{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 $\eta \notin \mathcal{A}_A$, $p_{i,j}(\eta, \cdot) \in \mathbb{Q}[x_1, \dots, x_{i-1}, x_j]$ is monic in x_j . Consequently, (x_i, \dots, x_n) is in Noether position w.r.t. the ideal of $\mathbb{C}[\mathbf{x}]$ generated by $f^A(\eta, \cdot) \cup \Delta_i^A(\eta, \cdot)$. Finally, taking $\mathcal{O} = \tilde{\mathcal{O}} \cap \text{GL}(n, t, \mathbb{C})$, the conclusion follows. \square

4 ONE-BLOCK QE 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 $\mathbf{f} = (f_1, \dots, f_s) \subset \mathbb{C}[\mathbf{x}, \mathbf{y}]$ satisfying Assumptions (A) and (B). Further, we denote by $Z(\Psi)$ the zero set of any semi-algebraic formula Ψ , i.e., $Z(\Psi) = \{\mathbf{y} \in \mathbb{R}^t \mid \Psi(\mathbf{y}) \text{ is true}\}$.

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 $\mathbb{Q}(\mathbf{y})$ as a ground field.

More precisely, we start by picking randomly (A, α) in $\text{GL}(n, t, \mathbb{Q}) \times \mathbb{Q}^n$ and apply the change of variables $\mathbf{x} \mapsto A \cdot \mathbf{x}$ to the input \mathbf{f} to obtain a new sequence f^A . As A acts only on \mathbf{x} , $\pi(V(f^A) \cap \mathbb{R}^{n+t}) = \pi(\mathcal{V}_{\mathbb{R}})$. Hence, a quantifier-free formula that solves our problem for f^A is also a solution of the same problem for \mathbf{f} .

Let $\text{jac}_{\mathbf{x}}(f^A)$ be the Jacobian matrix of f^A w.r.t. the variables $\mathbf{x} = (x_1, \dots, x_n)$. We denote by J_1, \dots, J_n the columns of $\text{jac}_{\mathbf{x}}(f^A)$ respectively. For $1 \leq i \leq d$, let $W_i^{A, \alpha}$ be the union of 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 $f^A \cup \{x_1 - \alpha_1, \dots, x_d - \alpha_d\}$.

We prove later in Lemma 8 that, for generic (A, α) , the ideals of $\mathbb{Q}(\mathbf{y})[\mathbf{x}]$ 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 $F \subset \mathbb{Q}[\mathbf{y}][\mathbf{x}]$ such that the ideal of $\mathbb{Q}(\mathbf{y})[\mathbf{x}]$ generated by F is radical and zero-dimensional and computes a quantifier-free formula Φ_F in \mathbf{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 $\Phi = \bigvee_{i=1}^{d+1} \Phi_i$ as the output of our algorithm.

The pseudo-code below summarizes our algorithm, we introduce two additional subroutines:

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

Algorithm 1: One-block quantifier elimination

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

- 1 Choose randomly $(A, \alpha) \in \text{GL}(n, \mathbb{Q}) \times \mathbb{Q}^n$
 - 2 $f^A \leftarrow f(A \cdot \mathbf{x})$
 - 3 $[J_1, \dots, J_n] \leftarrow \text{jac}_{\mathbf{x}}(f^A)$
 - 4 $d \leftarrow \text{GenericDimension}(f^A)$
 - 5 for $1 \leq i \leq d+1$ do
 - 6 $W_i^{A,\alpha} \leftarrow (n-d)$ `Minors` ($[J_{i+1}, \dots, J_n] \cup \{f^A, x_1 - \alpha_1, \dots, x_{i-1} - \alpha_{i-1}\}$)
 - 7 $\Phi_i \leftarrow \text{RealRootClassification}(W_i^{A,\alpha})$
 - 8 return $\Phi \leftarrow \bigvee_{i=1}^{d+1} \Phi_i$
-

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

For such an input F , `RealRootClassification` computes a semi-algebraic formula Φ_F and a polynomial $w_\infty \in \mathbb{Q}[\mathbf{y}]$ 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 $\mathbb{Q}(\mathbf{y})$ 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 $\mathbb{Q}[\mathbf{x}, \mathbf{y}]$ generated by F w.r.t. the $\text{grevlex}(\mathbf{x}) > \text{grevlex}(\mathbf{y})$ order. We consider the leading coefficients of the elements of G_F in variables \mathbf{x} w.r.t. the $\text{grevlex}(\mathbf{x})$ order, which are polynomials

in $\mathbb{Q}[\mathbf{y}]$. Then, w_F is taken as the square-free part of the product of these leading coefficients. The polynomial w_F defines a proper algebraic subset of \mathbf{y} -space over which the matrix H_F does not have good specialization property ([22, Proposition 16]).

Next, we choose randomly a matrix $Q \in \text{GL}(\delta, \mathbb{Q})$. As the entries of H_F lie in $\mathbb{Q}(\mathbf{y})$, so do the leading principal minors M_1, \dots, M_δ of $Q^T \cdot H_F \cdot Q$. Let m_1, \dots, m_δ be the numerators of those minors, which are in $\mathbb{Q}[\mathbf{y}]$. 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 $\bigwedge_{i=1}^\delta (m_i \neq 0) \wedge (w_F \neq 0)$. 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

$$\Phi_F = \left(\bigvee_{\eta \in L_0} \left(\bigwedge_{i=1}^\delta \text{sign } M_i = \text{sign } M_i(\eta) \right) \right) \wedge (w_F \neq 0).$$

Then, w_∞ is taken as the product of the m_i 's and w_F . We return Φ_F, w_∞ as the output of `RealRootClassification` for F . The correctness of this algorithm is given in [22, Proposition 28].

In the pseudo-code below, we introduce the subroutines

- `HermiteMatrix` which takes as input a polynomial sequence $F \subset \mathbb{Q}[\mathbf{y}][\mathbf{x}]$ such that the ideal $\langle F \rangle \subset \mathbb{Q}(\mathbf{y})[\mathbf{x}]$ is zero-dimensional and computes the parametric Hermite matrix associated to F w.r.t. the $\text{grevlex}(\mathbf{x})$ 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 $m_1, \dots, m_\delta, w_F \in \mathbb{Q}[\mathbf{y}]$ and computes a finite set of points that intersects every connected component of the semi-algebraic set defined by $\bigwedge_{i=1}^\delta m_i \neq 0 \wedge w_F \neq 0$. 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 $w_{1,\infty} = w_{2,\infty} = y_1$

Algorithm 2: RealRootClassification

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

Output: A formula Φ_F and a polynomial $w_\infty \in \mathbb{Q}[\mathbf{y}]$.

- 1 $H_F, w_F \leftarrow \text{HermiteMatrix}(F)$
- 2 Choose randomly $Q \in \text{GL}(\delta, \mathbb{Q})$ // δ is the size of H_F
- 3 $(M_1, \dots, M_\delta) \leftarrow \text{PrincipalMinors}(Q^T \cdot H_F \cdot Q)$
- 4 $(m_1, \dots, m_\delta) \leftarrow \text{Numerators}(M_1, \dots, M_\delta)$
- 5 $L \leftarrow \text{SamplePoints}\left(\left(\bigwedge_{i=1}^\delta m_i \neq 0\right) \wedge w_F \neq 0\right)$
- 6 for $\eta \in L$ do
- 7 if $\text{Signature}(H_F(\eta)) \neq 0$ then
- 8 $\Phi_F \leftarrow \Phi_F \vee \left(\bigwedge_{i=1}^\delta \text{sign } M_i = \text{sign } M_i(\eta)\right)$
- 9 $\Phi_F \leftarrow \Phi_F \wedge (w_F \neq 0)$
- 10 $w_\infty \leftarrow w_F \cdot \prod_{i=1}^\delta m_i$
- 11 return Φ_F, w_∞

and the Hermite matrices:

$$H_1 = \begin{pmatrix} 2 & 0 \\ 0 & -2y_3 + y_2^2/(2y_1) \end{pmatrix}, \quad H_2 = \begin{pmatrix} 2 & -y_2/y_1 \\ -y_2/y_1 & (-2y_1y_3 + y_2^2)/y_1^2 \end{pmatrix}.$$

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 $\pi(V(f) \cap \mathbb{R}^5)$.

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 \mathcal{O} be the Zariski open subset of $\text{GL}(n, t, \mathbb{C})$ defined in Proposition 6 and $A \in \mathcal{O} \cap \text{GL}(n, t, \mathbb{Q})$. There exists a non-empty Zariski open subset \mathcal{X} of \mathbb{C}^d such that for $\alpha \in \mathcal{X} \cap \mathbb{Q}^d$, the ideal of $\mathbb{Q}(\mathbf{y})[\mathbf{x}]$ 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 \mathcal{Z}_A of \mathbb{C}^t . Thus, the ideal of $\mathbb{Q}(\mathbf{y})[\mathbf{x}]$ 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_ℓ^A be the $(n-d)$ minors of the Jacobian matrix J associated to 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 f^A with the M_1^A, \dots, M_ℓ^A with $x_1 - \alpha_1, \dots, x_{i-1} - \alpha_{i-1}$. Further, we denote by $W_i^A \subset \mathbb{Q}(\mathbf{y})[\mathbf{x}]$ the ideal generated by $f^A, M_1^A, \dots, M_\ell^A$.

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 f^A and M_1^A, \dots, M_ℓ^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 $\mathbb{Q}(\mathbf{y})[\mathbf{x}]_m$ the localized ring where divisions by powers of m are allowed.

By [31, Lemma B.12] there exists a non-empty Zariski open set $\mathcal{O}'_{m,n-d}$ such that for $A \in \text{GL}(n, t, \mathbb{C})$, 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 $\mathbb{Q}(\mathbf{y})[\mathbf{x}]_m$ is radical and coincides with the localization of W_i^A in $\mathbb{Q}(\mathbf{y})[\mathbf{x}]_m$. By [31, Prop. 3.4], there exists a non-empty Zariski open set $\mathcal{O}'' \subset \text{GL}(n, t, \mathbb{C})$ such that for $A \in \mathcal{O}''$, 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 \mathcal{O} (defined in Proposition 6), all non-empty Zariski open sets $\mathcal{O}'_{m,k}$ and \mathcal{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 $\mathcal{X}_i \subset \mathbb{C}^{i-1}$ such that for $\alpha = (\alpha_1, \dots, \alpha_{i-1}) \in \mathcal{X}_i$, $\langle W_i^A \rangle + \langle x_1 - \alpha_1, \dots, x_{i-1} - \alpha_{i-1} \rangle$ is radical in $\mathbb{Q}(\mathbf{y})[\mathbf{x}]$. Choosing α outside the set of critical values of π_i restricted to the algebraic set defined by W_i^A in $\overline{\mathbb{Q}(\mathbf{y})}^n$ is enough. By Sard's theorem, this set of critical values is contained in the vanishing set of a non-zero polynomial $v \in \mathbb{Q}[\mathbf{y}][\mathbf{x}]$. Now note that it suffices to define \mathcal{X}_i as the complement of the vanishing set of the coefficients of v when it is seen in $\mathbb{Q}[\mathbf{x}][\mathbf{y}]$ and $\mathcal{X} = \bigcap_{i=1}^{d+1} \mathcal{X}_i$. \square

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

Proposition 9. Assume that Assumptions (A) and (B) hold. Let $\mathcal{O} \subset \text{GL}(n, t, \mathbb{C})$ and $\mathcal{X} \subset \mathbb{C}^d$ be defined respectively in Proposition 6 and Lemma 8. Then for $A \in \mathcal{O} \cap \text{GL}(n, t, \mathbb{Q})$ and $\alpha \in \mathcal{X} \cap \mathbb{Q}^d$, 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 \mathbf{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, $Z(\Phi) = \bigcup_{i=1}^{d+1} Z(\Phi_i) \subset \pi(\mathcal{V}_{\mathbb{R}})$.

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

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

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

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

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

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 $\pi(\mathcal{V}_{\mathbb{R}})$. \square

5 COMPLEXITY ANALYSIS

We now estimate the arithmetic complexity of Algorithm 1 once $A \in \mathcal{O} \cap \text{GL}(n, t, \mathbb{Q})$ and $\alpha \in \mathcal{X} \cap \mathbb{Q}^n$ as in Proposition 6 are found from a random choice. In this section, the input f forms a regular sequence of $\mathbb{Q}[\mathbf{x}, \mathbf{y}]$ (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 $F \subset \mathbb{Q}[\mathbf{x}, \mathbf{y}]$ and G be the reduced Gröbner basis of F w.r.t. the $\text{grevlex}(\mathbf{x}) > \text{grevlex}(\mathbf{y})$ 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 \mathbf{x} and \mathbf{y} equals the degree of g w.r.t. only \mathbf{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 $\mathbb{Q}[\mathbf{y}]$. 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 f . The zero-dimensional ideal of $\mathbb{Q}(\mathbf{y})[\mathbf{x}]$ generated by $W_i^{A,\alpha}$ is denoted by $\langle W_i^{A,\alpha} \rangle$. The quotient ring $\mathbb{Q}(\mathbf{y})[\mathbf{x}] / \langle W_i^{A,\alpha} \rangle$ is a finite dimensional $\mathbb{Q}(\mathbf{y})$ -vector space. Let G_i be the reduced Gröbner basis of the ideal of $\mathbb{Q}[\mathbf{x}, \mathbf{y}]$ generated by $W_i^{A,\alpha}$ w.r.t. $\text{grevlex}(\mathbf{x}) > \text{grevlex}(\mathbf{y})$ and B_i be the monomial basis of $\mathbb{Q}(\mathbf{y})[\mathbf{x}] / \langle W_i^{A,\alpha} \rangle$ constructed using G_i as 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 $\mathbb{Q}(\mathbf{y})[\mathbf{x}] / \langle W_i^{A,\alpha} \rangle$. \square

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 $\mathbb{Q}(\mathbf{y})[\mathbf{x}] / \langle W_i^{A,\alpha} \rangle$ when 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 dense Zariski open subset \mathcal{Q} of $\mathbb{C}[\mathbf{x}, \mathbf{y}]_{\leq D}^s$ such that, for $f \in \mathcal{Q}$, the following inequality holds for $1 \leq i \leq d+1$:

$$\sum_{b \in B_i} \deg_{\mathbf{x}}(b) \leq (n+s-i) D^s (D-1)^{n-i-s+2} \binom{n-i+1}{s}.$$

Proof. By [26, Theorem 2.2], there exists a dense Zariski open subset $\mathcal{Q}_{1,1} \subset \mathbb{C}[\mathbf{x}, \mathbf{y}]_{\leq D}^s$ such that for $f \in \mathcal{Q}_{1,1}$, the degree of $\langle W_1^{A,\alpha} \rangle$, which equals to the cardinality of B_1 , is bounded by

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

On the other hand, by [35, Corollary 3.2], there exists a dense Zariski open subset $\mathcal{Q}_{1,2} \subset \mathbb{C}[\mathbf{x}, \mathbf{y}]_{\leq D}^s$ such that for $f \in \mathcal{Q}_{1,2}$, the witness degree, i.e., the highest degree appeared in the reduced Gröbner basis of $W_1^{A,\alpha}$ w.r.t. $\text{grevlex}(\mathbf{x})$, 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 $\mathcal{Q}_1 = \mathcal{Q}_{1,1} \cap \mathcal{Q}_{1,2}$ and, for $f \in \mathcal{Q}_1$, we obtain

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

For $1 \leq i \leq d$, 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 $V(f^A(\alpha_1, \dots, \alpha_{i-1}, x_i, \dots, x_n))$. Therefore, by replacing n by $n-i+1$ in the above bound, we deduce that, for $1 \leq i \leq d$, there exists a dense Zariski open subset $\mathcal{Q}_i \subset \mathbb{C}[\mathbf{x}, \mathbf{y}]_{\leq D}^s$ such that

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

For $i = d+1$, the cardinality of B_{d+1} is bounded by D^s and the highest degree in B_{d+1} is bounded by $s(D-1)$. Thus, the bound holds for $i = d+1$. Taking $\mathcal{Q} = \bigcap_{i=1}^{d+1} \mathcal{Q}_i$, we conclude the proof. \square

Further, \mathcal{D} denotes $2(n+s-1)D^s(D-1)^{n-s+1}\binom{n}{s}$. Now we show that Assumption (C) holds generically then prove Theorem 1.

Proposition 12. There exists a dense Zariski open subset $\mathcal{P} \subset \mathbb{C}[\mathbf{x}, \mathbf{y}]_{\leq D}^s$ such that, for every $\mathbf{f} \in \mathcal{P}$, there exists a dense Zariski open subset $\mathcal{K}_{\mathbf{f}} \subset \text{GL}(n, t, \mathbb{C}) \times \mathbb{C}^n$ such that for $(A, \alpha) \in \mathcal{K}_{\mathbf{f}}$, Assumption (C) holds for every system $W_i^{A, \alpha}$.

Proof. Let y_{t+1} be a new variable and ${}^h\mathbb{Q}[\mathbf{x}, \mathbf{y}, y_{t+1}]_D$ be the set of homogeneous polynomials in $\mathbb{Q}[\mathbf{x}, \mathbf{y}, y_{t+1}]$ of degree D . For $F \in \mathbb{Q}[\mathbf{x}, \mathbf{y}]$, we denote by ${}^hF \in \mathbb{Q}[\mathbf{x}, \mathbf{y}, y_{t+1}]$ the homogenization of F w.r.t. all the variables (\mathbf{x}, \mathbf{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 $\mathbb{C}[\mathbf{x}, \mathbf{y}, y_{t+1}]$ 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. $\text{grevlex}(\mathbf{x} > \mathbf{y} > y_{t+1})$ do not involve any of the variables y_1, \dots, y_{t+1} . By the proof of [22, Prop. 30], 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 $\mathbb{C}[\mathbf{x}, \mathbf{y}, y_{t+1}]/\langle {}^hF, y_1, \dots, y_j \rangle_h$ for every $0 \leq j \leq t$, then F satisfies the property (C1). This property means that (y_1, \dots, y_{t+1}) forms a regular sequence in the quotient ring $\mathbb{C}[\mathbf{x}, \mathbf{y}, y_{t+1}]/\langle {}^hF \rangle_h$. 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 $\mathcal{P}_1 \subset \mathbb{C}[\mathbf{x}, \mathbf{y}]_{\leq D}^s$ such that for $\mathbf{f} \in \mathcal{P}_1$, there exists a dense Zariski open subset $\mathcal{K}_{\mathbf{f}, 1} \subset \text{GL}(n, t, \mathbb{C}) \times \mathbb{C}^n$ such that for $(A, \alpha) \in \mathcal{K}_{\mathbf{f}, 1}$, the quotient ring $\mathbb{C}[\mathbf{x}, \mathbf{y}, y_{t+1}]/\langle {}^hW_1^{A, \alpha} \rangle_h$ 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 $\mathbb{C}[\mathbf{x}, \mathbf{y}, y_{t+1}]/\langle {}^hW_1^{A, \alpha} \rangle_h$. 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 $\mathcal{P}_i \subset \mathbb{C}[\mathbf{x}, \mathbf{y}]_{\leq D}^s$ and $\mathcal{K}_{\mathbf{f}, i} \subset \text{GL}(n, t, \mathbb{C}) \times \mathbb{C}^n$ for each $\mathbf{f} \in \mathcal{P}_i$. Taking $\mathcal{P} = \bigcap_{i=1}^{d+1} \mathcal{P}_i$, and $\mathcal{K}_{\mathbf{f}} = \bigcap_{i=1}^{d+1} \mathcal{K}_{\mathbf{f}, i}$, we conclude the proof. \square

Proof of Theorem 1. It is well-known that Assumptions (A) and (B) are generic. Also, the set of regular sequences is dense in $\mathbb{C}[\mathbf{x}, \mathbf{y}]_{\leq D}^s$. Thus, there exists a dense Zariski open subset $\mathcal{R} \subset \mathbb{C}[\mathbf{x}, \mathbf{y}]_{\leq D}^s$ such that for any $\mathbf{f} \in \mathcal{R}$, \mathbf{f} forms a regular sequence satisfying Assumptions (A) and (B). As $V(\mathbf{f})$ has dimension $d+t$ and \mathbf{f} forms a regular sequence in $\mathbb{Q}[\mathbf{x}, \mathbf{y}]$, $d = n-s$. Algorithm 1 consists of $(d+1)$ calls to `RealRootClassification` on $W_i^{A, \alpha}$. Let \mathcal{P} be the dense Zariski open set in Proposition 12 and $\mathcal{Q} = \mathcal{P} \cap \mathcal{R}$. Then, for $\mathbf{f} \in \mathcal{Q}$, `SamplePoints` is called on a list of polynomials in $\mathbb{Q}[\mathbf{y}]$ of degree bounded by \mathcal{D} . The number of principal minors is equal to the dimension of the quotient ring $\mathbb{Q}(\mathbf{y})[\mathbf{x}]/\langle W_i^{A, \alpha} \rangle$, which is also bounded

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

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 is done by RAGlib [29] which uses `msolve` [5] for polynomial 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.

Start with random dense systems, we fix the total degree $D = 2$ and run our algorithm for various (t, n, s) . In Table 1, `SamplePoints` accounts for the major part of our timings. While our algorithm can tackle these examples, neither maple nor mathematica finish within 72h. The theoretical degree bound agrees with the practical observations. This agrees with our complexity result. On smaller problems, we observe that formulas computed by maple and mathematica have larger degrees than our output. Hence, these implementations, based on CAD, suffer from its doubly exponential complexity while our implementation takes advantage of the singly exponential complexity of our algorithm.

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 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, our algorithm runs faster here than in Table 1 while these examples are out of reach of maple and mathematica.

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 $D = 2$

Table 3 gives the timings for structured systems. We separate the variables \mathbf{x} into blocks of total degree 1; $[i, n - i]$ means that the degree in $[x_1, \dots, x_i]$ and $[x_{i+1}, \dots, x_n]$ are respectively 1. 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] Anai, H., and Weispfenning, V. Reach set computations using real quantifier elimination. In *Hybrid Systems: Computation and Control* (2001), Springer Berlin Heidelberg, pp. 63–76.
- [2] Bardet, M., Faugère, J.-C., and Salvy, B. On the complexity of the F5 Gröbner basis algorithm. *J. Symb. Comput.* 70 (2015), 49–70.
- [3] Basu, S., Pollack, R., and Roy, M.-F. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM* 43, 6 (Nov. 1996), 10021045.
- [4] Basu, S., Pollack, R., and Roy, M.-F. *Algorithms in Real Algebraic Geometry*. Springer-Verlag, Berlin, Heidelberg, 2006.
- [5] Berthomieu, J., Eder, C., and Safey El Din, M. *msolve: A Library for Solving Polynomial Systems*. Preprint, Feb. 2021.
- [6] Brown, C. W. Improved projection for Cylindrical Algebraic Decomposition. *J. Symb. Comput.* 32, 5 (2001), 447 – 465.
- [7] Brown, C. W., and Gross, C. Efficient preprocessing methods for quantifier elimination. In *Computer Algebra in Scientific Computing* (Berlin, Heidelberg, 2006), Springer Berlin Heidelberg, pp. 89–100.
- [8] Collins, G. E. Quantifier elimination for real closed fields by cylindrical algebraic decomposition: a synopsis. *ACM SIGSAM Bulletin* 10, 1 (1976), 10–12.
- [9] Collins, G. E., and Hong, H. Partial Cylindrical Algebraic Decomposition for quantifier elimination. *J. Symb. Comput.* 12, 3 (1991), 299 – 328.
- [10] Cox, D. A., Little, J., and OShea, D. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, (Undergraduate Texts in Mathematics). Springer-Verlag, Berlin, Heidelberg, 2007.
- [11] Davenport, J. H., and Heintz, J. Real quantifier elimination is doubly exponential. *J. Symb. Comput.* 5, 1 (1988), 29 – 35.
- [12] Dolzmann, A., Sturm, T., and Weispfenning, V. A new approach for automatic theorem proving in real geometry. *J. Autom. Reason.* 21, 3 (Dec. 1998), 357380.
- [13] Dolzmann, A., and Gilch, L. A. Generic hermitian quantifier elimination. In *Artificial Intelligence and Symbolic Computation* (Berlin, Heidelberg, 2004), B. Buchberger and J. Campbell, Eds., Springer Berlin Heidelberg, pp. 80–93.
- [14] Eisenbud, D. *Commutative Algebra: With a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995.
- [15] Faugère, J.-C. FGb: A Library for Computing Gröbner Bases. In *Mathematical Software - ICMS 2010* (2010), vol. 6327 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, pp. 84–87.
- [16] Faugère, J.-C., Safey El Din, M., and Spaenlehauer, P.-J. On the complexity of the generalized minrank problem. *J. Symb. Comput.* 55 (2013), 30 – 58.
- [17] Grigor’ev, D. Y. Complexity of deciding Tarski algebra. *J. Symb. Comput.* 5, 12 (Feb. 1988), 65108.
- [18] Hermite, C. Sur le nombre des racines d’une équation algébrique comprises entre des limites données. extrait d’une lettre à m. borchardt. *J. Reine Angew. Math.* 52 (1856), 39–51.
- [19] Hong, H. An improvement of the projection operator in Cylindrical Algebraic Decomposition. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 1990), ISSAC ’90, Association for Computing Machinery, p. 261264.
- [20] Hong, H., and Safey El Din, M. Variant real quantifier elimination: Algorithm and application. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 2009), ISSAC ’09, Association for Computing Machinery, p. 183190.
- [21] Hong, H., and Safey El Din, M. Variant quantifier elimination. *J. Symb. Comput.* 47, 7 (2012), 883 – 901. *International Symposium on Symbolic and Algebraic Computation* (ISSAC 2009).
- [22] Le, H. P., and Safey El Din, M. Solving parametric systems of polynomial equations over the reals through Hermite matrices. Preprint, Nov. 2020.
- [23] Liska, R., and Steinberg, S. L. Applying Quantifier Elimination to Stability Analysis of Difference Schemes. *The Computer Journal* 36, 5 (01 1993), 497–503.
- [24] McCallum, S. An improved projection operation for Cylindrical Algebraic Decomposition of three-dimensional space. *J. Symb. Comput.* 5 (1988), 141 – 161.
- [25] McCallum, S. On projection in CAD-based quantifier elimination with equational constraint. In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 1999), ISSAC ’99, Association for Computing Machinery, p. 145149.
- [26] Nie, J., and Ranestad, K. Algebraic degree of polynomial optimization. *SIAM J. on Optimization* 20, 1 (Apr. 2009), 485502.
- [27] Pedersen, P., Roy, M.-F., and Szpirglas, A. Counting real zeros in the multivariate case. In *Computational Algebraic Geometry* (Boston, MA, 1993), F. Eyssette and A. Galligo, Eds., Birkhäuser Boston, pp. 203–224.
- [28] Renegar, J. On the computational complexity and geometry of the first-order theory of the reals. Part III: Quantifier elimination. *J. Symb. Comput.* 13, 3 (Mar. 1992), 329352.
- [29] Safey El Din, M. Real algebraic geometry library, RAGlib (version 3.4), 2017.
- [30] Safey El Din, M., and Schost, E. 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.* (NY, USA, 2003), ISSAC 03, ACM, p. 224231.
- [31] Safey El Din, M., and Schost, É. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM* 63, 6 (Jan. 2017), 48:1–48:37.
- [32] Seidenberg, A. A new decision method for elementary algebra. *Annals of Mathematics* 60, 2 (1954), 365–374.
- [33] Seidl, A., and Sturm, T. A generic projection operator for partial cylindrical algebraic decomposition. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 2003), ISSAC ’03, Association for Computing Machinery, p. 240247.
- [34] Shafarevich, I. R. *Basic Algebraic Geometry 1: Varieties in Projective Space*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
- [35] Spaenlehauer, P.-J. On the complexity of computing critical points with Gröbner bases. *SIAM Journal on Optimization* 24 (07 2014), 1382–1401.
- [36] Strzeboski, A. W. Cylindrical Algebraic Decomposition using validated numerics. *J. Symb. Comput.* 41, 9 (2006), 1021 – 1038.
- [37] Sturm, T., and Tiwari, A. Verification and synthesis using real quantifier elimination. In *Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 2011), ISSAC ’11, Association for Computing Machinery, p. 329336.
- [38] Sturm, T., and Weispfenning, V. Computational geometry problems in REDLOG. In *Selected Papers from the International Workshop on Automated Deduction in Geometry* (Berlin, Heidelberg, 1996), Springer-Verlag, p. 5886.
- [39] Tarski, A. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, 1951.
- [40] Weispfenning, V. The complexity of linear problems in fields. *J. Symb. Comput.* 5, 1 (1988), 3–27.

- [41] Weispfenning, V. Comprehensive gröbner bases. *Journal of Symbolic Computation* 14, 1 (1992), 1–29.
- [42] Weispfenning, V. A new approach to quantifier elimination for real algebra. In *Quantifier Elimination and Cylindrical Algebraic Decomposition* (Vienna, 1998), Springer Vienna, pp. 376–392.