A probabilistic algorithm to compute the real dimension of a semi-algebraic set

Mohab Safey El Din, Elias Tsigaridas

A probabilistic algorithm to compute the real dimension of a semi-algebraic set

Mohab Safey El Din
Université Pierre and Marie Curie and Institut Universitaire de France
INRIA Paris-Rocquencourt
Mohab.Safey@lip6.fr

Elias Tsigaridas
Université Pierre and Marie Curie and INRIA Paris-Rocquencourt
Elias.Tsigaridas@inria.fr

April 6, 2013

Abstract

Let R be a real closed field (e.g. the field of real numbers) and $\mathscr{S} \subset \mathsf{R}^n$ be a semi-algebraic set defined as the set of points in R^n satisfying a system of s equalities and inequalities of multivariate polynomials in n variables, of degree at most D, with coefficients in an ordered ring Z contained in R.

We consider the problem of computing the *real dimension*, d, of $\mathscr{S}$. The real dimension is the first topological invariant of interest; it measures the number of degrees of freedom available to move in the set. Thus, computing the real dimension is one of the most important and fundamental problems in computational real algebraic geometry.

The problem is $\mathrm{NP}_{\mathbb{R}}$-complete in the Blum-Shub-Smale model of computation. The current algorithms (probabilistic or deterministic) for computing the real dimension have complexity $(s\,D)^{O(d(n-d))}$, that becomes $(s\,D)^{O(n^2)}$ in the worst-case.

The existence of a probabilistic or deterministic algorithm for computing the real dimension with single exponential complexity with a factor better than $O(n^2)$ in the exponent in the worst-case, is a longstanding open problem.

We provide a positive answer to this problem by introducing a probabilistic algorithm for computing the real dimension of a semi-algebraic set with complexity $(s\,D)^{O(n)}$.

1 Introduction

A *semi-algebraic set* $\mathscr{S} \subset \mathsf{R}^n$, where R is a real closed field, is defined as the set of points in R^n satisfying a Boolean formula whose atoms are polynomial equalities and inequalities.

Computational real algebraic or semi-algebraic geometry is the study of effective algorithms for computing with semi-algebraic sets. Besides being a fascinating and important research area on its own, it is also one of the cornerstones of theoretical computer science.

Many important results rely on the foundations of real algebraic geometry. Let us mention non-linear computational geometry [20, 44, 45], the recent breakthroughs in combinatorial geometry on the discrete version of Kakeya problem [30, 34, 47], and the new algorithms for non-negative matrix factorization [1, 38] based on testing the emptiness of semi-algebraic sets. Last but not least, we emphasize the intrinsic connection between computational real algebraic geometry and game theory, especially stochastic games [17, 21, 31, 39, 48].

Typical computational challenges in real algebraic geometry are algorithms for deciding the emptiness and/or computing at least one point at each semi-algebraically connected component of a semi-algebraic set [11, 13, 26, 29, 41, 42], algorithms to perform geometric operations such as projection (this operation is tightly coupled with quantifier elimination) [11, 13, 28, 41], answering connectivity queries (roadmaps) [10, 20, 32], computing the real dimension of a semi-algebraic set [35, 36, 50] or computing more sophisticated topological information, such as the number of semi-algebraically connected components, the Euler-Poincaré characteristic, Betti numbers [8, 9, 12, 13].

Denote by s the number of polynomials involved in the description of a semi-algebraic set, by n the number of variables, and by D the maximum of the degrees of these polynomials. We can solve almost all the problems in computational real algebraic geometry using the generic approach of cylindrical algebraic decomposition [24] albeit in double exponential time, $(s\,D)^{2^{O(n)}}$. Even though huge effort has been invested the last 25 years to derive algorithms with single exponential complexity w.r.t. the number of variables, there are problems that are still missing an algorithm with such a complexity bound. Moreover, even in the case where the complexity is single exponential, the exponent is not always $O(n)$.

Let us emphasize that improving the exponents in the complexity bounds of algorithms in computational real algebraic geometry is not only a theoretical challenge. It introduces new algebraic and geometric techniques that find applications in more general domains, and eventually leads to efficient implementations for real-world problems. For instance, the first improvement of the long-standing $O(n^2)$ exponent in the complexity bound of Canny's probabilistic algorithm [20] to $O(n^{3/2})$ is based on a new geometric connectivity result that introduced the use of a baby steps giant steps algorithmic technique in this problem [43].

On the other hand, the problem of computing the real dimension lacks, up to now, an algorithm with single exponential complexity and exponent $O(n)$.

Problem statement and state-of-the-art. In this paper we address the problem of computing the real dimension of a semi-algebraic set. The following definition is in order:

Definition 1. [13, Section 5.3] *Let $\mathscr{S}$ be a semi-algebraic-set of R^n, where R is a real closed field. The* **real dimension** *of S is the largest integer d such that there exists an injective semi-algebraic map from $(0,1)^d$ to $\mathscr{S}$. By definition the dimension of the empty set is -1.*

The best known complexity bound, in the worst case, for computing the real dimension of a semi-algebraic set is due to Koiran and it is $(s\,D)^{O(n^2)}$ [36], where s is the number of polynomials used to

describe the semi-algebraic set. It is based on quantifier elimination techniques, see [13, Alg. 14.10] and references therein. A partial improvement of the $O(n^2)$ in the exponent is due to Vorobjov [50]. He presented an algorithm with complexity $(s\,D)^{O(d(n-d))}$, where d is the real dimension. This bound is output sensitive, and when d is a constant, then it becomes $(sD)^{O(n)}$. Basu, Pollack, and Roy [14] slightly improved the result of Vorobjov, based on [22]. They presented a complexity bound that depends on whether $d \geq n/2$ or $d < n/2$. This result has a better dependence on the number of polynomials, s, than the one of Vorobjov [50].

On the other hand, it is well understood that we can compute the (Krull) dimension of an algebraic variety over algebraically closed fields in time $D^{O(n)}$ [23, 26], see also [35]. In the algebraically closed field case, we can consider a sufficiently generic, random, collection of d hyperplanes, for $1 \leq d \leq n$, and check whether their intersection with the algebraic set under consideration is finite. The largest d where this is achieved imposes that the Krull dimension of the algebraic set is d. However, when we are interested in computing the real dimension of a real algebraic, or semi-algebraic set, this strategy is not applicable.

It is of great interest to know if the problem of computing the dimension admits the same complexity bound in the real case and in the algebraically closed case. Quoting Koiran [36] *"The main open problem is whether* $\mathsf{DIM}_{\mathbb{R}}$ *[the real dimension] can be solved in time* $(s\,D)^{O(n)}$*"*. Vorobjov [50] also mentions that *"For a real variety V existence of a probabilistic dimension algorithm with complexity bound* $(s\,D)^{O(n)}$ *is an open problem"*.

The purpose of the present work is to provide a positive answer to this open problem.

Besides the intrinsic mathematical interest for an improved algorithm for computing the real dimension, improvement of the complexity bound has important consequences. Some algorithms in computational real algebraic geometry consider the real dimension of a semi-algebraic set as part of their input, e.g. [13, Theorem. 13.37]. Let us also mention the recent bounds in [6, 7] on the number of semi-algebraically connected components of a semi-algebraic set that depend on the real dimension of some real algebraic set. Moreover, effective algorithms for computing the real dimension are needed to estimate efficiently the degrees of freedom in robotic mechanisms (see e.g. [33, 40]).

The problem is also very important from the complexity theory point of view, as Koiran [36] proved that it is $\mathrm{NP}_{\mathbb{R}}$-complete in the Blum-Shub-Smale computation model [16].

Our results. We present an efficient algorithm for computing the real dimension of a semi-algebraic set.

Our algorithm reduces the unbounded case to the bounded one, using a standard technique of computational real algebraic geometry introduced in [11].

Previous approaches for computing the real dimension of a semi-algebraic set $\mathscr{S}$ rely on finding the largest integer d for which there exists a d-dimensional linear subspace, such that the projection of $\mathscr{S}$ on this subspace has dimension d. To do so they use quantifier elimination. Therefore, the exponent in the complexity is the dimension, d, multiplied by the number of quantified variables, $n-d$.

The algorithm that we present, instead of projecting the semi-algebraic set under consideration, exploits geometric properties of fundamental objects of algebraic geometry, that is *polar varieties*. Roughly speaking, polar varieties are the critical loci of projections, e.g. [3, 4, 5] and references therein. More precisely, we are able to prove the following: Let V be algebraic set defined by the polynomial equalities of the input and U the open semi-algebraic set defined by the polynomial

inequalities of the input. Then, up to a generic change of coordinates, d is the largest integer such that $\mathscr{S}$ is equal to the intersection of U and the limit of the critical locus of the $d+1$ polar variety V, after we perturbed it symbolically. This way the computation of the real dimension reduces to finding the largest integer d with this property.

The algorithm is probabilistic since we perform a random linear change of coordinates in the beginning. If we work over the integers, then we denote by τ the maximum bit size of the coefficients *after* the linear change of coordinates.

Our main result is encapsulated in the following theorem:

Theorem 1. *Let $F = (f_1, \ldots, f_p) \in \mathsf{Z}[X_1, \ldots, X_n]^p$, $G = (g_1, \ldots, g_s) \in \mathsf{Z}[X_1, \ldots, X_n]^s$, where the degree of each f_i, resp. g_j, is at most D. There exists a probabilistic algorithm for computing the real dimension of the semi-algebraic set defined by*

$$f_1 = \cdots = f_p = 0, \quad g_1 > 0, \ldots, g_s > 0 \ ,$$

in $(s\,D)^{O(n)}$ operations in Z.

If $\mathsf{Z} = \mathbb{Z}$, then the Boolean complexity of the algorithm $\tau\,(s\,D)^{O(n)}$.

To the best of our knowledge this is the first algorithm for computing the real dimension of a real algebraic or semi-algebraic set within this complexity bound.

Organization of the paper. The rest of the paper is structured as follows: In the next Section we present the necessary preliminaries from real algebraic geometry. In Section 3 we present the genericity properties that the semi-algebraic set under consideration should satisfy. We prove that a semi-algebraic set can satisfy these properties if we apply a random linear change of coordinates. Section 4 presents the geometric result that is the crux of the matter of our algorithm. Finally, in Section 5 we present the algorithm ComputeRealDimension for computing the real dimension, its various subroutines, the proof of correctness and the complexity analysis.

2 Preliminaries

In this section, we introduce some basic notions and some notations that are used throughout the paper.

As sketched in the introduction we will introduce some infinitesimals to deform real algebraic sets. This will lead us to consider various ground fields and semi-algebraic sets defined over these fields. We refer the reader to [13, Chapter 2] for a more detailed exposition of these notions on real fields, real closed fields, infinitesimals and semi-algebraic sets. We will also use basic notions coming from algebraic geometry since we will use the knowledge of the dimension of some algebraic sets to deduce the real dimension of semi-algebraic sets under study. For a more detailed exposition of these notions, we refer the reader to [46, Chapter 1]. The section finishes with some notions on critical points and polar varieties that are extensively used in the sequel.

Ground fields. Let Q be a real field, R be a real closed field and C be the algebraic closure of R. We consider a field $\mathbb{K}$ containing Q (e.g. R or C) and let ε be an infinitesimal. In the sequel, $\mathbb{K}\langle\varepsilon\rangle$ stands for the Puiseux series field. We say that $z = \sum_{i \geq i_0} a_i \varepsilon^{i/q} \in \mathbb{K}\langle\varepsilon\rangle$ is *bounded over* $\mathbb{K}$ if and only if $i_0 \geq 0$. We say that $\mathbf{z} = (z_1, \ldots, z_n) \in \mathbb{K}\langle\varepsilon\rangle^n$ is *bounded over* $\mathbb{K}$ if each z_i is bounded

over $\mathbb{K}$. Given a bounded element $z \in \mathbb{K}\langle\varepsilon\rangle$, we denote by $\lim_{\varepsilon\to 0} z$ the number $a_0 \in \mathbb{K}$. Given a bounded element $\mathbf{z} \in \mathbb{K}\langle\varepsilon\rangle^n$, we denote by $\lim_{\varepsilon\to 0}\mathbf{z}$ the point $(\lim_{\varepsilon\to 0}(z_1), \ldots, \lim_{\varepsilon\to 0}(z_n)) \in \mathbb{K}^n$. Given a subset $A \subset \mathbb{K}\langle\varepsilon\rangle^n$, we denote by $\lim_{\varepsilon\to 0}(A)$ the set $\{\lim_{\varepsilon\to 0}(z) \mid z \in A \text{ and } z \text{ is bounded}\}$. Given a semi-algebraic (resp. constructible) set $A \subset \mathsf{R}^n$ (resp. $A \subset \mathsf{C}^n$) defined by a quantifier-free formula Φ with polynomials in $\mathsf{R}[X_1, \ldots, X_n]$, we denote by $\mathrm{ext}(A, \mathsf{R}\langle\varepsilon\rangle)$ (resp. $\mathrm{ext}(A, \mathsf{C}\langle\varepsilon\rangle)$) the set of solutions of Φ in $\mathsf{R}\langle\varepsilon\rangle^n$ (resp. $\mathsf{C}\langle\varepsilon\rangle^n$).

In the sequel, we will work with n-variate polynomials with coefficients in Q, $\mathsf{Q}[\zeta]$ and $\mathsf{Q}[\varepsilon, \zeta]$ or ε and ζ are infinitesimals with $0 < \varepsilon < \zeta$. Sign conditions on finite families of polynomials with coefficients in Q define semi-algebraic sets in R^n, those with coefficients in $\mathsf{Q}[\zeta]$ (resp. $\mathsf{Q}[\varepsilon, \zeta]$) define semi-algebraic sets in $\mathsf{R}\langle\zeta\rangle^n$ (resp. $\mathsf{R}\langle\zeta\rangle\langle\varepsilon\rangle^n$).

Basic definitions on algebraic sets. Let $\bar{\mathbb{K}}$ stand for an algebraic closure of $\mathbb{K}$. We consider *algebraic sets* in $\bar{\mathbb{K}}^n$ defined by polynomial equations with coefficients in $\mathbb{K}$. A Zariski open set is a set whose complementary is an algebraic set. A *constructible set* in $\bar{\mathbb{K}}^n$ is the set of common solutions of a system of a finite number of n-variate polynomial equations and inequalities with coefficients in $\mathbb{K}$.

Let $V \subset \bar{\mathbb{K}}^n$ be an algebraic set defined by polynomial equations in $\mathbb{K}[X_1, \ldots, X_n]$.

We will consider the dimension of V, referring to its *Krull dimension* (see e.g. [25]). This notion of dimension coincides with other notions coming from differential or algebraic geometry (see e.g. [25, Part II]). Roughly speaking, it is the number of *generic* hyperplanes such that their intersection with V is a finite set of points. The Krull dimension of a constructible set is the Krull dimension of its Zariski closure. If W is another algebraic set and $V \subset W$, then the Krull dimension of V is less than or equal to the Krull dimension of W.

The algebraic set V is said to be irreducible if it cannot be decomposed as the union of two algebraic sets defined by polynomial equations with coefficients in $\mathbb{K}$. If V is not irreducible it can be uniquely decomposed as a finite union of irreducible algebraic sets; these sets are called the irreducible components of V.

When all the irreducible components of V have the same Krull dimension, we say that V is *equidimensional*. The ideal associated to V is the set of polynomials with coefficients in $\mathbb{K}$ which vanish on V. There exists a finite family of polynomials which generate it in $\mathbb{K}[X_1, \ldots, X_n]$; let us denote it by $f_1, \ldots, f_p$.

Assume that V is equidimensional of Krull dimension d. A point $\mathbf{x} \in V$ is called *regular* (or *smooth*) if the Jacobian matrix

$$\begin{bmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial f_p}{\partial X_1} & \cdots & \frac{\partial f_p}{\partial X_n} \end{bmatrix}$$

has rank $n - d$ at $\mathbf{x}$. The kernel of the above Jacobian matrix at $\mathbf{x}$ is the tangent space to V at $\mathbf{x}$; we denote it by $T_{\mathbf{x}}V$. Points in V that are not regular are said to be *singular*. An algebraic set with no singular points is smooth.

Semi-algebraic sets and algebraic sets. Let C be the algebraic closure of R, and $S \subset \mathsf{R}^n$ be a semi-algebraic set. The smallest algebraic set containing $\mathcal{S}$ is called the Zariski closure of S. It is well-known that the Krull dimension of the Zariski closure of S equals the real dimension of S

(see e.g. [19, Proposition 2.8.2]). In particular if W is an algebraic set that contains S, one can conclude that the real dimension of S is less than or equal to the Krull dimension of W.

Let $S \subset \mathsf{R}^n$ and $S' \subset \mathsf{R}^n$. Consider a semi-algebraic map $\varphi : S \to S'$ and R' be a real closed field containing R. We will consider the extension of φ to R', denoted by $\mathrm{ext}(\varphi, \mathsf{R}')$, as the semi-algebraic function $\mathrm{ext}(S, \mathsf{R}') \to \mathrm{ext}(S', \mathsf{R}')$ whose graph is the extension of the graph of φ to S'.

If $S \subset S'$, then by Definition 1 the real dimension of S is less than or equal to the real dimension of S'.

If $\mathbf{x} \in S$, we say that $\mathbf{x}$ is a *smooth point* of S if it is smooth in the Zariski closure of S; a semi-algebraic set is said to be smooth if it is contained in the set of regular points of its Zariski closure (this is direct a consequence of [19, Definition 3.3.4]).

We also consider canonical projections $\pi_i : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_i)$.

Change of variables. Let $\mathbb{K}$ be a field containing Q and $\bar{\mathbb{K}}$ be its algebraic closure. Consider $f \in \mathbb{K}[X_1, \ldots, X_n]$ and $V \subset \bar{\mathbb{K}}^n$ be the set of roots of f in $\bar{\mathbb{K}}$ and $\mathbf{A} \in \mathrm{GL}_n(\mathsf{Q})$. We denote by $f^{\mathbf{A}}$ the polynomial $f(\mathbf{AX})$ and by $V^{\mathbf{A}} \subset \bar{\mathbb{K}}^n$. In other words, $V^{\mathbf{A}}$ is the image of V by the map $\mathbf{x} \to \mathbf{A}^{-1}\mathbf{x}$.

Similarly, we will also consider change of variables on semi-algebraic sets. If S is a semi-algebraic set in R^n and $\mathbf{A} \in \mathrm{GL}_n(\mathsf{Q})$, then $S^{\mathbf{A}}$ denotes the image of S by the map $\mathbf{x} \to \mathbf{A}^{-1}\mathbf{x}$.

Critical points and polar varieties. Let $f_1, \ldots, f_p$ be polynomials in $\mathbb{K}[X_1, \ldots, X_n]$ and $V \subset \mathsf{C}^n$ be the algebraic set defined by $f_1 = \cdots = f_p = 0$. For $1 \leq i \leq n-p$, we define the *polar variety* $\mathrm{crit}(\pi_i, V)$ as the set of points in V at which all p-minors of the truncated Jacobian matrix

$$\begin{bmatrix} \frac{\partial f_1}{\partial X_{i+1}} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial f_p}{\partial X_{i+1}} & \cdots & \frac{\partial f_p}{\partial X_n} \end{bmatrix}$$

vanish. By convention for $i \geq n-p+1$, we set $\mathrm{crit}(\pi_i, V) = V$ and for $i = 0$ we set $\mathrm{crit}(\pi_i, V) = \emptyset$.

We refer to [5] for a detailed study of polar varieties. Below, we recall some basic results that are used in the paper.

Given a polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$ and $V \subset \bar{\mathbb{K}}^n$ defined by $f = 0$, we denote by $\mathrm{crit}(\pi_i, V) \subset \bar{\mathbb{K}}^n$ defined by

$$f = \frac{\partial f}{\partial X_{i+1}} = \cdots = \frac{\partial f}{\partial X_n} = 0 \ .$$

Assuming f is square-free, the set of singular points of V is defined by the vanishing of F and all its partial derivatives. The set $\mathrm{crit}(\pi_i, V)$ is called *polar variety associated to* π_i. When V is smooth, $\mathrm{crit}(\pi_i, V)$ is the set of *critical points* of the restriction of π_i to V (i.e. the set of regular points $\mathbf{x} \in V$ such that $\pi_i(T_{\mathbf{x}}V)$ has dimension $\leq i-1$). When V is not smooth $\mathrm{crit}(\pi_i, V)$ is the union of the singular points of V and the critical points of the restriction of π_i to V.

Let us also mention that for $i = 1$, $\mathrm{crit}(\pi_1, V)$ contains the local minimizers and maximizers of the restriction of π_1 to $V \cap \mathsf{R}^n$.

3 Genericity properties

In this paper, a property is called generic (in some suitable parameter space) if it holds in a non-empty Zariski open subset of the parameter space under consideration.

Definition 2. *Let $f \in \mathsf{Q}(\zeta)[X_1, \ldots, X_n]$, $V \subset \mathsf{C}\langle\zeta\rangle^n$ be the algebraic variety defined by $f = 0$, and $V_\varepsilon \subset \mathsf{C}\langle\zeta\rangle\langle\varepsilon\rangle^n$ be the algebraic variety defined by $f - \varepsilon = 0$. We say that f satisfies property N if the following conditions hold:*

N_1 *for all $1 \leq i \leq n$, $\mathrm{crit}(\pi_i, V_\varepsilon)$ is either empty or is smooth and equidimensional of Krull dimension $i-1$;*

N_2 *for all $\mathbf{x} \in V \cap \mathsf{R}\langle\zeta\rangle^n$, $\pi_d^{-1}(\pi_d(\mathbf{x})) \cap (V \cap \mathsf{R}\langle\zeta\rangle^n)$ is finite where d is larger than or equal to the real dimension of V at $\mathbf{x}$.*

Note that in the above definition, we consider a polynomial with coefficients in $\mathsf{Q}(\zeta)$. We state below that for a generic choice of an $n \times n$ invertible matrix $\mathbf{A}$ with entries in Q, $f^{\mathbf{A}}$ satisfies N.

Indeed we need such a statement because our algorithm performs symbolic manipulations on the input by introducing an infinitesimal ζ (to reduce the study to bounded semi-algebraic sets) and next chooses randomly $\mathbf{A}$ to ensure that after applying the change of variables $\mathbf{x} \to \mathbf{A}^{-1}\mathbf{x}$ some polynomial satisfies N.

Thus, the rest of this Section is devoted to prove that up to a generic choice of $\mathbf{A} \in \mathrm{GL}_n(\mathsf{Q})$, $f^{\mathbf{A}}$ satisfies N.

Proposition 2. *There exists a non-empty Zariski open set $\mathscr{O} \subset \mathrm{GL}_n(\mathsf{C})$ such that for $\mathbf{A} \in \mathscr{O} \cap \mathrm{GL}_n(\mathsf{Q})$, $f^{\mathbf{A}}$ satisfies N.*

Proof. We will prove that there exists a non-empty Zariski open set $\mathscr{O}' \subset \mathrm{GL}_n(\mathsf{C})$ (resp. $\mathscr{O}'' \subset \mathrm{GL}_n(\mathsf{C})$) such that for $\mathbf{A} \in \mathscr{O}' \cap \mathrm{GL}_n(\mathsf{Q})$, $f^{\mathbf{A}}$ satisfies N_1 (resp. N_2). Taking $\mathscr{O} = \mathscr{O}' \cap \mathscr{O}''$ is sufficient to conclude.

We start with N_1. [3, Proposition 3] (see also [5, Theorem 6] for a more general statement) states that when f has coefficients in Q and defines a smooth algebraic set $V \subset \mathsf{C}^n$, there exists a non-empty Zariski open set $\Omega' \subset \mathrm{GL}_n(\mathsf{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathsf{Q}) \cap \Omega'$ and $1 \leq i \leq n$, $\mathrm{crit}(\pi_i, V^{\mathbf{A}})$ is either empty or is equidimensional of Krull dimension $i-1$. The proof of this result is based on the use of the Weak Transversality Theorem of Thom-Sard (see e.g. [27]). It allows to characterize the set of "bad" matrices, i.e. the complement of Ω' in $\mathrm{GL}_n(\mathsf{C})$ as the smallest algebraic set containing the critical values of a polynomial mapping with coefficients in the same base field as the one containing the coefficients of f.

By [42, Lemma 3.5], V_ε is smooth. Thus, one can apply *mutatis mutandis* the proof of [3, Proposition 3] to $f - \varepsilon$ with $\mathsf{C}\langle\zeta\rangle\langle\varepsilon\rangle$ as a base field. We obtain the existence of a non-empty Zariski open set $\Omega' \subset \mathrm{GL}_n(\mathsf{C}\langle\zeta\rangle\langle\varepsilon\rangle)$ such that for $\mathbf{A} \in \Omega'$ and $1 \leq i \leq n$, $\mathrm{crit}(\pi_i, V_\varepsilon^{\mathbf{A}})$ is either empty or is equidimensional of Krull dimension $i-1$. Recall that $\mathrm{GL}_n(\mathsf{C}\langle\zeta\rangle\langle\varepsilon\rangle) - \Omega'$ is Zariski closed and is characterized as the set of critical values of a polynomial mapping in $\mathsf{Q}(\varepsilon, \zeta)$ since $f - \varepsilon$ has coefficients in $\mathsf{Q}(\varepsilon, \zeta)$. If we multiply this polynomial by the least common multiple of the denominators of its coefficients, we obtain a polynomial P with coefficients in $\mathsf{Q}[\varepsilon, \zeta]$. Without loss of generality, we can assume that the coefficients of P have no non-trivial gcd. Hence, P can be written as

$$P = P_0 + \varepsilon^{v_\varepsilon} Q_\varepsilon + \zeta^{v_\zeta} Q_\zeta + \varepsilon\zeta Q \ ,$$

where v_ε and v_ζ are positive integers and

- P_0 has coefficients in Q (it is obtained by substituting ε and ζ by 0 in P);
- Q_ε (resp. Q_ζ) has coefficients in $\mathsf{Q}[\varepsilon]$ (resp. $\mathsf{Q}[\zeta]$) and is not identically 0 when ε (resp. ζ) is substituted to 0;
- Q has coefficients in $\mathsf{Q}[\varepsilon, \zeta]$.

Note that since the coefficients of P have no non-trivial gcd, at least one of the three polynomials P_0, Q_ε and Q_ζ are not identically 0. If $P_0 \neq 0$ (resp. $Q_\varepsilon \neq 0$ or $Q_\zeta \neq 0$), we define $\mathscr{O}' \subset \mathrm{GL}_n(\mathsf{C})$ as the non-empty Zariski defined by $P_0 \neq 0$ (resp. $Q_\varepsilon \neq 0$ or $Q_\zeta \neq 0$).

Now remark that since ε and ζ are infinitesimals, for all $\mathscr{O}' \cap \mathrm{GL}_n(\mathsf{Q}) \subset \Omega'$; in other words for all $\mathbf{A} \in \mathscr{O}' \cap \mathrm{GL}_n(\mathsf{Q})$, $f^{\mathbf{A}}$ satisfies N_1 as requested.

Now we deal with N_2. Below, by abuse of notations the extensions of cartesian products $]0,1[^i$ in $\mathsf{R}\langle\zeta\rangle$ are denoted by $]0,1[$; also by convention $]0,1[^0 = \{0\}$. The set $V \bigcap \mathsf{R}\langle\zeta\rangle^n$ is semi-algebraic and so we can partition it into smooth semi-algebraic sets $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ [13, Chapter 5, Section 5], and homeomorphic to $]0,1[^{d_1}, \ldots,]0,1[^{d_\ell}$, respectively, where $0 \leq k \leq n$. By [18, pp. 47], for $\mathbf{x} \in V \bigcap \mathsf{R}\langle\zeta\rangle^n$, the local real dimension of $V \bigcap \mathsf{R}\langle\zeta\rangle^n$ at $\mathbf{x}$ is given by $\max_{\mathbf{x} \in \overline{\mathcal{S}_i}} d_i$, where $\overline{\mathcal{S}_i}$ denotes the Euclidean closure of $\mathcal{S}_i$.

For $1 \leq i \leq \ell$, we denote by V_i the Zariski closure of $\mathcal{S}_i$. By [19, Proposition 2.8.2] note that the Krull dimension of V_i is d_i, for $1 \leq i \leq \ell$. By Noether normalization [2], there exists a non-empty Zariski open set $\Omega_i'' \subset \mathrm{GL}_n(\mathsf{C}\langle\zeta\rangle\langle\varepsilon\rangle)$ such that for all $\mathbf{A} \in \Omega_i''$ and $\mathbf{x} \in \mathsf{C}\langle\zeta\rangle^{d_i}$, $\pi_{d_i}^{-1}(\mathbf{x}) \cap V_i^{\mathbf{A}}$ is finite. As a consequence, for all $\mathbf{x} \in \mathsf{R}\langle\zeta\rangle^{d_i}$, $\pi_{d_i}^{-1}(\mathbf{x}) \cap \mathcal{S}_i$ is finite. We let $\Omega'' = \bigcap_{i=1}^{\ell} \Omega_i''$. The complement of Ω'' in $\mathrm{GL}_n(\mathsf{C}\langle\zeta\rangle\langle\varepsilon\rangle)$ can be characterized using algebraic elimination algorithms (such as Gröbner bases) run with parameters as for entries of a generic matrix; we refer to [37] for such algebraic algorithms for detecting defects of Noether normalization. As above, since the input has coefficients in $\mathsf{Q}(\zeta)$, Ω'' can be defined by a polynomial inequality $P \neq 0$ with coefficients in $\mathsf{Q}[\varepsilon, \zeta]$: Following *mutatis mutandis* the approach for proving N_1, one can deduce from the inequality $P \neq 0$ another inequality with coefficients in Q defining a non-empty Zariski open set $\mathscr{O}''$ such that $\mathscr{O}'' \cap \mathrm{GL}_n(\mathsf{Q}) \subset \Omega''$. This finishes the proof. □

4 Geometric Statement

In this Section we let f and $g_1, \ldots, g_s$ be polynomials in $\mathsf{Z}[X_1, \ldots, X_n]$, $S \subset \mathsf{R}^n$ be the semi-algebraic set defined by

$$f = 0, \quad g_1 > 0, \ldots, g_s > 0$$

and $U \subset \mathsf{R}^n$ be the open semi-algebraic set defined by $g_1 > 0, \ldots, g_s > 0$. We will also consider the algebraic set $V \subset \mathsf{C}^n$ defined by $f = 0$. Given an infinitesimal ε, we denote by $V_\varepsilon \subset \mathsf{C}\langle\varepsilon\rangle^n$ the algebraic set defined by $f = \varepsilon$.

The rest of this Section is devoted to prove this result below.

Proposition 3. *Assume that f satisfies N, is non-negative over R^n, and that $V \cap \mathsf{R}^n$ is bounded. Then for $0 \leq i \leq n$, $(\lim_{\varepsilon \to 0} \mathrm{crit}(\pi_i, V_\varepsilon)) \bigcap U = S$ if and only if the real dimension of S is $\leq i - 1$.*

Remark 4. *[6, Proposition 3.4] provides a similar statement but with different assumptions on f that are not suitable for our setting.*

Before proving the above result, we start with a few lemmata.

4.1 Auxiliary results

The following proposition is a variant of statements that are commonly used in computational real algebraic geometry (see e.g. [15, 42] or [13, Proposition 12.38]).

We let ζ be an infinitesimal.

Proposition 5. *Assume that f is non-negative over R^n and that $V \cap \mathsf{R}^n$ is non-empty. Let C be a semi-algebraically connected component of $V \cap \mathsf{R}^n$. Then there exist semi-algebraically connected components $C_{\varepsilon,1}, \ldots, C_{\varepsilon,\ell}$ of $V_\varepsilon \bigcap \mathsf{R}\langle\varepsilon\rangle^n$, such that $C = \bigcup_{i=1}^{\ell} \lim_{\varepsilon\to 0} C_{\varepsilon,i}$.*

Moreover if there exists a ball $B \subset \mathsf{R}^n$ such that $C \subset B$ and C does not intersect the boundary of B, then $C_{\varepsilon,i} \subset \mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$ and $C_{\varepsilon,i}$ does not intersect the boundary of $\mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$, for $1 \leq i \leq \ell$.

Proof. Consider $\mathbf{x} \in C$. By assumption, f is non-negative over R^n. Since $f(\mathbf{x}) = 0$ there exists a semi-algebraically connected component $\mathcal{S} \subset \mathsf{R}^n$ of the semi-algebraic set defined by $f > 0$ such that $\mathbf{x}$ is in the closure of $\mathcal{S}$ (for the Euclidean topology). Then, for all $r > 0$ the ball $B(\mathbf{x}, r)$ centered at $\mathbf{x}$ of radius r contains a point of $\mathcal{S}$ (at which f is positive). By the curve selection Lemma [13, Theorem 3.19] there exists a continuous semi-algebraic function $\gamma : [0,1] \to \mathcal{S}$ with $\gamma(0) = \mathbf{x}$ and $f(\gamma(t)) > 0$ for $t \neq 0$.

Consider the extensions $\tilde{\gamma} = \mathrm{ext}(\gamma, \mathsf{R}\langle\varepsilon\rangle)$ and $\tilde{f} = \mathrm{ext}(f, \mathsf{R}\langle\varepsilon\rangle)$. By the semi-algebraic intermediate value Theorem [13, Theorem 2.11], there exists $t_\varepsilon \in \mathrm{ext}([0,1], \mathsf{R}\langle\varepsilon\rangle)$ such that $\tilde{f}(\tilde{\gamma}(t_\varepsilon)) = \varepsilon$. We denote $\tilde{\gamma}(t_\varepsilon)$ by $\mathbf{x}_\varepsilon$ and we have $\lim_{\varepsilon\to 0} \mathbf{x}_\varepsilon = \mathbf{x}$ because $\mathbf{x}_\varepsilon \in \mathrm{ext}(B(\mathbf{x}, r), \mathsf{R}\langle\varepsilon\rangle)$ for all $r > 0$. Also, let $C_{\mathbf{x}_\varepsilon}$ be the semi-algebraically connected component of $V_\varepsilon \cap \mathsf{R}\langle\varepsilon\rangle^n$ that contains $\mathbf{x}_\varepsilon$; we associate to $\mathbf{x}$ this semi-algebraically connected component $C_{\mathbf{x}_\varepsilon}$ of $V_\varepsilon \cap \mathsf{R}\langle\varepsilon\rangle^n$.

Since there are finitely many semi-algebraically connected components of $V_\varepsilon \cap \mathsf{R}\langle\varepsilon\rangle^n$, there are finitely many semi-algebraically connected components of $C_{\varepsilon,1}, \ldots, C_{\varepsilon,\ell}$ which are associated to a point $\mathbf{x}$ in C. This proves that $C \subset \bigcup_{i=1}^{\ell} \lim_{\varepsilon\to 0} C_{\varepsilon,i}$.

We prove now that $\bigcup_{i=1}^{\ell} \lim_{\varepsilon\to 0} C_{\varepsilon,i} \subset C$. Let $\mathbf{x} \in \lim_{\varepsilon\to 0} C_{\varepsilon,i}$ for some $1 \leq i \leq \ell$; we need to prove that $\mathbf{x} \in C$. Then, there exists $\mathbf{x}_\varepsilon \in C_{\varepsilon,i}$ bounded over R such that $\lim_{\varepsilon\to 0} \mathbf{x}_\varepsilon = \mathbf{x}$. Now, recall that $C_{\varepsilon,i}$ is associated to some point $\mathbf{x}' \in C$; this means that there exists $\mathbf{x}'_\varepsilon \in C_{\varepsilon,i}$ bounded over R such that $\lim_{\varepsilon\to 0} \mathbf{x}'_\varepsilon = \mathbf{x}'$. Since $C_{i,\varepsilon}$ is semi-algebraically connected, there exists a continuous semi-algebraic function $\gamma : [0,1] \to C_{i,\varepsilon}$ such that $\gamma(0) = \mathbf{x}_\varepsilon$ and $\gamma(1) = \mathbf{x}'_\varepsilon$; we have that $\Gamma = \gamma([0,1])$ is a semi-algebraically connected semi-algebraic set. By [13, Theorem 3.20], $\Gamma = \gamma([0,1])$ is closed and bounded. By [13, Proposition 12.36], we conclude that $\lim_{\varepsilon\to 0} \Gamma$ is semi-algebraically connected. Since $\lim_{\varepsilon\to 0}$ is a ring homomorphism, $\lim_{\varepsilon\to 0} \Gamma$ is contained in $V \cap \mathsf{R}^n$. Now notice that $\lim_{\varepsilon\to 0}(\gamma(0)) = \mathbf{x}$ and that $\lim_{\varepsilon\to 0}(\gamma(1)) = \mathbf{x}'$. Since we have proved that $\lim_{\varepsilon\to 0} \Gamma$ is semi-algebraically connected we deduce that $\mathbf{x} \in C$ as requested.

Now, we assume that C is bounded and let $B \subset \mathsf{R}^n$ be a ball such that $C \subset B$ and C does not intersect the boundary of B. To conclude the proof it remains to prove that for $1 \leq i \leq \ell$, $C_{\varepsilon,i} \subset \mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$ and $C_{\varepsilon,i}$ does not intersect the boundary of $\mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$.

Consider $\mathbf{x}_\varepsilon \in C_{\varepsilon,i}$ bounded over R such that $\lim_{\varepsilon\to 0} \mathbf{x}_\varepsilon \in C$. Such a point exists, as we argued in the first part of the proof that $\lim_{\varepsilon\to 0} C_{\varepsilon,i} \subset C$.

We argue by contradiction. Assume that there exists $\mathbf{x}'_\varepsilon$ in the Euclidean closure of $C_{\varepsilon,i} - \mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$. Since $C_{\varepsilon,i}$ is semi-algebraically connected, there exists a continuous semi-algebraic function $\gamma : [0,1] \to C_{\varepsilon,i}$ such that $\gamma(0) = \mathbf{x}_\varepsilon$ and $\gamma(1) = \mathbf{x}'_\varepsilon$. Note that by the intermediate value theorem [13, Theorem 2.11] (applied to the polynomial defining the boundary of B) there exists $\vartheta \in [0,1]$ such that $\gamma(\vartheta)$ lies in the boundary of $\mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$. We deduce that $\lim_{\varepsilon\to 0} \gamma(\vartheta)$ belongs to the boundary of B.

By [13, Theorem 3.20], $\gamma([0,1])$ is closed and bounded. We also notice that $\gamma([0,1])$ is semi-algebraically connected. By [13, Proposition 12.36], we conclude that $\lim_{\varepsilon\to 0}\gamma([0,1])$ is semi-algebraically connected. We deduce that $\lim_{\varepsilon\to 0}(\gamma([0,1])) \subset C$. We deduce that $\lim_{\varepsilon\to 0}\gamma(\vartheta)$ belongs to C.

Consequently, we have $\lim_{\varepsilon\to 0}\gamma(\vartheta)$ belongs to C and to the boundary of B. This contradicts the fact that, by assumption, C does not intersect the boundary of B. Thus, we conclude that $C_{\varepsilon,i} \subset \mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$ and $C_{\varepsilon,i}$ does not intersect the boundary of $\mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$. □

The following lemma relates the real dimension of a semi-algebraic set in $\mathsf{R}\langle\varepsilon\rangle^n$ with the real dimension of its image by $\lim_{\varepsilon\to 0}$. Its proof uses quite standard tools from real algebraic geometry.

Lemma 6. *Let $\mathcal{S}_\varepsilon \subset \mathsf{R}\langle\varepsilon\rangle^n$ (resp. $\mathcal{Z}_\varepsilon \subset \mathsf{C}\langle\varepsilon\rangle^n$) be a semi-algebraic (resp. constructible) set and d be its real (resp. Krull) dimension. Then $\lim_{\varepsilon\to 0}\mathcal{S}_\varepsilon$ (resp. $\lim_{\varepsilon\to 0}\mathcal{Z}_\varepsilon$) has real (resp. Krull) dimension less or equal to d.*

Proof. The proof of this statement relies on [13, Proposition 5.29] which states that if A is a semi-algebraic subset of R^m and $h : A \to \mathsf{R}^n$ is a semi-algebraic mapping, then the real dimension of $h(A)$ is less than or equal to the real dimension of A. Thus, it suffices to prove that the ring homomorphism $\lim_{\varepsilon\to 0}$ is a semi-algebraic function, i.e. a function whose graph is a semi-algebraic function. This is a quite routine statement in real algebraic geometry; we give the proof since we could not find a reference stating it explicitly. To do that, we reuse some ingredients of [13, Proposition 12.36].

Recall that by assumption $\mathcal{S}_\varepsilon$ is a semi-algebraic set of $\mathsf{R}\langle\varepsilon\rangle^n$ and that, by definition $\mathsf{R}\langle\varepsilon\rangle$ is the real closure of $\mathsf{R}(\varepsilon)$. Then, by [13, Proposition 2.82], there exists a quantifier-free Boolean formula of conjunctions and disjunctions of polynomials in $\mathsf{R}[\varepsilon][X_1,\ldots,X_n]$ which define $\mathcal{S}_\varepsilon$. Below, we denote by $\Psi(\mathbf{X},\varepsilon)$ such a formula.

Consider the following set

$$T = \{(\mathbf{x}, x_{n+1}) \in \mathsf{R}^{n+1} \mid \Psi(\mathbf{x}, x_{n+1}) \wedge x_{n+1} > 0\} \ ,$$

and let $\overline{T}$ its closure and H be the hyperplane defined by $X_{n+1} = 0$ in R^{n+1}. As in the proof of [13, Proposition 12.36], the following equalities hold:

$$\mathcal{S} = \lim_{\varepsilon\to 0}\mathcal{S}_\varepsilon = \overline{T} \bigcap H.$$

We can express the limit using a formula in the first order theory of reals. For $\mathbf{x} \in \mathcal{S}_\varepsilon$ and $\mathbf{y} \in \mathcal{S}$ we have

$$\Phi_1 := \left[(\forall r > 0)\,(\exists \varepsilon_0) : (\forall \varepsilon)\,(0 < \varepsilon < \varepsilon_0) \Rightarrow \|\mathbf{x}-\mathbf{y}\|^2 < r^2\right] \Leftrightarrow \lim_{\varepsilon\to 0}\mathbf{x} = \mathbf{y} \ .$$

By quantifier elimination over the reals (see [24, 49] or [13, Theorem 2.77]), there exists a quantifier free formula Ψ_1 which is equivalent to Φ_1. The set

$$\{(\mathbf{x},\mathbf{y}) \in \mathsf{R}\langle\varepsilon\rangle^n \times \mathsf{R}^n \mid \Psi \wedge (\mathbf{y} \in \mathcal{S}) \wedge \Psi_1\} \ ,$$

is the graph of $\lim_{\varepsilon\to 0}$ and is semi-algebraic. This concludes the proof.

The proof in the complex case uses exactly the same techniques as above transposed to algebraically closed fields, i.e. if A and B are constructible sets and $h : A \to B$ is a regular map (see [46, Chapter 1]), then the Krull dimension of $h(A)$ is less than or equal to $h(B)$ and quantifier elimination over algebraically closed fields (see e.g. [13, Chapter 1]). □

Lemma 7. *Consider $\mathbf{x} \in V \cap \mathsf{R}^n$ and assume that f is non-negative over R^n and that there exists a neighbourhood $\mathscr{B} \subset \mathsf{R}^n$ of $\mathbf{x}$ such that $V \bigcap \mathscr{B} \bigcap \mathsf{R}^n$ is a finite set. Then, there exists $\mathbf{x}_\varepsilon \in \mathrm{crit}(\pi_1, V_\varepsilon)$ such that $\lim_{\varepsilon \to 0} \mathbf{x}_\varepsilon = \mathbf{x}$.*

Proof. By assumption $V \bigcap \mathscr{B} \bigcap \mathsf{R}^n$ is a finite set. Hence, there exists a sufficiently small $r \in \mathsf{R}$, $r > 0$, such that f is positive at all points in a ball, B, with center at $\mathbf{x}$ and radius r, except $\mathbf{x}$. That is $\mathbf{x}$ is the only point of $V \bigcap R^n$ in B; hence $\{\mathbf{x}\}$ is a bounded semi-algebraically connected component of $V \bigcap \mathsf{R}^n$.

By Proposition 5, there exist semi-algebraically connected components $C_{\varepsilon,1}, \ldots, C_{\varepsilon,\ell}$ of $V_\varepsilon, \mathsf{R}\langle\varepsilon\rangle^n$ such that $\{\mathbf{x}\} = \bigcup_{i=1}^{\ell} \lim_{\varepsilon \to 0} C_{\varepsilon,i}$, $C_{\varepsilon,i} \subset \mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$, and $C_{\varepsilon,i}$ does not intersect the boundary of $\mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$, $1 \leq i \leq \ell$.

We deduce that for $1 \leq i \leq \ell$, $C_{\varepsilon,i}$ is closed and bounded. However, $C_{\varepsilon,i} \subset \mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$ and it is closed and bounded; as a consequence, it has a non-empty intersection with $\mathrm{crit}(\pi_1, V_\varepsilon)$. Since we already observed that $\lim_{\varepsilon \to 0} C_{\varepsilon,i} \subset \{\mathbf{x}\}$, we deduce that for all $\mathbf{x}_\varepsilon \in \mathrm{crit}(\pi_i, V_\varepsilon) \cap C_{\varepsilon,i}$, $\lim_{\varepsilon \to 0} \mathbf{x}_\varepsilon = \mathbf{x}$. Our conclusion follows. □

Lemma 8. *Assume that f is non-negative over R^n and that $V \cap \mathsf{R}^n$ is bounded and non-empty. Then, for $1 \leq i \leq n$, $\mathrm{crit}(\pi_i, V_\varepsilon)$ is not empty and intersects all bounded semi-algebraically connected components of $V_\varepsilon \cap \mathsf{R}\langle\varepsilon\rangle^n$.*

Proof. Since $V \cap \mathsf{R}^n$ is bounded and non-empty there exists a semi-algebraically connected component C and a ball $B \subset \mathsf{R}^n$ such that $C \subset B$ and $C \cap B = \emptyset$. By Proposition 5, we deduce that there exist semi-algebraically connected components $C_{\varepsilon,1}, \ldots, C_{\varepsilon,k}$ of $V_\varepsilon \cap \mathsf{R}\langle\varepsilon\rangle^n$ such that $C = \bigcup_{\ell=1}^{k} \lim_{\varepsilon \to 0} C_{\varepsilon,\ell}$. Moreover since we assume that $V \cap \mathsf{R}^n$ is bounded, there exists a ball $B \subset \mathsf{R}^n$ such that $C \subset B$ and $C \cap B = \emptyset$. Using again Proposition 5, we conclude that $C_{\varepsilon,\ell} \subset \mathrm{ext}(B, \mathsf{R}\langle\varepsilon\rangle)$ for $1 \leq \ell \leq k$; hence $C_{\varepsilon,\ell}$ is closed and bounded.

Below, we prove that any bounded semi-algebraically connected component C_ε of $V_\varepsilon \cap \mathsf{R}\langle\varepsilon\rangle^n$ has a non-empty intersection with $\mathrm{crit}(\pi_i, V_\varepsilon)$. Then $\pi_1(C_\varepsilon)$ is closed and bounded (see [13, Theorem 3.20]). The extreme values of $\pi_1(C_\varepsilon)$ are attained at critical points of the restriction of π_1 to $V_\varepsilon \cap \mathsf{R}\langle\varepsilon\rangle^n$. In other words, C_ε has a non-empty intersection with $\mathrm{crit}(\pi_1, V_\varepsilon)$. Now, note that $\mathrm{crit}(\pi_1, V_\varepsilon) \subset \mathrm{crit}(\pi_i, V_\varepsilon)$, by definition. □

Lemma 9. *Let $f \in \mathsf{C}[X_1, \ldots, X_n]$ and $V \subset \mathsf{C}^n$ be defined by $f = 0$. Take $\alpha = (\alpha_1, \ldots, \alpha_{i-1}) \in \mathsf{C}^i$ and let $V_{i,\alpha}$ the algebraic set $V \bigcap \pi_{i-1}^{-1}(\alpha)$ and φ_i be the canonical projection $(x_1, \ldots, x_n) \mapsto x_i$. Then, the following holds:*

$$\mathrm{crit}(\varphi_i, V_{i,\alpha}) \subset \mathrm{crit}(\pi_i, V).$$

Proof. By definition $\mathrm{crit}(\pi_i, V)$ is defined by the vanishing of f and of the partial derivatives $\frac{\partial f}{\partial X_{i+1}}, \ldots, \frac{\partial f}{\partial X_n}$. Besides, the set $V_{i,\alpha}$ is defined by the system

$$f = 0, X_1 - \alpha_1 = \cdots = X_{i-1} - \alpha_{i-1} = 0.$$

By definition, $\mathrm{crit}(\varphi_i, V_{i,\alpha})$ is defined by the above equations and the vanishing of the maximal minors of the Jacobian matrix associated to $f, X_1 - \alpha_1, \ldots, X_{i-1} - \alpha_{i-1}, X_i$. The triangular shape of this Jacobian matrix implies that $\mathrm{crit}(\varphi_i, V_{i,\alpha})$ is defined by $f = 0, X_1 - \alpha_1 = \cdots = X_{i-1} - \alpha_{i-1} = 0$ and the vanishing of the partial derivatives $\frac{\partial f}{\partial X_{i+1}}, \ldots, \frac{\partial f}{\partial X_n}$.

The lemma follows from the observation that the system that defines $\mathrm{crit}(\pi_i, V_i)$ is contained in the system that defines $\mathrm{crit}(\varphi_i, V_{i,\alpha})$. □

4.2 Proof of Proposition 3 and Consequences

Proof of Proposition 3. First we prove the necessary condition. Assume that for a given $i \in \{0, \ldots, n\}$ it holds

$$\Big(\lim_{\varepsilon\to 0}(\mathrm{crit}(\pi_i, V_\varepsilon))\Big) \bigcap U = S \ .$$

We prove that this implies that the real dimension of S is $\leq i-1$. When S is empty, this is immediate; thus we can assume that S is non-empty.

By definition, $V \bigcap U = S$, therefore $V \bigcap \mathsf{R}^n$ is non-empty; note also that S is bounded since we assume that $V \bigcap \mathsf{R}^n$ is bounded.

Combining Lemma 8 and N_1, we conclude that $\mathrm{crit}(\pi_i, V_\varepsilon)$ has Krull dimension $i-1$. Lemma 6 implies that $\lim_{\varepsilon\to 0}(\mathrm{crit}(\pi_i, V_\varepsilon))$ has Krull dimension $\leq i-1$. We deduce that $(\lim_{\varepsilon\to 0}(\mathrm{crit}(\pi_i, V_\varepsilon))) \bigcap \mathsf{R}^n$ has real dimension $\leq i-1$. Consequently, $(\lim_{\varepsilon\to 0}(\mathrm{crit}(\pi_i, V_\varepsilon))) \bigcap U$ has real dimension $\leq i-1$. By assumption, $(\lim_{\varepsilon\to 0}(\mathrm{crit}(\pi_i, V_\varepsilon))) \bigcap U = S$; we conclude that S has real dimension $\leq i-1$.

Next, we assume that the real dimension of S is $\leq i-1$; we prove below that this implies that $(\lim_{\varepsilon\to 0}(\mathrm{crit}(\pi_i, V_\varepsilon))) \bigcap U = S$.

The inclusion $(\lim_{\varepsilon\to 0}(\mathrm{crit}(\pi_i, V_\varepsilon))) \bigcap U \subseteq S$ follows from the fact that $\mathrm{crit}(\pi_i, V_\varepsilon) \subseteq V_\varepsilon$, $\lim_{\varepsilon\to 0} V_\varepsilon \subseteq V$, and $V \bigcap U \subset S$.

It remains to prove the inverse inclusion, that is $S \subseteq (\lim_{\varepsilon\to 0}(\mathrm{crit}(\pi_i, V_\varepsilon))) \bigcap U$.

If S is empty, then it is immediate that $S \subseteq (\lim_{\varepsilon\to 0}(\mathrm{crit}(\pi_i, V_\varepsilon))) \bigcap U$. In the sequel, we assume that S is not empty.

Let $\mathbf{x} = (\alpha_1, \ldots, \alpha_n) \in S$; since $S = U \bigcap V$ by definition, we have $\mathbf{x} \in U$ and $\mathbf{x} \in V \bigcap \mathsf{R}^n$. Thus, we need to prove that there exists a point $\mathbf{x}_\varepsilon \in \mathrm{crit}(\pi_i, V_\varepsilon)$, such that $\lim_{\varepsilon\to 0} \mathbf{x}_\varepsilon = \mathbf{x}$. This is what we do below.

Recall that we have assumed that the real dimension of S is $\leq i-1$. Since $V \bigcap U = S$, we deduce that the real dimension of $V \bigcap U$ is $\leq i-1$. It follows that the local real dimension of $V \bigcap U$ at $\mathbf{x}$ is at most $i-1$. We claim that the real dimension of $V \bigcap \mathsf{R}^n$ at $\mathbf{x}$ is $\leq i-1$.

Indeed, let $S_1, \ldots, S_k$ be smooth semi-algebraic sets of respective dimension d_j which form a finite partition of V. The local real dimension of $V \bigcap \mathsf{R}^n$ at $\mathbf{x}$ is the maximum of the d_j's for j such that $\mathbf{x} \in \overline{S_j}$. Since U is open, $S_j \bigcap U$ is either empty or smooth of dimension d_j. Note also that the semi-algebraic sets $S_1 \bigcap U, \ldots, S_k \bigcap U$ form a partition of $V \bigcap U$. Therefore, the local real dimension of $V \bigcap \mathsf{R}^n$ at $\mathbf{x}$ is the same as the local real dimension of $V \bigcap U$ at $\mathbf{x}$ which is $\leq i-1$ as requested.

Denoting $\pi_{i-1}(\mathbf{x})$ by $\mathbf{x}_{i-1}$, we deduce by N_2 that $\pi_{i-1}^{-1}(\mathbf{x}_{i-1}) \bigcap V \bigcap \mathsf{R}^n$ is finite. Now, let $\tilde{f}$ be the polynomial obtained after instantiating the first $i-1$ variables with the first $i-1$ coordinates of $\mathbf{x}$, that is

$$\tilde{f} = f(X_i, \ldots, X_n) = f(\alpha_1, \ldots, \alpha_{i-i}, X_i, \ldots, X_n) \ .$$

We let $\tilde{x} = (\alpha_i, \ldots, \alpha_n)$ and $\tilde{V}$ (resp. $\tilde{V}_\varepsilon \subset \mathbf{C}\langle\varepsilon\rangle^{n-i+1}$) be the algebraic set defined by $\tilde{f} = 0$ (resp. $\tilde{f} = \varepsilon$). By assumption, f is non-negative over R^n. Therefore, $\tilde{f}$ is non-negative over R^{n-i+1}. We also consider the canonical projections

$$\tilde{\varphi}_i : (\mathbf{x}_i, \ldots, \mathbf{x}_n) \to \mathbf{x}_i \quad \text{and} \quad \varphi_i : (\mathbf{x}_1, \ldots, \mathbf{x}_n) \to \mathbf{x}_i.$$

By applying Lemma 7 to $\tilde{V}$ and $\tilde{f}$, there exists $\tilde{\mathbf{x}}_\varepsilon \in \mathrm{crit}(\tilde{\varphi}_i, \tilde{V}_\varepsilon)$, such that $\lim_{\varepsilon\to 0} \tilde{\mathbf{x}}_\varepsilon = (\alpha_i, \ldots, \alpha_n)$. Now define $\mathbf{x}_\varepsilon = (\alpha_1, \ldots, \alpha_{i-1}, \tilde{\mathbf{x}}_\varepsilon)$ and $V'_\varepsilon = V_\varepsilon \bigcap \pi_{i-1}^{-1}(\alpha_1, \ldots, \alpha_{i-1})$.

Since $\tilde{\mathbf{x}}_\varepsilon \in \operatorname{crit}(\tilde{\varphi}_i, \tilde{V}_\varepsilon)$, it is immediate that $\mathbf{x}_\varepsilon \in \operatorname{crit}(\varphi_i, V'_\varepsilon)$, and using Lemma 9 $\mathbf{x}_\varepsilon \in \operatorname{crit}(\pi_i, V_\varepsilon)$. To summarize, we have established $\mathbf{x}_\varepsilon \in \operatorname{crit}(\pi_i, V_\varepsilon)$ and $\lim_{\varepsilon\to 0} \mathbf{x}_\varepsilon = \mathbf{x}$ as requested. This finishes the proof. □

The following corollary is a direct consequence of Proposition 3 and it is crucial for the proof of correctness of our algorithm. Recall that, by convention, $\operatorname{crit}(\pi_0, V_\varepsilon)$ is the empty set.

Corollary 10. *Assume that f satisfies property N and that V is bounded. Let d be the real dimension of S. Then, $d \geq 0$ if and only if there exist an integer i in $\{1, \ldots, n\}$ such that $(\lim_{\varepsilon\to 0} \operatorname{crit}(\pi_i, V_\varepsilon)) \bigcap U \neq (\lim_{\varepsilon\to 0} \operatorname{crit}(\pi_{i-1}, V_\varepsilon)) \bigcap U$ and $d+1$ is the largest of these integers.*

Proof. Note that the assumptions of Proposition 3 are satisfied. This implies that, for $0 \leq i \leq n$, $(\lim_{\varepsilon\to 0} \operatorname{crit}(\pi_i, V_\varepsilon)) \bigcap U = S$ if and only if $d \leq i - 1$. As a consequence, we deduce that

$$S = \left(\lim_{\varepsilon\to 0} \operatorname{crit}(\pi_{d+1}, V_\varepsilon)\right) \bigcap U = \cdots = \left(\lim_{\varepsilon\to 0} \operatorname{crit}(\pi_n, V_\varepsilon)\right) \bigcap U$$

and $S \neq (\lim_{\varepsilon\to 0} \operatorname{crit}(\pi_i, V_\varepsilon)) \bigcap U$ for $1 \leq i \leq d$. This concludes the proof. □

5 Algorithm and proof of Theorem 1

There is an error in the main theorem and the stated bound does not hold.

5.1 Main algorithm

The input of our algorithm is two sets of polynomials $F = (f_1, \ldots, f_p)$ and $G = (g_1, \ldots, g_s)$ in $\mathsf{Z}[X_1, \ldots, X_n]$. The output is the real dimension of the semi-algebraic set $\mathscr{S} \subset \mathsf{R}^n$ defined by

$$f_1 = \cdots = f_p = 0, \quad g_1 > 0, \ldots, g_s > 0 \ .$$

The main idea of the algorithm is to perform symbolic manipulations to define a polynomial f with coefficients in $\mathsf{R}[\zeta]$ such that

- f and the semi-algebraic set $S \subset \mathsf{R}\langle\zeta\rangle^{n+1}$ defined by $f = 0$ and $g_1 > 0, \ldots, g_s > 0$ satisfy the assumptions of Corollary 10, and
- the real dimension of S is the same as the real dimension of $\mathscr{S}$.

Then, we apply the results of the previous section (Section 4) using as ground field (that is the field where the coefficients of the input polynomials belong to) $\mathsf{R}\langle\zeta\rangle$.

Let us recall the notations that we use: $S \subset \mathsf{R}\langle\zeta\rangle^{n+1}$ is the semi-algebraic set defined by $f = 0, g_1 > 0, \ldots, g_s > 0$, $U \subset \mathsf{R}\langle\zeta\rangle^{n+1}$ is the open semi-algebraic set defined by $g_1 > 0, \ldots, g_s > 0$, and $V \subset \mathsf{C}\langle\zeta\rangle^{n+1}$, resp. $V_\varepsilon \subset \mathsf{C}\langle\zeta\rangle\langle\varepsilon\rangle^{n+1}$, is the algebraic set defined by $f = 0$, resp. $f = \varepsilon$.

From Corollary 10, $d \geq 0$ if and only if there exists an integer i in $\{1, \ldots, n\}$ such that

$$\left(\lim_{\varepsilon\to 0} \operatorname{crit}(\pi_i, V_\varepsilon)\right) \bigcap U \neq \left(\lim_{\varepsilon\to 0} \operatorname{crit}(\pi_{i-1}, V_\varepsilon)\right) \bigcap U \,,$$

and $d+1$ is the largest of these integers (notice that by convention $\operatorname{crit}(\pi_0, V_\varepsilon) = \emptyset$; see Section 2).

Subroutines. We need three subroutines. The first one is called Random; it takes as input an integer n and returns a randomly chosen $n \times n$ matrix in $\mathrm{GL}_n(\mathsf{Z})$.

The second routine IsEmpty takes as input a polynomial H and a set of polynomials $\mathcal{G} = (G_1, \ldots, G_s)$ in $\mathsf{Z}[\zeta, \eta, \varepsilon][X_1, \ldots, X_n]$, where ζ, η, and ε are infinitesimals. Let $V \subset \mathsf{C}\langle\zeta\rangle\langle\eta\rangle\langle\varepsilon\rangle^n$ be the algebraic set defined by $H = 0$ and $U \in \mathsf{R}\langle\zeta\rangle\langle\eta\rangle\langle\varepsilon\rangle^n$ the open semi-algebraic set defined by $G_1 > 0, \ldots, G_s > 0$. The subroutine decides if the semi-algebraic set $V \bigcap U$ is empty or not.

Let δ be the maximum of the degrees of the monomials in $\zeta, \eta, \varepsilon, X_1, \ldots, X_n$ appearing in H and $\mathcal{G}$. If $\mathsf{Z} = \mathbb{Z}$, then we denote by τ the maximum bit size of the integers appearing in H and $\mathcal{G}$. The algorithm returns True if the semi-algebraic set $V \bigcap U$ is empty, and False otherwise. It is based on [13, Algorithm 13.1].

Lemma 11. *Using the above notations, algorithm* $\mathsf{IsEmpty}(H, \mathcal{G})$ *decides if the semi-algebraic set defined by* $H = 0$ *and* $G_1 > 0, \ldots, G_s > 0$ *is empty or not within* $(s\,\delta)^{O(n)}$ *arithmetic operations in* Z. *When* $\mathsf{Z} = \mathbb{Z}$, *then the Boolean complexity of* IsEmpty *is* $\tau\,(s\,\delta)^{O(n)}$.

When IsEmpty is called by the main algorithm, the input polynomials have coefficients in $\mathsf{Z}[\zeta]$.

The third subroutine, DisjointPolar, takes as input a polynomial $f \in \mathsf{Z}[\zeta][X_1, \ldots, X_{n+1}]$, $G = (g_1, \ldots, g_s) \subset \mathsf{Z}[X_1, \ldots, X_n]$, $Q \in \mathsf{Z}[\zeta][X_1, \ldots, X_{n+1}]$, and an integer $i \in \{1, \ldots, n\}$ (where ζ is an infinitesimal that we manipulate as a variable). The polynomial Q defines a sphere in $\mathsf{R}\langle\zeta\rangle^{n+1}$ that strictly contains the semi-algebraic set S. For example $Q = (\zeta(X_1^2 + \cdots + X_n^2 + X_{n+1}^2) - 2)$.

The routine $\mathsf{DisjointPolar}(f, G, Q, i)$ returns True if

$$\left(\lim_{\varepsilon \to 0} \mathrm{crit}(\pi_i, V_\varepsilon) \cap U\right) \neq \left(\lim_{\varepsilon \to 0} \mathrm{crit}(\pi_{i-1}, V_\varepsilon)\right) \cap U,$$

and False otherwise. Below, we denote by δ the maximal degree of the monomials in $\zeta, X_1, \ldots, X_n$ appearing in f, G and Q.

The routine DisjointPolar is described Section 5.2, where we also prove the following Lemma.

Lemma 12. *Let* $f \in \mathsf{Z}[\zeta][X_1, \ldots, X_{n+1}]$, $G = (g_1, \ldots, g_s) \subset \mathsf{Z}[X_1, \ldots, X_n]$, $B \in \mathsf{Z}[\zeta][X_1, \ldots, X_{n+1}]$, *and* $i \geq 0$. *Let* S *be the semi-algebraic set defined by* $\{f = 0 \wedge G > 0\}$, *and let* $Q \leq 0$ *define a ball that strictly contains* S. *Assume that* f *satisfies* N *and is non-negative over* $\mathsf{R}\langle\zeta\rangle^n$ *and that* $(\lim_{\varepsilon \to 0} \mathrm{crit}(\pi_i, V_\varepsilon)) \bigcap U$ *is not empty. There exists an algorithm* DisjointPolar *which decides if* $(\lim_{\varepsilon \to 0} \mathrm{crit}(\pi_i, V_\varepsilon)) \cap U \neq (\lim_{\varepsilon \to 0} \mathrm{crit}(\pi_{i-1}, V_\varepsilon)) \cap U$ *within* $(s\,\delta)^{O(n)}$ *operations in* Z.

If $\mathsf{Z} = \mathbb{Z}$ *and the maximum bit size of the integers in the coefficients of the input polynomials is* τ, *then the Boolean complexity of the algorithm is* $\tau\,(s\,\delta)^{O(n)}$.

We can now describe our main algorithm ComputeRealDimension.

Algorithm 1: ComputeRealDimension(F, G)

Input: $F = (f_1, \ldots, f_p)$ and $G = (g_1, \ldots, g_s)$ in $\mathsf{Z}[X_1, \ldots, X_n]$
Output: The real dimension of the semi-algebraic set defined by $f_1 = \cdots = f_p = 0, g_1 > 0, \ldots, g_s > 0$

1 $f_0 \leftarrow \sum_i f_i^2$;
2 **if** IsEmpty(f_0, G) **then** RETURN -1 ;
3 ;
4 $f \leftarrow f_0 + (\zeta(X_1^2 + \cdots + X_n^2 + X_{n+1}^2) - 1)^2$;
5 $Q \leftarrow (\zeta(X_1^2 + \cdots + X_n^2 + X_{n+1}^2) - 2)$;
6 $\mathbf{A} \leftarrow$ Random(n) ;
7 $f^{\mathbf{A}}(\mathbf{X}) \leftarrow f(\mathbf{A}\,\mathbf{X})$ and $G^{\mathbf{A}}(\mathbf{X}) \leftarrow G(\mathbf{A}\,\mathbf{X})$ and $Q^{\mathbf{A}}(\mathbf{X}) \leftarrow Q(\mathbf{A}\,\mathbf{X})$;
8 **for** $n \geq i \geq 1$ **do**
9 **if** DisjointPolar($f^{\mathbf{A}}$, $G^{\mathbf{A}}$, $Q^{\mathbf{A}}$, i) **then** RETURN $i - 1$;
10 ;

The proof of Theorem 1 consists of proving the correctness and complexity estimate of ComputeRealDimension.

Correctness. Let d be the real dimension of the semi-algebraic set $\mathscr{S} \subset \mathsf{R}^n$ defined by $f_1 = \cdots = f_p = 0, g_1 > 0, \ldots, g_s > 0$.

At Step 2 we test whether the semi-algebraic set is empty or not. In the sequel we assume that the semi-algebraic set is not empty, and so $d \geq 0$.

We also denote by $V \subset \mathsf{C}\langle\zeta\rangle^{n+1}$ the algebraic set defined by $f = 0$ where f is defined at Step 4. Assume for the moment that the semi-algebraic set S has real dimension d and that $V \cap \mathsf{R}\langle\zeta\rangle^n$ is bounded. At Step 7, the real dimension of the semi-algebraic set $S^{\mathbf{A}}$, defined by $f^{\mathbf{A}} = 0$ and $g_1^{\mathbf{A}} > 0, \ldots, g_s^{\mathbf{A}} > 0$, is also d. Since $\mathbf{A}$ is randomly chosen we can assume that it lies in the non-empty Zariski open set $\mathscr{O}$ defined in Proposition 2. Therefore, $f^{\mathbf{A}}$ satisfies property N (see Definition 2) and $V^{\mathbf{A}} \cap \mathsf{R}\langle\zeta\rangle^{n+1}$ (and consequently $S^{\mathbf{A}}$) is bounded. In other words, all the assumptions of Corollary 10 are satisfied.

In the for-loop, starting with $i = n$, the algorithm looks for the largest integer i such that

$$\left(\lim_{\varepsilon \to 0} \operatorname{crit}(\pi_i, V_\varepsilon^{\mathbf{A}})\right) \cap U^{\mathbf{A}} \neq \left(\lim_{\varepsilon \to 0} \operatorname{crit}(\pi_{i-1}, V_\varepsilon^{\mathbf{A}})\right) \cap U^{\mathbf{A}} \ .$$

Each time we enter in the loop $\left(\lim_{\varepsilon \to 0} \operatorname{crit}(\pi_i, V_\varepsilon^{\mathbf{A}})\right) \cap U^{\mathbf{A}}$ is not empty (and actually equals $S^{\mathbf{A}}$). The other assumptions of Lemma 12 are obviously satisfied. Also, by Corollary 10 and Lemma 12, we deduce that when $d \geq 0$, at Step 9 the algorithm will return d.

To finish the proof it remains to establish that S is bounded and its real dimension is the same as the real dimension of $\mathscr{S}$.

We start with the boundedness statement. The polynomial f is the sum of the squares of $f_1, \ldots, f_p$ and the square of the polynomial $\zeta(X_1^2 + \cdots + X_n^2 + X_{n+1}^2) - 1$. The set of roots in $\mathsf{R}\langle\zeta\rangle^{n+1}$ of this latter polynomial is the n-dimensional sphere, $\mathbb{S}_{n+1}$, with center at the origin and radius $1/\sqrt{\zeta}$. It is straightforward that $V \cap \mathsf{R}\langle\zeta\rangle^{n+1}$ is bounded and since $S = V \cap U$, we deduce that S is bounded.

Now, we prove that S has the same real dimension, d, as the semi-algebraic set $\mathscr{S}$. The proof consists of two steps. We prove consecutively that

(i) $\mathrm{ext}(\mathscr{S}, \mathsf{R}\langle\zeta\rangle) \subset \mathsf{R}\langle\zeta\rangle^n$ has real dimension d, and

(ii) S has the same real dimension as $\mathrm{ext}(\mathscr{S}, \mathsf{R}\langle\zeta\rangle) \subset \mathsf{R}\langle\zeta\rangle^n$.

Statement *(i)* is a straightforward consequence of the Lemma below.

Lemma 13. *Let $\mathcal{S}$ be a semi-algebraic subset of R^n and consider its extension $\mathrm{ext}(\mathcal{S}, \mathsf{R}\langle\zeta\rangle)$. Then $\mathcal{S}$ and $\mathrm{ext}(\mathcal{S}, \mathsf{R}\langle\zeta\rangle^n)$ have the same real dimension.*

Proof. Let d be the real dimension of $\mathcal{S}$ and d' be the real dimension of $\mathrm{ext}(\mathcal{S}, \mathsf{R}\langle\zeta\rangle)$. Then there is an injective map $\varphi : \mathcal{S} \to [0,1]^d$. We consider the extension of φ, that is $\mathrm{ext}(\varphi, \mathsf{R}\langle\zeta\rangle)$. It is also injective [13, Exercise 2.17] and by the definition of the real dimension (see Definition 1) we deduce that $d' \leq d$. Now remark that $\lim_{\zeta\to 0} \mathrm{ext}(\mathcal{S}, \mathsf{R}\langle\zeta\rangle) = \mathcal{S}$. By Lemma 6 we deduce that $d \leq d'$ which finishes the proof. □

To prove *(ii)*, we consider the restriction of π_n to S. It is a semi-algebraic and injective function, since for all $(\mathbf{x}, x_{n+1}) \in \mathsf{R}\langle\zeta\rangle^n \times \mathsf{R}\langle\zeta\rangle$ with $\mathbf{x} \in \mathrm{ext}(\mathscr{S}, \mathsf{R}\langle\zeta\rangle)$ and $(\mathbf{x}, x_{n+1}) \in \mathbb{S}_{n+1}$, $x_{n+1} = \sqrt{\frac{1}{\zeta} - ||\mathbf{x}||^2}$. Moreover, $\pi_n(S) = \mathrm{ext}(\mathscr{S}, \mathsf{R}\langle\zeta\rangle)$.

By [13, Proposition 5.29] we deduce that the real dimension of S is equal to the real dimension of $\mathrm{ext}(\mathscr{S}, \mathsf{R}\langle\zeta\rangle)$; which is d by *(i)*. □

Complexity Analysis. The complexity estimate is straightforward by Lemmata 11 and 12. The first call to IsEmpty costs at most $(s\,D)^{O(n)}$ arithmetic operations. Next, the algorithm calls n times the sub-routine DisjointPolar with input polynomials of total degree $O(D)$. Each call costs $(s\,D)^{O(n)}$ operations in Z. Since all functions in the complexity class $n(s\,D)^{O(n)}$ lie in the complexity class $(s\,D)^{O(n)}$, we deduce that ComputeRealDimension runs within $(s\,D)^{O(n)}$ arithmetic operations in Z.

This is a probabilistic bound because of the random change of coordinates that we apply to f and G at Step 7 to ensure property N (Definition 2).

5.2 The subroutine DisjointPolar and Proof of Lemma 12

In order to describe DisjointPolar, we need to recall some fundamental algorithmic specifications and complexity results in computational real algebraic geometry. Sometimes we need to prove some statements which are quite folklore in the area; proofs of these facts are given in the Appendix.

Quantifier Elimination over the reals. Let $\mathbf{X} = (X_1, \ldots, X_n)$ and $\mathbf{Y} = (Y_1, \ldots, Y_t)$ be finite sequences of variables, Ω be the existential quantifier $\exists$ or the universal quantifier $\forall$ and $\mathcal{P}(\mathbf{X}, \mathbf{Y})$ be a Boolean function of s atomic predicates $H_i(\mathbf{X}, \mathbf{Y}) \rhd_i 0$, where $\rhd_i \in \{>, <, =\}$ and $H_i \in \mathsf{Z}[\mathbf{X}, \mathbf{Y}]$, for $1 \leq i \leq s$. We let $\delta = \max(\deg(H_i), 1 \leq i \leq s)$ and when $\mathsf{Z} = \mathbb{Z}$, τ is the maximum of the bit size of the coefficients in the H_i's

One-block quantifier elimination over the reals consists in computing a quantifier-free formula which is equivalent to the first order quantified formula $\Phi : (\Omega\,\mathbf{X} \in \mathsf{R}^n)\,\mathcal{P}(\mathbf{X}, \mathbf{Y})$.

The following theorem is a simplification of the general purpose quantifier elimination algorithm in [13, Algorithm 14.5 and Theorem 14.16].

Theorem 14 (One Block Quantifier Elimination over the reals)**.** *There exists an algorithm* OneBlockQuantifierElimination *which takes as input* $\Omega, \mathcal{P}, \mathbf{X}, \mathbf{Y}$ *and returns a quantifier free formula* Ψ *of the form* $\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} h_{i,j} \rhd_{i,j} 0$*, where* $h_{i,j} \in \mathsf{Z}[Y_1, \ldots, Y_t]$ *and* $\rhd_{i,j} \in \{>, =\}$*, that is equivalent to* Φ*, such that*

$$I \leq s^{(t+1)}\, n\, \delta^{(t+1)O(n)}, \quad J_i \leq s^{(n+1)}\, \delta^{O(n)}, \quad \deg(h_{i,j}) \leq \delta^{O(n)} \ .$$

If $\mathsf{Z} = \mathbb{Z}$*, then the maximum bit size of the coefficients of* $h_{i,j}$ *is bounded by* $\tau\delta^{(t+1)O(n)}$*. The above transformation requires* $s^{(t+1)(n+1)}\delta^{(t+1)O(n)}$ *arithmetic operations in* Z*. The Boolean complexity of the algorithm is* $\tau s^{(t+1)(n+1)}\delta^{(t+1)O(n)}$*.*

Limits of semi-algebraic sets in $\mathsf{R}\langle\zeta\rangle\langle\eta\rangle\langle\varepsilon\rangle$ **when** $\varepsilon \to 0$**.** The routine UnivariateLimit takes as input a quantifier-free formula Ψ, which is a disjunction of conjunctions of polynomial equations/inequalities in $\mathsf{Z}[\zeta, \eta, \varepsilon][Z]$, and the infinitesimal ε. This formula defines a semi-algebraic set $\mathcal{S}_\varepsilon$ in $\mathsf{R}\langle\zeta\rangle\langle\eta\rangle\langle\varepsilon\rangle$. It outputs a semi-algebraic description of $\lim_{\varepsilon\to 0} \mathcal{S}_\varepsilon$. This is based on quantifier elimination over the reals [13, Theorem 14.16].

Lemma 15. *Let* δ *be the maximum of the degrees of the momonials in* ζ, η, ε *of the polynomials in* Ψ *and* ℓ *be the number of polynomials in* Ψ*. One can compute* UnivariateLimit(Ψ, ε) *within* $(\ell\,\delta)^{O(1)}$ *arithmetic operations in* Z*.*

When $\mathsf{Z} = \mathbb{Z}$ *and* τ *is a bound on the bit size of the integers of the coefficients in* Ψ*, then* UnivariateLimit(Ψ, ε) *runs within* $\tau(\ell\,\delta)^{O(1)}$ *bit operations.*

Computing limits of critical points. The routine LimitsOfCriticalPoints takes as input a polynomial H and a set of polynomials $\mathcal{G} = (G_1, \ldots, G_s)$ in $\mathsf{Z}[\zeta][X_1, \ldots, X_n]$. We denote by $V_\varepsilon \subset \mathsf{C}\langle\zeta\rangle\langle\varepsilon\rangle^n$ the algebraic set defined by $H - \varepsilon = 0$, by $U \subset \mathsf{R}\langle\zeta\rangle^n$ the open semi-algebraic set defined by $G_1 > 0, \ldots, G_s > 0$ and by δ the maximum of the degrees of the monomials in $\zeta, X_1, \ldots, X_n$ appearing in H and $\mathcal{G}$. If $\mathsf{Z} = \mathbb{Z}$, then we denote by τ the maximum bit size of the integers appearing in H and $\mathcal{G}$. It is based on [13, Algorithm 13.1] and [13, Algorithm 11.20].

Lemma 16. *Assume that* H *is non-negative over* $\mathsf{R}\langle\zeta\rangle^n$ *and that* $\mathrm{crit}(\pi_1, V_\varepsilon)$ *is finite. There exists an algorithm* LimitsOfOfCriticalPoints *which takes as input* H *and* $\mathcal{G}$ *as above, and returns* True *if* $(\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_1, V_\varepsilon)) \bigcap U$ *is non-empty else it returns* False*, within* $(s\,\delta)^{O(n)}$ *arithmetic operations in* Z*.*

When $\mathsf{Z} = \mathbb{Z}$ *and* τ *is the maximum bit size of the coefficients, then the Boolean complexity of* LimitsOfCriticalPoints *is* $\tau\,(s\,\delta)^{O(n)}$*.*

The routine IsRealizable**.** A typical call of this routine is IsRealizable(Φ), where Φ is a union of disjunctions of univariate polynomials in Z with coefficients in $\mathsf{Z}[\zeta, \eta]$.

The subroutine calls Algorithm 10.13 from [13] to compute all realizable sign condition of the polynomials and checks if there is at least one sign condition that is compatible with Φ. In this case it returns True, otherwise it returns False.

Lemma 17. *Let* Φ *be a union of disjunctions of univariate polynomials in* Z *with coefficients in* $\mathsf{Z}[\zeta, \eta]$ *such that all monomials in* Z, ζ, η *appearing in* Φ *have degree at most* δ*.*

The complexity of IsRealizable(Φ) *is* $\ell\,\delta^{O(1)}$ *operations in* Z*. If* $\mathsf{Z} = \mathbb{Z}$ *and the maximum bit size of the coefficients of the polynomials of the input is* τ*, then the Boolean complexity is* $\tau\,\ell\,\delta^{O(1)}$*.*

The routine DisjointPolar**.** Let $f \in \mathsf{Z}[\zeta][X_1, \ldots, X_n]$, a set of polynomials $G = (g_1, \ldots, g_s) \subset \mathsf{Z}[X_1, \ldots, X_n]$, a polynomial $Q \in \mathsf{Z}[\zeta][X_1, \ldots, X_n]$ and an integer i, such that $1 \leq i \leq n$.

The open semi-algebraic set of $\mathsf{R}\langle\zeta\rangle^n$ defined by $g_1 > 0, \ldots, g_s > 0$ is denoted by U. We introduce another infinitesimal η, with $\zeta > \eta > 0$, and we consider the semi-algebraic set $U_\eta \subset \mathsf{R}\langle\zeta\rangle\langle\eta\rangle^n$ defined by $g_1 \geq \eta, \ldots, g_s \geq \eta$. We also denote the latter inequalities by $G \geq \eta$. Note that U_η is closed.

In the sequel, we denote $\mathsf{R}\langle\zeta\rangle\langle\eta\rangle$ by $\mathbf{R}$ and $\mathsf{C}\langle\zeta\rangle\langle\eta\rangle$ by $\mathbf{C}$.

Finally, we introduce one more infinitesimal ε with $\zeta > \eta > \varepsilon$. Let $V_\varepsilon \subset \mathbf{C}\langle\varepsilon\rangle^n$ be the algebraic variety defined by $f - \varepsilon = 0$. To make the notation simpler, $\mathrm{ext}(U_\eta, \mathbf{R}\langle\varepsilon\rangle)$ will be denoted by $U_{\eta,\varepsilon}$ and $\mathrm{ext}(B, \mathbf{R}\langle\varepsilon\rangle)$ will be denoted by B_ε.

We assume that

- f satisfies property N (Definition 2) and is non-negative over $\mathsf{R}\langle\zeta\rangle^n$;
- that $Q \leq 0$ defines a ball B that strictly contains the semi-algebraic set defined by $f = 0$ and $g_1 > 0, \ldots, g_s > 0$.
- and the solution set of $g_1 > 0, \ldots, g_s > 0$ has a non-empty intersection with $\mathrm{crit}(\pi_i, V_\varepsilon)$;

Then, DisjointPolar(f, G, Q, i) returns True if $(\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_i, V_\varepsilon)) \bigcap U \neq (\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_{i-1}, V_\varepsilon)) \bigcap U$, and False otherwise. Before giving a detailed description, we briefly give a geometric view of the operations performed by DisjointPolar.

The algorithm works as follows. We consider separately the case $i = 1$ (Step 1). By convention $\mathrm{crit}(\pi_0, V_\varepsilon)$ is the empty set. Therefore, $(\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_0, V_\varepsilon)) \bigcap U = \emptyset$ and if $i = 1$, then it suffices to check whether $(\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_1, V_\varepsilon)) \bigcap U$ is empty or not.

When $i \geq 2$, the algorithm starts by testing if $\mathrm{crit}(\pi_{i-1}, V_\varepsilon) \bigcap U_{\eta,\varepsilon}$ is empty. We will see that when this is the case, it implies that $(\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_{i-1}, V_\varepsilon)) \bigcap U$ is empty. Since by assumption $(\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_{i-1}, V_\varepsilon)) \bigcap U$ is not empty, the routine returns True.

When $\mathrm{crit}(\pi_{i-1}, V_\varepsilon) \bigcap U_{\eta,\varepsilon}$ is empty, the routine constructs a formula that defines the following semi-algebraic set

$$A_\varepsilon = \{(\mathbf{x}, \mathbf{y}, z) \in \mathbf{R}\langle\varepsilon\rangle^{2n+1} \quad | \quad \mathbf{x} \in (\mathrm{crit}(\pi_i, V_\varepsilon) - \mathrm{crit}(\pi_{i-1}, V_\varepsilon)) \bigcap U_{\eta,\varepsilon} \bigcap B_\varepsilon,$$
$$\mathbf{y} \in \mathrm{crit}(\pi_{i-1}, V_\varepsilon) \bigcap U_{\eta,\varepsilon} \bigcap B_\varepsilon,\ ||x - y|| = z > 0\} \ .$$

Next, we use quantifier elimination to compute a semi-algebraic description of the semi-algebraic set $\lim_{\varepsilon\to 0} \pi_Z(A_\varepsilon) \subset \mathbf{R}$ (where π_Z is the projection on the Z-coordinate). We will prove that

$$\left(\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_i, V_\varepsilon)\right) \bigcap U \neq \left(\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_{i-1}, V_\varepsilon)\right) \bigcap U \iff \lim_{\varepsilon\to 0} \pi_Z(A_\varepsilon) \bigcap \{z > 0\} \neq \emptyset \ .$$

For the correctness proof of DisjointPolar we will need the following lemma.

Lemma 18. *Assume that f is non-negative over $\mathbf{R}^n$ and satisfies* N*. If $\mathbf{x} \in (\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_i, V_\varepsilon)) \bigcap \mathbf{R}^n$, then there exists $\mathbf{x}_\varepsilon \in \mathrm{crit}(\pi_i, V_\varepsilon) \bigcap \mathbf{R}\langle\varepsilon\rangle^n$ such that $\lim_{\varepsilon\to 0} \mathbf{x}_\varepsilon = \mathbf{x}$.*

Proof. Consider the polynomial $H = f + \sum_{k=i}^n (\frac{\partial f}{\partial X_k})^2$ and notice that $H(\mathbf{x}) = 0$. Then, apply Proposition 5 to the semi-algebraically connected component of the real solution set of $H = 0$ containing $\mathbf{x}$. Thus, there exists $\mathbf{x}_\varepsilon \in \mathbf{R}\langle\varepsilon\rangle^n$ such that $H(\mathbf{x}_\varepsilon) - \varepsilon = 0$ and $\lim_{\varepsilon\to 0} \mathbf{x}_\varepsilon = \mathbf{x}$. This implies that $\mathbf{x}_\varepsilon \in \mathrm{crit}(\pi_{i-1}, V_\varepsilon) \bigcap \mathbf{R}\langle\varepsilon\rangle^n$. □

Algorithm 2: DisjointPolar(f, G, Q, i)

Input: $f \in \mathsf{Z}[\zeta][X_1, \ldots, X_n]$, $G = (g_1, \ldots, g_s) \subset \mathsf{Z}[X_1, \ldots, X_n]$, $Q \in \mathsf{Z}[\zeta][X_1, \ldots, X_n]$, and i
Output: True if $(\lim_{\varepsilon \to 0} \operatorname{crit}(\pi_i, V_\varepsilon)) \bigcap U \neq (\lim_{\varepsilon \to 0} \operatorname{crit}(\pi_{i-1}, V_\varepsilon)) \bigcap U$. False otherwise.
Assumptions: f satisfies N and is non-negative over $\mathsf{R}\langle\zeta\rangle^n$, $Q \leq 0$ defines a ball strictly containing S, $(\lim_{\varepsilon \to 0} \operatorname{crit}(\pi_i, V_\varepsilon)) \bigcap U \neq \emptyset$, and $1 \leq i \leq n$

1 **if** $i = 1$ **then** RETURN LimitsOfCriticalPoints(f, G) ;

2 $P_1 \leftarrow \{(f(\mathbf{X}) - \varepsilon)^2 + \left(\frac{\partial f(\mathbf{X})}{\partial X_{i+1}}\right)^2 + \cdots + \left(\frac{\partial f(\mathbf{X})}{\partial X_n}\right)^2 = 0 \wedge G \geq \eta \wedge Q \leq 0\}$;

3 $P_2 \leftarrow \mathsf{Subs}(\mathbf{X} = \mathbf{Y}, \{(f(\mathbf{X}) - \varepsilon)^2 + \left(\frac{\partial f(\mathbf{X})}{\partial X_i}\right)^2 + \cdots + \left(\frac{\partial f(\mathbf{X})}{\partial X_n}\right)^2 = 0 \wedge G \geq \eta \wedge Q \leq 0\})$;

4 **if** IsEmpty(P_2) **then** RETURN False ;

5 ;

6 $\Phi \leftarrow [\, P_1(\mathbf{X}) \wedge P_2(\mathbf{Y}) \wedge \frac{\partial f(\mathbf{X})}{\partial X_i} \neq 0 \wedge \|\mathbf{X} - \mathbf{Y}\|^2 > Z^2 \wedge Z > 0\,]$;

7 $\Psi \leftarrow$ OneBlockQuantifierElimination$(\exists, \Phi, [\mathbf{X}, \mathbf{Y}], [Z, \zeta, \eta, \varepsilon])$;

8 /* $\Psi = [\Psi_1, \ldots, \Psi_I]$ */

9 $\widetilde{\Psi} \leftarrow [\mathsf{UnivariateLimit}(\Psi_1, \varepsilon), \ldots \mathsf{Limit}(\Psi_I, \varepsilon)]$;

10 **for** $1 \leq k \leq I$ **do**

11 **if** IsRealizable$(\widetilde{\Psi}_k \wedge (Z > 0))$ **then** RETURN True ;

12 ;

13 RETURN False ;

We can now prove Lemma 12.

Correctness. By assumption, f is non-negative over $\mathsf{R}\langle\zeta\rangle^n$ and satisfies N. Thus $\operatorname{crit}(\pi_1, V_\varepsilon)$ is finite. Moreover, all the assumptions of Lemma 16 are satisfied that implies correctness when $i = 1$.

In what follows, we assume that $i \geq 2$.

Note that the systems P_1 and P_2 at Steps 2 and 3 define respectively the sets

$$\operatorname{crit}(\pi_i, V_\varepsilon) \bigcap U_{\eta,\varepsilon} \bigcap B_\varepsilon \quad \text{and} \quad \operatorname{crit}(\pi_{i-1}, V_\varepsilon) \bigcap U_{\eta,\varepsilon} \bigcap B_\varepsilon \ .$$

At Step 4, the call to IsEmpty returns True if and only if $\operatorname{crit}(\pi_{i-1}, V_\varepsilon) \bigcap U_{\eta,\varepsilon} \bigcap B_\varepsilon$ is empty. We claim that if this latter set is empty then $(\lim_{\varepsilon \to 0} \operatorname{crit}(\pi_{i-1}, V_\varepsilon)) \bigcap U$ is empty. Since by assumption $(\lim_{\varepsilon \to 0} \operatorname{crit}(\pi_i, V_\varepsilon)) \bigcap U$ is not empty, DisjointPolar runs correctly by returning True at Step 4. Now we prove our claim.

Assume by contradiction that there exists $\mathbf{x} \in (\lim_{\varepsilon \to 0} \operatorname{crit}(\pi_{i-1}, V_\varepsilon)) \bigcap U$. Then, by assumption $\mathbf{x} \in B$ and $g_1(\mathbf{x}) > 0, \ldots, g_s(\mathbf{x}) > 0$. We deduce that for $1 \leq k \leq s$, we have $g_k(\mathbf{x}) > \eta$. The latter inequality is strict because $\mathbf{x} \in \mathsf{R}\langle\zeta\rangle^n$ and the coefficients of g_k lies in $\mathsf{R}\langle\zeta\rangle\langle\eta\rangle$.

Since f is non-negative over $\mathsf{R}\langle\zeta\rangle^n$, there exists $\mathbf{x}_\varepsilon \in \operatorname{crit}(\pi_{i-1}, V_\varepsilon) \cap \mathbf{R}\langle\varepsilon\rangle^n$ such that $\lim_{\varepsilon \to 0} \mathbf{x}_\varepsilon = \mathbf{x}$, by Lemma 18. As a consequence, for $1 \leq k \leq s$ we have $g_k(\mathbf{x}_\varepsilon) \geq \eta$ (otherwise, using $\lim_{\varepsilon \to 0}$, this would contradict $\mathbf{x} \in U_\eta$). As a consequence, we have $\mathbf{x}_\varepsilon \in \operatorname{crit}(\pi_{i-1}, V_\varepsilon) \bigcap U_{\eta,\varepsilon}$. Finally, since

$\mathbf{x} \in (\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_{i-1}, V_\varepsilon)) \bigcap U$, it is at positive distance to the boundary of B. Since $\lim_{\varepsilon\to 0} \mathbf{x}_\varepsilon$ is $\mathbf{x}$, $\mathbf{x}_\varepsilon$ and $\mathbf{x}$ are infinitesimally close and $\mathbf{x}_\varepsilon$ lies in B_ε at positive distance from its boundary w.r.t ε. We conclude that there exists $\mathbf{x}_\varepsilon \in \mathrm{crit}(\pi_{i-1}, V_\varepsilon) \bigcap U_{\eta,\varepsilon} \bigcap B_\varepsilon$ which is a contradiction.

In the rest of the proof we can assume now that $\mathrm{crit}(\pi_{i-1}, V_\varepsilon) \bigcap U_\varepsilon \bigcap B_\varepsilon$ is not empty.
In the discussion preceding the correctness proof we considered the semi-algebraic set

$$\begin{aligned} A_\varepsilon = \{(\mathbf{x}, \mathbf{y}, z) \in \mathbf{R}\langle\varepsilon\rangle^{2n+1} \quad | \quad & \mathbf{x} \in (\mathrm{crit}(\pi_i, V_\varepsilon) - \mathrm{crit}(\pi_{i-1}, V_\varepsilon)) \bigcap U_{\eta,\varepsilon} \bigcap B_\varepsilon, \\ & \mathbf{y} \in \mathrm{crit}(\pi_{i-1}, V_\varepsilon) \bigcap U_{\eta,\varepsilon} \bigcap B_\varepsilon, \\ & ||x - y|| = z > 0\} \ . \end{aligned}$$

We can also describe A_ε as

$$A_\varepsilon = \{(\mathbf{x}, \mathbf{y}, z) \in \mathbf{R}\langle\varepsilon\rangle^{2n+1} | P_1(\mathbf{x}) \wedge P_2(\mathbf{y}) \wedge \frac{\partial f(\mathbf{X})}{\partial X_i} \neq 0 \wedge \|\mathbf{x} - \mathbf{y}\| > z^2 \wedge z > 0\} \ .$$

We refer to Steps 2 and 3 for the definitions of P_1 and P_2 and the polynomials that they involve.

If we replace the three infinitesimals ε, η, and ζ with three new variables e, h, and t respectively, in the formula Φ defined at Step 7, then we get polynomials $P_1(\mathbf{X}, e, h, t)$, $\frac{\partial f(\mathbf{X}, e, h, t)}{\partial X_i}$, and $P_2(\mathbf{Y}, e, h, t)$. In this way we define the following semi-algebraic set

$$A = \{(\mathbf{x}, \mathbf{y}, z, e, h, t) \in \mathsf{R}^{2n+4} \mid P_1(\mathbf{x}, e, h, t) \wedge P_2(\mathbf{y}, e, h, t) \wedge \frac{\partial f(\mathbf{X}, e, h, t)}{\partial X_i} \neq 0 \wedge \|\mathbf{x} - \mathbf{y}\| > z^2 \wedge z > 0\} \ .$$

By the definition of an extension (ext), see Section 2, of a semi-algebraic set we get

$$\pi_{\mathbf{x},\mathbf{y},z}\left(\mathrm{ext}(A, \mathbf{R}\langle\varepsilon\rangle) \bigcap \{e = \varepsilon, h = \eta, t = \zeta\}\right) = A_\varepsilon \subset \mathbf{R}\langle\varepsilon\rangle^n \ , \tag{1}$$

where $\pi_{\mathbf{x},\mathbf{y},\mathbf{z}} : (\mathbf{x}, \mathbf{y}, z, e, h, t) \mapsto (\mathbf{x}, \mathbf{y}, z)$. We deduce that

$$\pi_z(\pi_{\mathbf{x},\mathbf{yz}}(\mathrm{Ext}(A, \mathbf{R}\langle\varepsilon\rangle) \bigcap \{e = \varepsilon, h = \eta, t = \zeta\})) = \pi_z(A_\varepsilon) \ ,$$

where $\pi_z : (\mathbf{x}, \mathbf{y}, z) \mapsto z$.

The application of OneBlockQuantifierElimination at Φ (Step 7) actually computes a semi-algebraic formula defining $\pi_{z,e,h,t}(A)$. By (1) and the above discussion, one can conclude that substituting e, h and t by ε, η and ζ in this formula provides a semi-algebraic formula defining $\pi_z(A_\varepsilon)$.

Finally, we have to prove that indeed IsRealizable returns the correct answer. This means that the following formula is true:

$$\exists z \in \mathbf{R}, z > 0 \wedge z \in \lim_{\varepsilon\to 0} \pi_z(A_\varepsilon) \Leftrightarrow \left(\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_i, V_\varepsilon)\right) \bigcap U \neq \left(\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_{i-1}, V_\varepsilon)\right) \bigcap U \ ,$$

for some given value of $i \in \{2, \ldots, n\}$.

The if statement. If such a z exists, then there are distinct points $\mathbf{x}_\varepsilon, \mathbf{y}_\varepsilon$ in $\mathbf{R}\langle\varepsilon\rangle^n$ and $z_\varepsilon \in \mathbf{R}\langle\varepsilon\rangle$, such that $(\mathbf{x}_\varepsilon, \mathbf{y}_\varepsilon, z) \in A_\varepsilon$, that is

$$\begin{gathered} \mathbf{x}_\varepsilon \in (\mathrm{crit}(\pi_i, V_\varepsilon) - \mathrm{crit}(\pi_{i-1}, V_\varepsilon)) \bigcap U_{\eta,\varepsilon} \bigcap B_\varepsilon, \quad \mathbf{y}_\varepsilon \in \mathrm{crit}(\pi_{i-1}, V_\varepsilon) \bigcap U_{\eta,\varepsilon} \bigcap B_\varepsilon \ , \\ \text{and } \lim_{\varepsilon\to 0} ||\mathbf{x}_\varepsilon - \mathbf{y}_\varepsilon|| = z^2 > 0 \ . \end{gathered}$$

This means that $\mathbf{x}_\varepsilon$ and $\mathbf{y}_\varepsilon$ are not infinitesimally close, w.r.t. ε. Notice that, by definition of A_ε, $\mathbf{x}_\varepsilon$ and $\mathbf{y}_\varepsilon$ both lie in B_ε that is bounded over $\mathbf{R}$. Consequently, they are bounded over $\mathbf{R}$ and their limits as $\varepsilon \to 0$ exist. The limits as $\varepsilon \to 0$ are different and thus

$$\lim_{\varepsilon\to 0}\left(\mathrm{crit}(\pi_i, V_\varepsilon)\bigcap U_{\eta,\varepsilon}\bigcap B_\varepsilon\right) \neq \lim_{\varepsilon\to 0}\left(\mathrm{crit}(\pi_{i-1}, V_\varepsilon)\bigcap U_{\eta,\varepsilon}\bigcap B_\varepsilon\right),$$

because $\mathbf{x}_\varepsilon$ and $\mathbf{y}_\varepsilon$ are not infinitesimally close. Notice that $\lim_{\varepsilon\to 0}\mathbf{x}_\varepsilon$ lies in $\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_i, V_\varepsilon)$ and $U_\eta \subset \mathrm{ext}(U, \mathbf{R})$. Similarly $\lim_{\varepsilon\to 0}\mathbf{y}_\varepsilon$ lies in $\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_{i-1}, V_\varepsilon)$ and $U_\eta \subset \mathrm{ext}(U, \mathbf{R})$. Combining these inclusions with the fact that $\mathbf{x}_\varepsilon$ and $\mathbf{y}_\varepsilon$ are not infinitesimally close w.r.t ε, we conclude that

$$\left(\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_i, V_\varepsilon)\right)\bigcap U_\eta \neq \left(\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_{i-1}, V_\varepsilon)\right)\bigcap U_\eta \ .$$

The only if statement. Assume that

$$\left(\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_i, V_\varepsilon)\right)\bigcap U \neq \left(\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_{i-1}, V_\varepsilon)\right)\bigcap U \ .$$

We have to prove that there exists $(\mathbf{x}_\varepsilon, \mathbf{y}_\varepsilon, z_\varepsilon) \in A_\varepsilon$ and that $\lim_{\varepsilon\to 0}\|\mathbf{x}_\varepsilon - \mathbf{y}_\varepsilon\| = \lim_{\varepsilon\to 0} z_\varepsilon > 0$.

First, we prove the existence of $\mathbf{x}_\varepsilon$. Take $\mathbf{x} \in ((\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_i, V_\varepsilon))\bigcap U \setminus (\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_{i-1}, V_\varepsilon))\bigcap U)$. By noticing that $\mathbf{x} \in U_\eta$, we deduce that

$$\mathbf{x} \in \left((\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_i, V_\varepsilon))\bigcap U_\eta \setminus (\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_{i-1}, V_\varepsilon))\bigcap U_\eta\right) \ .$$

We claim that this implies that there exists $\mathbf{x}_\varepsilon \in \mathrm{crit}(\pi_i, V_\varepsilon)\bigcap U_{\eta,\varepsilon}$ such that

$$\mathbf{x} = \lim_{\varepsilon\to 0}\mathbf{x}_\varepsilon \in \left(\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_i, V_\varepsilon)\right)\bigcap U_\eta.$$

Indeed, since $\mathbf{x} \in \lim_{\varepsilon\to 0}\mathrm{crit}(\pi_i, V_\varepsilon)$ and f is non-negative over $\mathsf{R}\langle\zeta\rangle^n$, we deduce that there exists $\mathbf{x}_\varepsilon \in \mathrm{crit}(\pi_i, V_\varepsilon) \cap \mathbf{R}\langle\varepsilon\rangle^n$ with $\lim_{\varepsilon\to 0}\mathbf{x}_\varepsilon = \mathbf{x}$ (Lemma 18).

Moreover, $\mathbf{x} \in U_\eta$. But $\mathbf{x} \in \mathsf{R}\langle\zeta\rangle$ and the coefficients of the g_i's lie in $\mathsf{R}\langle\zeta\rangle$, thus $g_1(\mathbf{x}) > \eta, \ldots, g_s(\mathbf{x}) > \eta$. If there exists a k, $1 \leq k \leq s$, such that $g_k(\mathbf{x}_\varepsilon) \leq \eta$, then this would imply that $g_k(\lim_{\varepsilon\to 0}\mathbf{x}_\varepsilon) = g_k(\mathbf{x}) \leq \eta$. This contradicts the fact that $\mathbf{x} \in U_\eta$ and so $g_k(\mathbf{x}) > \eta$ for all k. We conclude that $\mathbf{x}_\varepsilon \in U_{\eta,\varepsilon}$ and so $\mathbf{x}_\varepsilon \in \mathrm{crit}(\pi_i, V_\varepsilon)\bigcap U_{\eta,\varepsilon}$ as we claimed.

We also deduce that $\mathbf{x}_\varepsilon \notin \mathrm{crit}(\pi_{i-1}, V_\varepsilon)\bigcap U_{\eta,\varepsilon}$. Since in this case

$$\mathbf{x} = \lim_{\varepsilon\to 0}\mathbf{x}_\varepsilon \in \left(\lim_{\varepsilon\to 0}\mathrm{crit}(\pi_{i-1}, V_\varepsilon)\right)\bigcap U \ ,$$

which is a contradiction. Thus, there exists $\mathbf{x}_\varepsilon \in (\mathrm{crit}(\pi_i, V_\varepsilon) - \mathrm{crit}(\pi_{i-1}, V_\varepsilon))\bigcap U_{\eta,\varepsilon}\bigcap B_\varepsilon$. The inclusion $\mathbf{x}_\varepsilon \in B_\varepsilon$ is a direct consequence of the fact that B_ε strictly contains the semi-algebraic set under consideration.

Now we prove the existence of $\mathbf{y}_\varepsilon$. Recall that $\mathbf{x}$ is obtained as the limit of $\mathbf{x}_\varepsilon$ that it is not infinitesimally close, w.r.t ε, to any point of the set $\mathrm{crit}(\pi_{i-1}, V_\varepsilon)$. By the assumption that $\mathrm{crit}(\pi_{i-1}, V_\varepsilon)\bigcap U_{\eta,\varepsilon}$ is not empty, there exists $\mathbf{y}_\varepsilon \in \mathrm{crit}(\pi_{i-1}, V_\varepsilon)\bigcap U_{\eta,\varepsilon}$ that is not infinitesimally close to $\mathbf{x}_\varepsilon$, w.r.t. ε.

As there exist $\mathbf{x}_\varepsilon$ and $\mathbf{y}_\varepsilon$ that are not infinitesimally close w.r.t. ε, there exists $z_\varepsilon \in \mathbf{R}\langle\varepsilon\rangle$ such that $z_\varepsilon > 0$ and $\|\mathbf{x}_\varepsilon - \mathbf{y}_\varepsilon\|^2 > z_\varepsilon^2$ and $\lim_{\varepsilon\to 0} z_\varepsilon > 0$.

Complexity analysis. When DisjointPolar is called with $i = 1$ its run time is the one of LimitsOfOfCriticalPoints. By Lemma 16, Step 1 costs $(s\,D)^{O(n)}$ arithmetic operations.

Now we assume that $i \geq 2$. Steps 2-3 and Step 6 are symbolic manipulations which produce Boolean combinations of $O(s)$ polynomials of total degree $2D$ involving $O(n)$ variables.

By Lemma 11, Step 4 costs at most $(s\,D)^{O(n)}$ arithmetic operations.

The complexity of one-block quantifier elimination at Step 7 is $(s\,D)^{O(n)}$ (Theorem 14).

The output of the quantifier elimination procedure consists of $(s\,D)^{O(n)}$ conjunctions of polynomials in $\mathsf{Z}[\zeta, \eta, Z][\varepsilon]$ of degree at most $D^{O(n)}$. Each conjunction involves at most $(s\,D)^{O(n)}$ polynomials.

After we apply UnivariateLimit (Step 9) we check if there is a realizable sign condition. According to Lemma 15 this costs $(s\,D)^{O(n)}$ arithmetic operations.

We call IsRealizable at most $(s\,D)^{O(n)}$ times (which is the number of conjunctions and thus the cardinality of $\widetilde{\Psi}$). Each call involves $(s\,D)^{O(n)}$ polynomials in $\mathsf{Z}[\zeta, \eta, Z]$ of degree at most $D^{O(n)}$ (Lemma 17). The arithmetic cost is $(s\,D^{O(n)})^{O(1)} = (s\,D)^{O(n)}$ (Sec. 5.2) which is also the cost for the whole for-loop and the algorithm.

Statements on bit complexity when $\mathsf{Z} = \mathbb{Z}$ are straightforward applying *mutatis mutandis* the same reasoning as above and using bit complexity results given in Theorem 14, and Lemmata 15, 16, and 17. □

5.3 Proofs of subroutines

Proof of Lemma 11 . We decide the emptiness of $V \bigcap U$ using the algorithm from [50, Proposition 2.2]. The cost is $(s\,\delta)^{O(n)}$ operations in Z. The Boolean complexity bound follows by combining [50, Proposition 2.2] with [13, Algorithm 13.1]. □

Proof of Lemma 15 . The quantifier free formula of the input represents the following semi-algebraic set

$$\mathcal{S}_\varepsilon = \{z \in \mathsf{R}\langle\zeta\rangle\langle\eta\rangle\langle\varepsilon\rangle \mid \Psi\} \ ,$$

where Ψ is a Boolean formula whose atoms are polynomials in Z with coefficients in $\mathsf{R}\langle\zeta\rangle\langle\eta\rangle\langle\varepsilon\rangle$. We can express the limit of $\mathcal{S}_\varepsilon$ as $\varepsilon \to 0$, $\mathcal{S}$, using the language of the first order theory over the reals [13, Sec. 3.1], that is

$$\mathcal{S} = \lim_{\varepsilon \to 0} \mathcal{S}_\varepsilon = \{z' \in \mathsf{R}\langle\zeta\rangle\langle\eta\rangle \mid (\forall r > 0)(\exists \varepsilon_0 > 0)(\forall \varepsilon)\,(\forall z)\, z \in \mathcal{S} \wedge (0 < \varepsilon < \varepsilon_0 \Rightarrow \|z - z'\|^2 < r^2)\} \ .$$

In this way, to compute the limit it suffices to eliminate the quantifiers from the previous formula.

For the elimination process, we treat ζ as a variable. To see that this is valid let Φ be the Boolean formula the describes $z \in \mathcal{S} \wedge (0 < \varepsilon < \varepsilon_0 \Rightarrow \|z - z'\|^2 < r^2)$. Then

$$A_{\zeta,\eta} = \{(z, z', r, \varepsilon_0, \varepsilon) \in \mathsf{R}\langle\zeta\rangle\langle\eta\rangle^5 \mid \Phi\} \ .$$

If we let $\zeta = t$ and $\eta = h$ in all the polynomials in Φ, then we get the set

$$A = \{\{(z, z', r, \varepsilon_0, \varepsilon, t, h) \in \mathsf{R}^6 \mid \Phi\}\} \ .$$

In this way

$$\pi_{-t}(\mathrm{ext}(A, \mathsf{R}\langle\zeta\rangle\langle\eta\rangle) \bigcap \{t = \zeta, h = \eta\}) = A_{\zeta,\eta} \subset \mathsf{R}\langle\zeta\rangle\langle\eta\rangle^5 \ ,$$

where π_{-th} is the projection $(z, z', r, \varepsilon_0, \varepsilon, t, h) \mapsto (z, z', r, \varepsilon_0, \varepsilon)$.

We notice that $\mathcal{S}$ is defined using a constant number of free variables, (ζ, η, and Z'), a constant number of quantified variables, (z, r, ε_0, ε), and a constant number of quantifier alternations. Following [13, Theorem 14.16], after we perform quantifier elimination, the output is a quantifier-free formula $\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} h_{i,j} \rhd_{i,j} 0$, where $h_{i,j} \in \mathsf{Z}[\zeta, \eta][Z']$ have degree at most $\delta^{O(1)}$, $I \leq (\ell\,\delta)^{O(1)}$, $J_i \leq (\ell\,\delta)^{O(1)}$, and the complexity of the quantifier elimination procedure is $(\ell\,\delta)^{O(1)}$ arithmetic operations in Z.

If $\mathsf{Z} = \mathbb{Z}$ and the input polynomials have coefficients of maximum bit size τ, then the Boolean complexity is $\tau\,(\ell\,\delta)^{O(1)}$. □

Proof of Lemma 16 . By assumption, $\mathrm{crit}(\pi_1, V_\varepsilon)$ is finite and H is non-negative over $\mathsf{R}\langle\zeta\rangle^n$. Thus, to compute $(\lim_{\varepsilon\to 0} \mathrm{crit}(\pi_1, V_\varepsilon)) \bigcap U$ it is sufficient to

(1) compute sample points in each connected component of $\mathrm{crit}(\pi_1, V_\varepsilon) \cap \mathsf{R}\langle\zeta\rangle\langle\varepsilon\rangle^n$; they will be encoded with a rational parametrization with coefficients in $\mathsf{Z}[\zeta, \varepsilon]$

$$q(T) = 0, X_1 = q_1(T)/q_0(T), \ldots, X_n = q_n(T)/q_0(T);$$

(2) use this parametrization to compute their limits and make the intersection with U.

The above parametrization is obtained using [13, Algorithm 13.1] with input $H - \varepsilon = \frac{\partial H}{\partial X_2} = \cdots = \frac{\partial H}{\partial X_n} = 0$. Following *mutatis mutandis* the same reasoning as in [50, Proposition 2.2], we deduce that the arithmetic cost in Z of this step is $(s\,\delta)^{O(n)}$.

Step (2) is performed using with [13, Algorithm 11.20] (Removal of an infinitesimal) for compute the limit of the sample points as $\varepsilon \to 0$ and sign determination algorithms for univariate polynomials to obtain the intersection with U (see [13, Algorithm 10.13]). The overall complexity is $(s\,\delta)^{O(n)}$ operations in Z [13, Chapters 10 and 11].

The Boolean complexity bound is straightforward from the above reasoning. □

Proof of Lemma 17 . The subroutine is based on Algorithm 10.13 from [13]. If the degree of the polynomials is at most δ and if there are at most ℓ polynomials, then the total cost is $\ell\,\delta^{O(1)}$ arithmetic operations in $\mathsf{Z}[\zeta, \eta]$ [13].

The operations that we need are computations of subresultant sequences for univariate polynomials in Z with coefficients in $\mathsf{Z}[\zeta, \eta]$. The coefficients of the polynomials in the sequence have degree at most $\delta^{O(1)}$ in ζ and η [13, Proposition 8.49]. Therefore the complexity of the algorithm is also $\ell\,\delta^{O(1)}$, when we count operations in Z.

The Boolean complexity is $\tau\,\ell\,\delta^{O(1)}$ and it is due to the bit size of the integers that appear in the subresultant sequence. □

Acknowledgments

Both authors are partially supported by the EXACTA grant of the National Science Foundation of China (NSFC 60911130369) and the French National Research Agency (ANR-09-BLAN-0371-01), GeoLMI (ANR 2011 BS03 011 06), HPAC (ANR ANR-11-BS02-013). Safey El Din is partially supported by the Institut Universitaire de France. Elias Tsigaridas is partially supported by an FP7 Marie Curie Career Integration Grant.

References

[1] S. Arora, R. Ge, R. Kannan, and A. Moitra. Computing a nonnegative matrix factorization–provably. In *Proceedings of the 44th symposium on Theory of Computing*, pages 145–162. ACM, 2012.

[2] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*, volume 19. Addison-Wesley Reading, MA, 1969.

[3] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real equation solving: the hypersurface case. *Journal of Complexity*, 13(1):5–27, 1997.

[4] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties: geometry and algorithms. *Journal of Complexity*, 21(4):377–412, 2005.

[5] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and E. Schost. On the geometry of polar varieties. *Applicable Algebra in Engineering, Communication and Computing*, 2010.

[6] S. Barone and S. Basu. Refined bounds on the number of connected components of sign conditions on a variety. *Discrete & Computational Geometry*, 47(3):577–597, 2012.

[7] S. Barone and S. Basu. Refined bounds on the number of connected components of sign conditions II. *arXiv preprint arXiv:1303.1577*, 2013.

[8] S. Basu. On bounding the Betti numbers and computing the Euler characteristic of semi-algebraic sets. In *Proc. 28-th annual ACM Symposium on Theory of Computing*, pages 408–417. ACM, 1996.

[9] S. Basu. Computing the first few Betti numbers of semi-algebraic sets in single exponential time. *Journal of Symbolic Computation*, 41(10):1125–1154, 2006.

[10] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets (extended abstract). In *STOC*, pages 168–173. ACM, 1996.

[11] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43(6):1002–1045, Nov. 1996.

[12] S. Basu, R. Pollack, and M.-F. Roy. Computing the first Betti number and the connected components of semi-algebraic sets. In *Proc. 37-th annual ACM Symposium on Theory of Computing*, pages 304–312. ACM, 2005.

[13] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, second edition, 2006. http://perso.univ-rennes1.fr/marie-francoise.roy/bpr-ed2-posted2.pdf.

[14] S. Basu, R. Pollack, and M.-F. Roy. Computing the dimension of a semi-algebraic set. *Journal of Mathematical Sciences*, 134:2346–2353, 2006.

[15] S. Basu and M.-F. Roy. Bounding the radii of balls meeting every connected component of semi-algebraic sets. *Journal of Symbolic Computation*, 45(12):1270–1279, 2010.

[16] L. Blum, M. Shub, and S. Smale. On a theory of computation over the real numbers; NP completeness, recursive functions and universal machines. In *Proc. 29th Annual Symposium on Foundations of Computer Science*, pages 387–397. IEEE, 1988.

[17] L. E. Blume and W. R. Zame. The algebraic geometry of perfect and sequential equilibrium. *Econometrica: Journal of the Econometric Society*, pages 783–794, 1994.

[18] J. Bochnak, M. Coste, and M.-F. Roy. *Géométrie algébrique réelle*, volume 12. Springer, 1987.

[19] J. Bochnak, M. Coste, and M.-F. Roy. *Real algebraic geometry*, volume 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, 1998.

[20] J. Canny. *The complexity of robot motion planning*. PhD thesis, MIT, 1987.

[21] K. Chatterjee, R. Majumdar, and T. Henzinger. Stochastic limit-average games are in EXPTIME. *Int. J. of Game Theory*, 37(2):219–234, 2008.

[22] A. Chistov, H. Fournier, L. Gurvits, and P. Koiran. Vandermonde matrices, NP-completeness, and transversal subspaces. *Foundations of Computational Mathematics*, 3(4):421–427, 2003.

[23] A. L. Chistov. Polynomial-time computation of the dimension of algebraic varieties in zero-characteristic. *Journal of Symbolic Computation*, 22(1):1–25, 1996.

[24] G. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. In *Automata Theory and Formal Languages*, pages 134–183. Springer, 1975.

[25] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.

[26] M. Giusti and J. Heintz. La détermination de la dimension et des points isolées dune variété algébrique peuvent s effectuer en temps polynomial. In *Computational Algebraic Geometry and Commutative Algebra, Cortona*, volume 34, pages 216–256, 1991.

[27] M. Golubitsky, V. Guillemin, and M. Golubitsky. *Stable mappings and their singularities*, volume 1. Springer Berlin, 1973.

[28] D. Y. Grigor'ev. Complexity of deciding tarski algebra. *Journal of symbolic Computation*, 5(1):65–108, 1988.

[29] D. Y. Grigor'ev and N. V. Jr. Solving systems of polynomial inequalities in subexponential time. *Journal of Symbolic Computation*, 5(12):37 – 64, 1988.

[30] L. Guth and N. H. Katz. Algebraic methods in discrete analogs of the Kakeya problem. *Advances in Mathematics*, 225(5):2828–2839, 2010.

[31] K. A. Hansen, M. Koucky, N. Lauritzen, P. B. Miltersen, and E. P. Tsigaridas. Exact algorithms for solving stochastic games. In *Proc. 43rd annual ACM Symposium on Theory of Computing*, pages 205–214. ACM, 2011.

[32] J. Heintz, M.-F. Roy, and P. Solernó. Single exponential path finding in semi-algebraic sets II: The general case. In *Algebraic geometry and its applications, collections of papers from Abhyankar's 60-th birthday conference*. Purdue University, West-Lafayette, 1994.

[33] Q. Jin and T. Yang. Overconstraint analysis on spatial 6-link loops. *Mechanism and machine theory*, 37(3):267–278, 2002.

[34] H. Kaplan, J. Matousek, and M. Sharir. Simple proofs of classical theorems in discrete geometry via the guth–katz polynomial partitioning technique. *Discrete & Computational Geometry*, pages 1–19, 2011.

[35] P. Koiran. Randomized and deterministic algorithms for the dimension of algebraic varieties. In *Proc. 38th Annual Symposium on Foundations of Computer Science.*, pages 36–45. IEEE, 1997.

[36] P. Koiran. The Real Dimension Problem is $\mathrm{NP}_{\mathbb{R}}$-complete. *Journal of Complexity*, 15(2):227–238, 1999.

[37] A. Logar. A computational proof of the Noether normalization lemma. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 259–273, 1989.

[38] A. Moitra. An almost optimal algorithm for computing nonnegative rank. In *SIAM Symposium on Discrete Algorithms*, pages 1454–1464, 2012.

[39] A. Neyman. Real algebraic tools in stochastic games. In *Stochastic Games and Applications*, pages 57–75. Springer, 2003.

[40] M. Raghavan and B. Roth. Inverse kinematics of the general 6r manipulator and related linkages. *Journal of Mechanical Design*, 115:502, 1993.

[41] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. Part I: Introduction. preliminaries. the geometry of semi-algebraic sets. the decision problem for the existential theory of the reals. *Journal of Symbolic Computation*, 13(3):255 – 299, 1992.

[42] F. Rouillier, M.-F. Roy, and M. Safey El Din. Finding at least one point in each connected component of a re al algebraic set defined by a single equation. *Journal of Complexity*, 16:716–750, 2000.

[43] M. Safey El Din and E. Schost. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete and Computational Geometry*, 45(1):181–220, 2011.

[44] J. T. Schwartz and M. Sharir. On the piano movers' problem I. the case of a two dimensional rigid polygonal body moving amidst polygonal barriers. *Communications on pure and applied mathematics*, 36(3):345–398, 1983.

[45] J. T. Schwartz and M. Sharir. On the piano movers' problem II. general techniques for computing topological properties of real algebraic manifolds. *Advances in applied Mathematics*, 4(3):298–351, 1983.

[46] I. Shafarevich. *Basic Algebraic Geometry 1*. Springer Verlag, 1977.

[47] J. Solymosi and T. Tao. An incidence theorem in higher dimensions. *Discrete & Computational Geometry*, pages 1–26, 2012.

[48] W. Szczechla, S. Connell, J. A. Filar, and O. Vrieze. On the puiseux series expansion of the limit discount equation of stochastic games. *SIAM journal on control and optimization*, 35(3):860–875, 1997.

[49] A. Tarski. *A decision method for elementary algebra and geometry.* University of California Press, 1951.

[50] N. Vorobjov. Complexity of computing the local dimension of a semialgebraic set. *J. Symb. Comput.*, 27(6):565–579, 1999.