Discrete Comput Geom 32:417–430 (2004)
DOI: 10.1007/s00454-004-1107-5

Discrete & Computational
Geometry

© 2004 Springer-Verlag New York, LLC

Properness Defects of Projections and Computation of at Least One Point in Each Connected Component of a Real Algebraic Set

Mohab Safey El Din[1] and Éric Schost[2]

[1]LIP6, Université Paris 6,
75015 Paris, France
Mohab.Safey@lip6.fr

[2]STIX, École Polytechnique,
Palaiseau, France
Eric.Schost@polytechnique.fr

Abstract. Computing at least one point in each connected component of a real algebraic set is a basic subroutine to decide emptiness of semi-algebraic sets, which is a fundamental algorithmic problem in effective real algebraic geometry. In this article we propose a new algorithm for the former task, which avoids a hypothesis of properness required in many of the previous methods. We show how studying the set of non-properness of a linear projection Π enables us to detect the connected components of a real algebraic set without critical points for Π. Our algorithm is based on this observation and its practical counterpoint, using the triangular representation of algebraic varieties. Our experiments show its efficiency on a family of examples.

1. Introduction

Finding at least one point in each connected component of a semi-algebraic set, or at least deciding if it is empty, is a fundamental problem in effective real algebraic geometry, which appears in many academic or industrial applications: filter banks [20], robotics [34], celestial mechanics, etc. A well known algorithm having such an output is Collins' Cylindrical Algebraic Decomposition algorithm [14]. It has complexity doubly exponential in the number of variables, in terms of arithmetic operations and size of the output. In practice, the best implementations are limited to problems having about five variables.

More recently, alternative algorithms were proposed in [25]–[27] and [9]–[11], with complexity single exponential in the number of variables. These algorithms reduce this question to the computation of at least one point in each connected component of several *real algebraic sets*. Thus, designing efficient algorithms for this last question is crucial to deal with inequalities efficiently. This paper is in keeping with this framework.

The Critical Point Method. We first briefly describe the state of the art for the latter problem. A widely used method is the critical point method. It consists in studying a map that reaches an extremum on each connected component of the real algebraic set under consideration, and whose critical locus is zero-dimensional.

In [25]–[27] and [9]–[11] the authors reduce the general case to the study of smooth and compact real algebraic sets, via several infinitesimal deformations. Indeed, any projection on a straight line reaches an extremum on each connected component of a compact real algebraic set. The above articles show how to choose a projection with zero-dimensional critical locus; this yields algorithms with complexities that are single exponential in the number of variables.

A similar approach is studied in [6] and [5], [7] respectively for smooth compact hypersurfaces and smooth compact complete intersections. In both cases the critical points of the projection on a generic line are shown to belong to a family of formal polar varieties. Studying these polar varieties allows them to define a notion of intrinsic geometric degree for real algebraic systems. The resulting algorithms are based on the representation of polynomials by straight-line programs; they have a complexity polynomial in both the intrinsic geometric degree and the complexity of evaluation of the input system. Recently, these results were extended to handle the case of non-compact, smooth varieties in [50] and [8].

In [44], [4] and [48] the authors utilize the square of the distance to a given point; such functions are simply called *distance functions* in what follows. In [44] the singular case is treated by a single infinitesimal deformation, while in [4] it is treated by iteratively studying the real points of the singular locus. No complexity estimate is given in either [44] or [4]. Nevertheless, an extensive family of examples was studied in [45]; on these examples the iterative approach of [4] performed better than the one using an infinitesimal deformation.

Several of the algorithms mentioned above require isolating the real solutions of zero-dimensional polynomial systems. Many solutions exist for this question; for completeness, we briefly review some of them.

A commonly used solution is the computation of a Gröbner basis [13], [19], [16], [17], possibly followed by the computation of a Rational Univariate Representation [1], [42]. We also mention the work of Giusti and collaborators [21]–[24], which culminated in the design of the algorithm of geometric resolution, whose real counterpart was mentioned above. Through such approaches, isolating the real solutions of a zero-dimensional system is reduced to studying the real roots of a univariate polynomial. For handling this task, refer to [53], [47] and [46]. We also mention the algorithms based on triangular sets, see [33], [32], [55], [31], [39], [38], [2] and [56] for a panoramic survey; the arithmetic of the real algebraic numbers of [41] is well adapted to this representation. Finally, symbolic-numeric techniques can also be used, see [15], [54] and references therein.

Projection Functions in the Non-Compact Case. The above algorithms detect the connected components of a real algebraic set by the presence of critical points, which are characterized by the vanishing of suitable minors of jacobian matrices. Two approaches were considered, using either distance functions or projections; it turns out that both suffer practical difficulties.

On the one hand, the degrees of the minors arising when using a distance function limit the performance of the algorithm designed in [4]. This makes it desirable to use projection functions in the first place, since the jacobian determinants characterizing the critical locus of a projection have better properties, see the discussion in Section 5.

On the other hand, algorithms using projections apply only to compact varieties: already simple examples like hyperbolas show that some projections may have no critical points on non-compact varieties. Yet, the reduction of the general case to the compact situation by infinitesimal deformations burdens the algorithms of [25]–[27] and [9]–[11], so that the practical performances of these algorithms do not reflect their good complexity.

Thus, using projection functions without compactification could lead to significant practical improvements. Our contribution in this article is to study such projections in the presence of non-compact connected components. From this geometric study, we deduce a new algorithm for the computation of a finite set of points that meets each connected component of a real algebraic set. Our first experiments show a promising behavior.

The Set of Properness of a Dominant Map. We use the notion of *properness* of a map, which we now introduce, together with the notion of a *dominant* map. Let $f : V \to W$ be a map of topological spaces. The map f is *proper* at $w \in W$ if there is a neighborhood B of w such that $f^{-1}(\overline{B})$ is compact, where $\overline{B}$ denotes the closure of B. In this article we consider maps between complex or real algebraic varieties. The notion of properness will be relative to the topologies induced by the metric topologies of $\mathbb{C}$ or $\mathbb{R}$.

Next, a map of irreducible complex varieties $f : V \to W$ is *dominant* if its image is dense in W, i.e. if the dimension of $f(V)$ as a complex constructible set equals the dimension of W. We extend this definition to the case of a map $V \to W$, where V is not necessarily irreducible. Then we require that the restriction of f to each irreducible component of V be dominant.

Let now $V \subset \mathbb{C}^n$ be an algebraic variety of dimension d and let $\Pi : V \to \mathbb{C}^d$ be a dominant projection. Then by the theorem of dimension of fibers [52, Chapter 1.6], Π has generically finite fibers. In this situation the set of points of $\mathbb{C}^d$ at which f is not proper is a hypersurface [30]; we denote by P_Π a square-free polynomial defining it. Our first result shows how P_Π can be used to obtain at least one point on each connected component of $V \cap \mathbb{R}^n$.

Theorem 1. *Let $V \subset \mathbb{C}^n$ be an equidimensional algebraic variety of dimension d. Let Π be the projection*:

$$\begin{array}{cccc} \Pi : & \mathbb{C}^n & \to & \mathbb{C}^d, \\ & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_d). \end{array}$$

Suppose that the restriction of Π to V is dominant and let P_Π be as above. Let D be a connected component of $V \cap \mathbb{R}^n$, such that D contains no singular point of V, and no critical point for Π. Then there exists a connected component of the semi-algebraic set defined by $P_\Pi \neq 0$ which is contained in $\Pi(D)$.

As a consequence, given a variety $V \subset \mathbb{C}^n$ and a projection Π satisfying the assumptions of Theorem 1, the connected components of $V \cap \mathbb{R}^n$ can be reached by (i) detecting the connected components which contain either singular points or critical points for Π; (ii) for all other connected components, computing at least one point in each connected component of $P_\Pi \neq 0$; and, given such a point y, studying the fiber $V \cap \Pi^{-1}(y)$.

To implement this idea, we use an adapted representation of algebraic sets, the *triangular set* representation.

Triangular Sets. The following definitions come from [3], [2], [38] and [37]; for a detailed survey of such notions, refer to [29]. This representation was already used in the article [4], in a similar context of real algebraic geometry.

Consider a lexicographic order on some variables $X_1, \ldots, X_n$. Given a non-constant polynomial P in $\mathbb{Q}[X_1, \ldots, X_n]$, we call *main variable* of P and denote by $\mathrm{mvar}(P)$ the greatest variable appearing in P with respect to this order. With these notations, a family $\mathcal{T} = (t_{d+1}, \ldots, t_n)$ of non-constant polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ is a *triangular set* iff $\mathrm{mvar}(t_i) \neq \mathrm{mvar}(t_j)$ for $t_i \neq t_j$. The *algebraic variables* are the main variables of the polynomials in $\mathcal{T}$; the other variables are called *transcendental*. The *initial* of a polynomial P is its leading coefficient, when P is considered as univariate in its main variable. The *separant* of P is the polynomial $\partial P / \partial \mathrm{mvar}(P)$.

Let $\mathcal{T}$ be a triangular set and let h be the product of its initials. The *saturated ideal* of $\mathcal{T}$ is the saturation of $\mathcal{T}$ with respect to h:

$$\mathrm{sat}(\mathcal{T}) = \langle \mathcal{T} \rangle : h^\infty = \{P \in \mathbb{Q}[X_1, \ldots, X_n] \mid \exists n \in \mathbb{N},\ h^n P \in \langle \mathcal{T} \rangle\}.$$

The *quasi-component* of $\mathcal{T}$ is the constructible set $W(\mathcal{T}) = V(\mathcal{T}) \backslash V(h)$. Thus the zero-set of $\mathrm{sat}(\mathcal{T})$ is the Zariski closure of $W(\mathcal{T})$, denoted by $\overline{W(\mathcal{T})}$.

A triangular set $\mathcal{T}$ is *regular* if, for i in $\{d+1, \ldots, n\}$, the initial h_i of t_i does not divide zero in $\mathbb{Q}[X_1, \ldots, \mathrm{mvar}(t_{i-1})]/\mathrm{sat}(t_{d+1}, \ldots, t_{i-1})$. A regular triangular set $\mathcal{T}$ is *separable* if, for i in $\{d+1, \ldots, n\}$, the separant s_i does not divide zero in $\mathbb{Q}[X_1, \ldots, \mathrm{mvar}(t_i)]/\mathrm{sat}(t_{d+1}, \ldots, t_i)$. A regular and separable triangular set $\mathcal{T}$ is *strongly normalized* if for i in $\{d+1, \ldots, n\}$, h_i depends only on the transcendental variables of $\mathcal{T}$.

The following two results show that such triangular sets provide a useful tool for our initial question. The first fundamental fact is proved in [37]: if $(P_1, \ldots, P_k)$ is any family of polynomials, there exists strongly normalized triangular sets $\mathcal{T}_1, \ldots, \mathcal{T}_\ell$ such that the equality $V(P_1, \ldots, P_k) = \bigcup_{i=1}^{\ell} \overline{W(\mathcal{T}_i)}$ holds. Thus, we can concentrate on the case of a variety given as the closure of the quasi-component of a strongly normalized triangular set. Then the second important fact is the translation of Theorem 1 to this context.

Theorem 2. *Let $\mathcal{T} \subset \mathbb{Q}[X_1, \ldots, X_n]$ be a strongly normalized triangular set with transcendental variables $X_1, \ldots, X_d$. Let Π be the projection*:

$$\begin{array}{cccc} \Pi : & \mathbb{C}^n & \to & \mathbb{C}^d, \\ & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_d), \end{array}$$

and let s and h be the product of respectively the separants and the initials of $\mathcal{T}$. Let $\overline{W(\mathcal{T})}$ be the Zariski closure of $W(\mathcal{T})$ and let D be a connected component of $\overline{W(\mathcal{T})} \cap \mathbb{R}^n$.

If $D \cap V(s)$ is empty, then there exists a connected component of the semi-algebraic set defined in $\mathbb{R}^d$ by $h \neq 0$ which is contained in $\Pi(D)$.

This theorem is the key to our algorithm; given $P_1, \ldots, P_k$ in $\mathbb{Q}[X_1, \ldots, X_n]$, this algorithm returns zero-dimensional systems whose set of real roots intersects each connected component of $V(P_1, \ldots, P_k) \cap \mathbb{R}^n$. We first compute a decomposition in strongly normalized triangular sets of the complex variety $V(P_1, \ldots, P_k)$. Then we apply Theorem 2 to each of these triangular sets: the connected components of the closure of its quasi-component are reached by studying both the intersection with the zero-set of the separants, and the hypersurface defined by the initials.

Complexity Issues and Practical Performances. In this paper we do not give complexity results. The crucial problem is to bound the geometric degree of the intermediate varieties appearing in the algorithm. Indeed, these varieties describe nested singular loci; the crudest upper bound on their degrees is doubly exponential in the number of variables. On the other hand, we are not aware of any lower bound for this question. Thus, the complexity of our algorithm in terms of size of the output is still a largely open problem, which should be solved before estimating its arithmetic complexity.

Our algorithm requires treating a semi-algebraic problem: computing at least one point in each connected component of a real semi-algebraic set defined by $P \neq 0$, with P in $\mathbb{Q}[X_1, \ldots, X_d]$. There exist algorithms with single exponential complexity for this task, see [25]–[27] and [9]–[11]. Yet, it is far from obvious to obtain an efficient implementation of such algorithms. For our first experiments, we found it better to use the projection step of the Cylindrical Algebraic Decomposition algorithm [14].

On the practical side, we compared our algorithm with the ones from [4] and [44], as well as with an implementation of the Cylindrical Algebraic Decomposition. These problems come mostly from academic or industrial applications of the FRISCO test-suite [12]. On almost all these tests, our algorithm ran faster than all other ones; we can also solve problems that were out of the reach of those algorithms.

Finally, we mention that an implementation of the algorithm presented here is available in the RAGLib library [49].

2. Proof of Theorem 1

Let $V \subset \mathbb{C}^n$ be an equidimensional variety and let Π be the projection:

$$\begin{array}{rccc} \Pi: & \mathbb{C}^n & \to & \mathbb{C}^d, \\ & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_d). \end{array}$$

Suppose that the restriction of Π to V is dominant. Let D be a connected component of $V \cap \mathbb{R}^n$ without singular point nor critical point for Π and let P_Π be a polynomial defining the set at which Π is not proper. Then Theorem 1 states that there exists a connected component S of the semi-algebraic set defined by $P_\Pi \neq 0$ contained in $\Pi(D)$.

We denote by U the image $\Pi(D)$. The proof of Theorem 1 uses the following classical result on the properness defects of a continuous map.

Lemma 1. *For all α in $\overline{U}\backslash U$, Π restricted to D is not proper at α.*

Proof. Let α be in $\overline{U}\backslash U$, and suppose that Π is proper at α. Then there exists an open set $B \subset \mathbb{R}^d$ containing α such that $\Pi^{-1}(\overline{B})$ is compact, where $\overline{B}$ is the closure of B for the metric topology. This implies that $U \cap \overline{B} = \Pi(\Pi^{-1}(\overline{B}) \cap D)$ is compact, hence closed. This contradicts the fact that α is in $\overline{U}\backslash U$. □

We can now prove Theorem 1. Let y be in U and let x be in D, such that $\Pi(x) = y$. By assumption, x is neither a critical point of Π restricted to V nor a singular point of V. Thus, from the implicit function theorem, there exists a neighborhood B of y included in $U = \Pi(D)$, so U is open. We then deduce that there exists a connected component S of $P_\Pi \neq 0$, such that $U \cap S \neq \emptyset$. Let us show that $S \subset U$, which will conclude the proof.

Indeed, suppose on the contrary that there exist $y_1 \in U \cap S$ and $y_2 \in S\backslash U$ and let $\gamma \subset S$ be a continuous path linking y_1 and y_2. Since U is open, there exists $y_0 \in \gamma$ such that $y_0 \in \overline{U}\backslash U$. From Lemma 1, Π restricted to V is not proper at y_0. Thus $P_\Pi(y_0) = 0$, which contradicts the fact that y_0 is in S. □

3. Proof of Theorem 2

Let $\mathcal{T} \subset \mathbb{Q}[X_1, \ldots, X_n]$ be a strongly normalized triangular set, with transcendental variables $X_1, \ldots, X_d$. Let Π be the projection:

$$\begin{array}{cccc} \Pi : & \mathbb{C}^n & \to & \mathbb{C}^d, \\ & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_d), \end{array}$$

and let s and h be the product of respectively the separants and the initials of $\mathcal{T}$. Let $\overline{W(\mathcal{T})}$ be the Zariski closure of $W(\mathcal{T})$ and let D be a connected component of $\overline{W(\mathcal{T})} \cap \mathbb{R}^n$. If $D \cap V(s)$ is empty, then Theorem 2 asserts that there exists a connected component S of the semi-algebraic set defined by $h \neq 0$ such that S is contained in $\overline{\Pi(D)}$.

Proving Theorem 2 requires us to relate the singular points of $\overline{W(\mathcal{T})}$, the critical points of Π on $\overline{W(\mathcal{T})}$ and the set of non-properness of Π to respectively the separants and the initials of $\mathcal{T}$. We use a series of intermediate results; the first of them is proved in [3] and [40].

Lemma 2. *$\overline{W(\mathcal{T})}$ is equidimensional of dimension d, and $\overline{W(\mathcal{T})} \cap V(s)$ has dimension less than d. The restriction of Π to $\overline{W(\mathcal{T})}$ is dominant.*

Lemma 3. *The singular points of $\overline{W(\mathcal{T})}$ and the critical points of Π on $\overline{W(\mathcal{T})}$ are included in $\overline{W(\mathcal{T})} \cap V(s)$.*

Proof. Let $\mathcal{S}$ be a finite family generating $\mathrm{sat}(\mathcal{T})$, so that $\{\mathcal{T}, \mathcal{S}\}$ also generates $\mathrm{sat}(\mathcal{T})$. From Lemma 2, this ideal is radical and equidimensional of dimension d [3], so the singular locus of $\overline{W(\mathcal{T})}$ is contained in the zero-set of the $n - d \times n - d$ minors of the jacobian of $\{\mathcal{T}, \mathcal{S}\}$. The product s of the separants of $\mathcal{T}$ appears as one of these minors, which proves the first part of the lemma.

Now, suppose that y is a critical point of the restriction of Π to the regular part of $\overline{W(\mathcal{T})}$. If the rank of the jacobian of $\mathcal{T}$ in y is less than $n-d$, then $y \in V(s)$, and we are done. Suppose now that the rank of the jacobian of $\mathcal{T}$ in y equals $n-d$. Then the tangent space $T_y\overline{W(\mathcal{T})}$ is the zero-set of $\mathbf{grad}_y(t_{d+1}), \ldots, \mathbf{grad}_y(t_n)$. Then y being critical for Π yields the inequality

$$\dim(\mathrm{Span}(\mathbf{u}_1, \ldots, \mathbf{u}_d, \mathbf{grad}_y(t_{d+1}), \ldots, \mathbf{grad}_y(t_n))) < n,$$

where $\mathbf{u}_1, \ldots, \mathbf{u}_d$ are unitary vectors on the axes corresponding to the transcendental variables of $\mathcal{T}$. In particular, the jacobian determinant of $\mathcal{T}$ with respect to the algebraic variables vanishes at y; i.e. y is in $V(s)$. □

Lemma 4. *Let $\Gamma \subset \mathbb{C}^d$ be the set where the restriction of Π to $\overline{W(\mathcal{T})}$ is not proper. Then Γ is contained in the zero-set of h.*

Proof. Let the primary decomposition of $\mathrm{sat}(\mathcal{T})$ in $\mathbb{C}[X_1, \ldots, X_n]$ be $\mathrm{sat}(\mathcal{T}) = \bigcap_{\ell \leq L} A_\ell$. Since $\mathrm{sat}(\mathcal{T})$ is radical, all ideals A_ℓ are prime. Correspondingly, we write the decomposition of $\overline{W(\mathcal{T})}$ into $\mathbb{C}$-irreducible components $\overline{W(\mathcal{T})} = \bigcup_{\ell \leq L} V_\ell$, where V_ℓ is the zero-set of A_ℓ.

We use this decomposition to apply a characterization from [30] of the set of non-properness, which is valid in the irreducible case. Let $K = \mathbb{C}(X_1, \ldots, X_d)$ denote the rational function field on the set of transcendental variables, let $\mathrm{sat}(\mathcal{T})_K$, $\mathcal{T}_K$ and $A_{\ell,K}$ be the extensions of the ideals $\mathrm{sat}(\mathcal{T})$, $\mathcal{T}$ and A_ℓ in the ring $K[X_{d+1}, \ldots, X_n]$. Then the following assertions come from a routine check: (i) for all ℓ, $A_{\ell,K}$ is prime of dimension zero; (ii) two distinct ideals $A_{\ell,K}$ and $A_{\ell',K}$ generate the unit ideal; (iii) $K[X_{d+1}, \ldots, X_n]/A_{\ell,K}$ is isomorphic to the function field $\mathbb{C}(V_\ell)$ of V_ℓ; (iv) $\mathrm{sat}(\mathcal{T})_K$ equals $\mathcal{T}_K$.

Thus using the Chinese Remainder Theorem, we deduce the isomorphism $K[X_{d+1}, \ldots, X_n]/\mathcal{T}_K \simeq \prod_{\ell \leq L} \mathbb{C}(V_\ell)$. For i in $d+1, \ldots, n$ and $\ell \leq L$, let $m_{i,\ell} \in K[T]$ be the monic minimal polynomial of X_i in the extension $K \to \mathbb{C}(V_\ell)$. We also let M_i be the monic minimal polynomial of X_i in $K \to K[X_{d+1}, \ldots, X_n]/\mathcal{T}_K$. Then M_i is the LCM of the polynomials $m_{i,\ell}$, for $\ell \leq L$.

Let now y be in $\mathbb{C}^d$, and suppose that the restriction of Π to $\overline{W(\mathcal{T})}$ is not proper at y. Then there exists $\ell_0 \leq L$ such that the restriction of Π to V_{ℓ_0} is not proper at y. Lemma 3.10 in [30] shows that there exists i_0 in $d+1, \ldots, n$ such that y cancels the denominator of one of the coefficients of m_{i_0,ℓ_0}. By Gauss' lemma, y cancels the denominator of one of the coefficients of M_{i_0}.

On the other hand, after dividing the polynomials in $\mathcal{T}$ by h, we obtain polynomials in $K[X_{d+1}, \ldots, X_n]$ that are monic in their main variable. The possible necessary reductions to obtain a reduced Gröbner basis for $\mathcal{T}_K$ do not introduce new denominators. Thus, all denominators that appear in M_{i_0} divide h. Thus y cancels h, which concludes the proof. □

We can now prove Theorem 2. Let D be a connected component of $\overline{W(\mathcal{T})} \cap \mathbb{R}^n$ such that $\overline{W(\mathcal{T})} \cap V(s) = \emptyset$. Then, from Lemma 3, D does not contain any critical point of

Π restricted to the regular part of $\overline{W(\mathcal{T})}$ nor any singular point of $\overline{W(\mathcal{T})}$. Moreover, the restriction of Π to $\overline{W(\mathcal{T})}$ is dominant.

We then apply Theorem 1 to $\overline{W(\mathcal{T})}$ and Π. Let Γ be the set of points at which the restriction of Π to $\overline{W(\mathcal{T})}$ is not proper. From Lemma 4, $\Gamma \subset V(h)$. Then, for all connected component S of $\mathbb{R}^d \setminus (\Gamma \cap \mathbb{R}^d)$, there exists a connected component S' of $\mathbb{R}^d \setminus (V(h) \cap \mathbb{R}^d)$ such that $S' \subset S$. We are done. □

4. Main Algorithm

We now describe our main algorithm, which computes at least one point in each connected component of a real algebraic variety. Given a family $(P_1, \dots, P_k) \subset \mathbb{Q}[X_1, \dots, X_n]$, we first decompose the zero-set of $(P_1, \dots, P_k)$ by means of strongly normalized triangular sets $(\mathcal{T}_1, \dots, \mathcal{T}_\ell)$.

For each of these triangular sets $\mathcal{T}$ we do the following: (i) find a dominant projection Π by reading the transcendental variables of $\mathcal{T}$; (ii) compute a set of generators of $\overline{W(\mathcal{T})} \cap V(s)$, where s is the product of the separants of $\mathcal{T}$, and recursively call the algorithm for this new algebraic variety; (iii) compute at least one point in each connected component of the semi-algebraic set defined by $h \neq 0$, where h is the product of the initials of $\mathcal{T}$, and recursively call the algorithms for the fibers of Π above these points.

Note that computing one point in the connected components of the open set $h \neq 0$ can be done using the projection step of the cylindrical algebraic decomposition algorithm [14].

Theorem 3. *The above algorithm halts. It returns a family of zero-dimensional polynomial systems whose real solutions intersect each connected component of the real algebraic set $V(P_1, \dots, P_k) \cap \mathbb{R}^n$.*

Proving that our algorithm halts requires the following result.

Lemma 5. *Let $\mathcal{T} \subset \mathbb{Q}[X_1, \dots, X_n]$ be a regular separable triangular set, let Π be the projection on the affine subspace containing the axes of the transcendental variables of $\mathcal{T}$ and let y be a point in this subspace. Then the dimension of $\overline{W(\mathcal{T})} \cap \Pi^{-1}(y)$ is less than the dimension of $\overline{W(\mathcal{T})}$.*

Proof. Suppose on the contrary that $\overline{W(\mathcal{T})} \cap \Pi^{-1}(y)$ has the same dimension as $\overline{W(\mathcal{T})}$. This implies that there exists an irreducible component V' of $\overline{W(\mathcal{T})}$ such that $\dim(\Pi^{-1}(y) \cap V') = \dim(V')$. Thus, since V' is irreducible, for all $x \in V'$, $\Pi(x) = y$. This contradicts the fact that the restriction of Π to V' is dominant. □

Proof of Theorem 3. We proceed by induction on the dimension d of $V(P_1, \dots, P_k)$. If $d = 0$, then halting and correctness are readily verified. So we may consider that this is also the case for $0, \dots, d-1$, and prove that halting and correctness hold in dimension d.

By Lemmas 2 and 5, all recursive calls are done on systems of dimension less than d. Thus, the algorithm ends, so we conclude by proving correctness. Let D be a connected component of $V(P_1, \dots, P_k) \cap \mathbb{R}^n$. D contains a connected component D' of an equi-dimensional component $\mathcal{V}' \subset \mathbb{C}^n$ of $V(P_1, \dots, P_k)$ represented by a strongly normalized triangular set $\mathcal{T}$. If $\overline{W(\mathcal{T})}$ is zero-dimensional, then the conclusion obviously holds.

Else, suppose $D' \cap V(s)$ (where s is the product of the separants of $\mathcal{T}$) is not empty, let $\mathcal{I}$ be the set of indices of transcendental variables of $\mathcal{T}$, and let Π be the projection on these variables. Then there exists a connected component of the real algebraic variety defined by a set of generators of $\overline{W(\mathcal{T})} \cap V(s)$, which has dimension less than $\overline{W(\mathcal{T})}$.

Now, suppose $D' \cap V(s) = \emptyset$. Then, from Theorem 2, there exists a connected component S of the semi-algebraic set defined by $h \neq 0$ (where h is the product of the initials of $\mathcal{T}$) contained in $\Pi(D')$. Then there exists a connected component S of the semi-algebraic set defined by $h \neq 0$ such that $S \subset \Pi(D)$. Thus, $V(\mathcal{G}) \cap V(\Pi^{-1}(y))$ meets D'. This proves the theorem. □

5. Experimental Results

We now present the experimental results of a first implementation of our algorithm. We compared this implementation with our implementation of the algorithms of [4] and [44], and the implementation of Cylindrical Algebraic Decomposition in `QEPCAD` [28]. The algorithm of [4] is based on the computation of the critical points of a distance function and treats the singular case by the iterated study of the nested singular loci. That of [44] only treats hypersurfaces, to which case we reduce by performing a sum of squares; then the critical points of a distance function are computed and singular cases are dealt with by performing an infinitesimal deformation.

As explained in the Introduction, algorithms computing one point in each connected component of a real algebraic set are basic tools to decide the emptiness of semi-algebraic sets. This motivates the fact that we will not only focus on the computation times but also on the *quality* of the output, expressed as the sum of the degrees of the zero-dimensional systems we obtain, and the maximum of these degrees. The polynomial systems used to perform these experiments come from academic or industrial applications. Most of them can be found in the FRISCO test-suite, see [12]. For the study of further examples, refer to [36].

Software. Implementing the algorithm of [4] and ours requires two subroutines. The first one performs radical and equi-dimensional decomposition by splitting lexicographic Gröbner bases using the techniques of [2] as described in [48] . The Gröbner bases computations are done using the software `AGb`, implemented in C++ by Faugère [18]. The second subroutine takes a Gröbner base generating a zero-dimensional ideal and computes a Rational Univariate Representation via the algorithm proposed in [42] from which the isolation of real roots is performed. The software used to perform these computations is `RS` [43], which is implemented in C by Rouillier.

The layout of both algorithms is implemented in Maple. For the algorithm proposed in [4], it manages the computation of the minors of a jacobian matrix characterizing the critical points of a distance function. For our algorithm, it manages the subresultant computations required to implement the projection step of the Cylindrical Algebraic Decomposition algorithm. Maple is linked to `AGb` and `RS` via the `Gb`/Maple interface

Table 1. Computation times (in seconds).

System	$n/d/D/\delta$	`Distance`	`Projections`
Neural	4/1/3/24	8	10
Wang	10/1/9/114	10	17
Buchberger	8/4/3/6	10	6
Butcher	8/3/4/3	9	6
Vermeer	5/1/3/26	3	6
Donati	4/1/31/10	3	3
Euler	10/3/2/2	12	15
DiscPb	4/2/6/4	940	45
Prodecco	4/2/4/2	137	137
Hairer-2	13/2/4/25	∞	32
F633	10/2/2/32	∞	91
F744	12/1/3/40	∞	80
F855	14/1/4/52	∞	1020

package provided by Faugère. This implementation of our algorithm, together with further developments, is available in the RAGLib library [49].

The implementation of Cylindrical Algebraic Decomposition we use is the one provided in `QEPCAD` [28] which is implemented in C by Hong and his collaborators. Our implementation of the algorithm of [44] is based on the Magma Kronecker package by Lecerf [35] which implements the algorithm of [24]. On this basis, we implemented the algorithm of [51] to solve polynomial systems with infinitesimal coefficients.

Results. The computations have been performed on a Bi-Pentium III 800 MHz with 1 Go of RAM. In Table 1 we give the computation times of the algorithm proposed in [4], named `Distance` in the tables, and our algorithm, named `Projections`. The timings are given in seconds, and they include the isolation of the real solutions of the zero-dimensional systems. We specify the number n of variables, the dimension d of the variety they define, the maximal degree D of their polynomials and the degree δ of the generated ideal. The sign ∞ means that no result was obtained after 2 days of computation.

For these systems, our algorithm solves more problems than the one proposed in [4], with computation times that are almost always better. Our implementation of the algorithm of [44] failed to give an answer in less than 2 days for all systems except for the Donati system, which was solved in 8652 seconds; the output consists of 186 solutions. The software `QEPCAD` only solved the systems Vermeer in 49 seconds, Neural and Donati in 1 second, for which it respectively returns 65,976, 205 and 10 real algebraic points. This shows the relevance of our approach compared with the Cylindrical Algebraic Decomposition.

Now, we discuss the comparison with the algorithm of [4]. The critical locus of a regular application is characterized by the vanishing of minors in a jacobian matrix. For our algorithm, this jacobian matrix is triangular, thus no linear algebra is required and a factorization of such minors is immediately obtained. For the algorithm proposed in [4], the jacobian matrix is not triangular. The computation of the required minors is not a limiting step, but their size does not allow their exploitation in an elimination algorithm. For example, for the system F744, the minors have about 10,000 monomials and degree 54.

We next comment on the algorithm of [44] and its behavior. Following [51], its complexity is in $Ln^{O(1)}\mathsf{M}((2D)^n)^2$ operations in $\mathbb{Q}$, where L is the complexity of evaluation of the input system, n is the number of variables, D is an upper bound on the degrees of the input polynomials and M is the complexity of univariate polynomial multiplication. Taking into account the coefficient growth gives a complexity of $Lhn^{O(1)}\mathsf{M}((2D)^n)^3$ bit operations, where we also denote by $\mathsf{M}(D)$ the bit complexity of integer multiplication in size D, and h is a bound of the bit-size of the coefficients of the input polynomials. Up to logarithmic factors, we have $\mathsf{M}(D) \in O(D)$; further, we always have $L \in d^{O(n)}$.

Recall that applying the algorithm of [44] requires performing a sum of squares, and infinitesimal deformation, and computing the critical points of an arbitrary distance function. We observed that, due to this preparation of the input, solving these systems often required a time close to the above worst-case estimate. This is the main justification of the computation times we observed for the algorithm of [44].

On the other hand, on these examples, the runtime of the algorithm is far from showing a doubly exponential behavior; an explanation is that we benefit from and make use of favorable geometric conditions. For instance, the time necessary to study the complementary of the hypersurfaces defined by the initials of the triangular sets was always negligible before the rest of the execution time, as they always had a low number of variables or also low degrees.

Now, we compare the size of the output of the algorithms we consider. In Tables 2 and 3 we give respectively the degrees of the zero-dimensional systems we obtain, and the number of real solutions.

For both algorithms, the first number given in Table 2 is the sum of the degrees of the zero-dimensional systems. It is followed by the list of the degrees of these systems in decreasing order. In this list, a notation such as δ^n indicates the presence of n systems of degree δ.

On these examples, our algorithm returns a set of zero-dimensional systems whose sum of degrees is always less than the one returned by the algorithm proposed in [4].

Table 2. Size of the output.

System	`Distance`	`Projections`
Neural	225 [54, 44, 36, 21, 15^3, 13, 6^2]	222 [54, 12^2, 36, 21, 15^2, 8^2, 6^4, 4^2, 3^3]
Wang	168 [48, 24, 12^8]	144 [32^2, 8^2, 4^{16}]
Buchberger	53 [12, 10, 6^2, 5, 4^2, 2, 1^4]	13 [2^6, 1]
Butcher	14 [3, 2, 1^9]	6 [3, 2, 1]
Vermeer	84 [38^2, 8]	56 [8^5, 6^2, 4]
Donati	175 [175]	119 [41, 20, 10^5, 8]
Euler	29 [7^2, 4, 2, 1^9]	11 [1^{11}]
DiscPb	1235 [477, 371, 170, 119, 51, 15, 7^4, 3, 1]	74 [15, 8^2, 4^7, 2^7, 1]
Prodecco	58 [36, 18, 1^4]	55 [36, 18, 1]
Hairer-2		44 [1^{44}]
F633		220 [6^3, 4^9, 3^2, 2^{75}, 1^{10}]
F744		216 [24, 16, 12^6, 9^2, 4^{20}, 3^2]
F855		298 [24, 16, 12^7, 9^2, 6, 4^{36}, 3^2]

Table 3. Number of real solutions.

System	`Distance`	`Projections`
Neural	59	56
Wang	16	16
Buchberger	21	7
Butcher	12	4
Vermeer	24	20
Donati	8	11
Euler	19	11
DiscPb	54	24
Prodecco	28	25
Hairer-2		44
F633		162
F744		52
F855		192

Moreover, the same remark holds for the maximum degree of the zero-dimensional systems returned by both algorithms, up to one example. Thus, the output of our algorithm seems to be more exploitable than that of the algorithm proposed in [4].

References

1. M. E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeros, multiplicities and idempotents for zero-dimensional systems. In *Algorithms in Algebraic Geometry and Applications*. *Proceedings MEGA '94*, pages 1–15. Volume 142 of Progress in Mathematics. Birkhäuser, Boston, MA, 1996.
2. P. Aubry. Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Ph.D. thesis, Université Paris 6, 1999.
3. P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, *Special Issue on Polynomial Elimination*, 28:105–124, 1999.
4. P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6):543–560, December 2002.
5. 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.
6. B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real elimination. *Mathematische Zeitschrift*, 238(1):115–144, 2001.
7. B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. A first approach to generalized polar varieties. To appear in *Wybernetica*, 2004.
8. B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties: geometry and algorithms. Preprint, 2003.
9. S. Basu. Algorithms in Semi-Algebraic Geometry. Ph.D. thesis, New York University, 1996.
10. S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of ACM*, 43(6):1002–1045, 1996.
11. S. Basu, R. Pollack, and M.-F. Roy. A new algorithm to find a point in every cell defined by a family of polynomials. In B. Caviness and J. Johnson, editors, *Quantifier Elimination and Cylindrical Algebraic Decomposition*. Texts and Monographs in Symbolic Computation. Springer-Verlag, New York, 1998.
12. D. Bini and B. Mourrain. The FRISCO test-suite. `http://www-sop.inria.fr/saga/POL/`, 2000.
13. B. Buchberger. Gröbner bases: an algorithmic method in polynomial ideal theory. In N. W. Bose and D. Reider, editors, *Multidimensional System Theory*, pages 374–383. Reidel, Dordrecht, 1985.
14. G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. *Automata Theory and Formal Languages*, pages 515–532. Volume 33 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, 1975.

15. I. Z. Emiris and B. Mourrain. Matrices in elimination theory. *Journal of Symbolic Computation*, 28(1–2):3–43, 1999.
16. J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, 1999.
17. J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *ISSAC* 2002, pages 75–83. ACM Press, New York, 2002.
18. J.C. Faugère. Gb. `http://fgbrs.lip6.fr/Gb/index.html`, 2003.
19. J.C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.
20. J.-C. Faugère, F. Moreau de Saint Martin, and F. Rouillier. Design of regular nonseparable bidimensional wavelets using groebner basis techniques. *IEEE SP Transactions*, *Special Issue on Theory and Applications of Filter Banks and Wavelets*, 46(4):845–856, April 1998.
21. M. Giusti, K. Hägele, J. Heintz, J.-E Morais, J.-L. Montaña, and L.-M. Pardo. Lower bounds for Diophantine approximation. In *Proceedings of MEGA* '96, in *Journal of Pure and Applied Algebra*, 117–118: 277–317, 1997.
22. M. Giusti, J. Heintz, J.-E. Morais, J. Morgenstern, and L.-M. Pardo. Straight-line programs in geometric elimination theory. Journal of Pure and Applied Algebra, 124:101–146, 1998.
23. M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. When polynomial equation systems can be solved fast? In *Proceedings of AAECC*-11, pages 205–231. Volume 948 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, 1995.
24. M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.
25. D. Grigoriev and N. Vorobjov. Solving systems of polynomials inequalities in subexponential time. *Journal of Symbolic Computation*, 5:37–64, 1988.
26. J. Heintz, M.-F. Roy, and P. Solerno. On the complexity of semi-algebraic sets. In *Proceedings IFIP*, pages 233–298, 1989.
27. J. Heintz, M.-F. Roy, and P. Solerno. On the theoretical and practical complexity of the existential theory of the reals. *The Computer Journal*, 36(5):427–431, 1993.
28. H. Hong et al. QEPCAD, Quantifier Elimination by Partial Cylindrical Algebraic Decomposition. `http://www.cs.usna.edu/~qepcad/B/QEPCAD.html`, 2003.
29. E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms, I: Polynomial systems. In U. Lager and F. Winkler, editors, *Symbolic and Numerical Scientific Computations*, pages 1–39. Springer-Verlag, New York, 2003.
30. Z. Jelonek. Testing sets for properness of polynomial mappings. *Mathematische Annalen*, 315(1):1–35, 1999.
31. M. Kalkbrener. *Three Contributions to Elimination Theory*. Ph.D. thesis, Kepler University, Linz, 1991.
32. D. Lazard. A new method for solving algebraic systems of positive dimension. *Discrete Applied Mathematics*, 33:147–160, 1991.
33. D. Lazard. Solving zero-dimensional algebraic systems. *Journal of Symbolic Computation*, 13:117–133, 1992.
34. D. Lazard. Stewart platform and Gröbner bases. In V. Parenti-Castelli and J. Lenaric, editors, *Proceedings of the Third International Workshop on Advances of Robot Kinematics*, pages 136–142. Ferrare, 1992.
35. G. Lecerf. Kronecker. `http://fermat.math.uvsq.fr/~lecerf/software/kronecker/`, 2003.
36. C. Le Guernic and M. Safey El Din. On the practical computation of one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and non-strict inequalities. Research Report 5079, INRIA, 2004.
37. F. Lemaire. Contribution à l'algorithmique en algèbre différentielle. Ph.D. thesis, Université des Sciences et Technologies de Lille, 2002.
38. M. Moreno Maza. Calculs de pgcd au-dessus des tours d'extensions simples et résolution des systèmes d'équations algébriques. Ph.D. thesis, Université Paris 6, 1997.
39. M. Moreno Maza and R. Rioboo. Polynomial gcd computations over tower of algebraic extensions. In G. Cohen, M. Giusti, and T. Mora, editors, *Proceedings AAECC*-11, pages 365–382. Number 948 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, 1995.
40. S. Morrison. The differential ideal $[P] : M^{\infty}$. *Journal of Symbolic Computation*, 28:631–656, 1999.
41. R. Rioboo. Towards faster real algebraic numbers. In *ISSAC* 2002, pages 221–228. ACM Press, New York, 2002.

42. F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Journal of Applicable Algebra in Engineering*, *Communication and Computing*, 9(5):433–461, 1999.
43. F. Rouillier. RS. `http://fgbrs.lip6.fr/RS/index.html`, 2003.
44. F. Rouillier, M.-F. Roy, and M. Safey El Din. Finding at least one point in each connected component of a real algebraic set defined by a single equation. *Journal of Complexity*, 16:716–750, 2000.
45. F. Rouillier, M. Safey El Din, and É. Schost. Solving the Birkhoff interpolation problem via the critical point method: an experimental study. In *Proceedings of ADG* 2000, pages 26–40, 2000.
46. F. Rouillier and P. Zimmermann. Efficient isolation of polynomial real roots. *Journal of Computational and Applied Mathematics*, 162(1):33–50, 2003.
47. M.-F. Roy. Basic algorithms in real algebraic geometry: from Sturm's theorem to the existential theory of reals. In *Lectures on Real Geometry in Memoriam of Mario Raimondo*, pages 1–67. Volume 23 of Expositions in Mathematics. de Gruyter, New York, 1996.
48. M. Safey El Din. Résolution réelle des systèmes polynomiaux de dimension positive. Ph.D. thesis, Université Paris 6, January 2001.
49. M. Safey El Din. RAGLib. `http://www-calfor.lip6.fr/~safey/RAGLib`, 2003.
50. M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *ISSAC* 2004, pages 224–231. ACM Press, New York, 2003.
51. É. Schost. Computing parametric geometric resolutions. *Journal of Applicable Algebra in Engineering Communication and Computing*, 13(4):349–393, 2003.
52. I. R. Shafarevich. *Basic Algebraic Geometry*, 1, second edition. Springer-Verlag, Berlin, second edition, 1994.
53. J. Uspensky. *Theory of Equations*. McGraw-Hill, New York, 1948.
54. J. Verschelde. Algorithm 795: Phcpack: a general-purpose solver for polynomial systems by homotopy continuation. *ACM Transactions on Mathematical Software*, 25(2):251–276, 1999.
55. D. Wang. An elimination method for polynomial systems. *Journal of Symbolic Computation*, 16:83–114, 1993.
56. D. Wang. *Elimination Methods*. Springer-Verlag, New York 2001.

Received October 30, 2002, *and in revised form February* 10, 2004. *Online publication July* 14, 2004.