Computing Sampling Points on a Singular Real Hypersurface using Lagrange's System

Mohab Safey El Din

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Computing Sampling Points on a Singular Real Hypersurface using Lagrange's System

Mohab Safey El Din

N° 5464

Janvier 2005

Thème SYM

ISSN 0249-6399 ISRN INRIA/RR--5464--FR+ENG

Computing Sampling Points on a Singular Real Hypersurface using Lagrange's System

Mohab Safey El Din*

Thème SYM — Systèmes symboliques
Projets SALSA

Rapport de recherche n° 5464 — Janvier 2005 — 19 pages

Abstract: Let f be a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree bounded by D and, for $t \in \mathbb{Q}$, $\mathcal{H}_t \subset \mathbb{C}^n$ the hypersurface defined by $f - t = 0$. Consider a polynomial $\phi \in \mathbb{Q}[X_1, \ldots, X_n]$ and the mapping $\phi : \mathbb{C}^n \to \mathbb{C}$. Suppose the ideal I generated by $\langle L.\mathbf{grad}(f) - \mathbf{grad}(\phi)\rangle$ is equi-dimensional, has dimension 1 and the ideal $I + \langle f\rangle$ is zero-dimensional. In this case, we provide efficient algorithmic tools to compute the limits of the critical points of ϕ restricted to $\mathcal{H}_t$ when $t \to 0$.
We prove that for a generic choice of a point (resp. a line) the above result apply when ϕ is the square of the euclidean distance to the chosen point (resp. the projection on the chosen line). Then, we provide algorithms to compute at least one point in each connected component of $\mathcal{H}_0 \cap \mathbb{R}^n$ which based on the improved computation of the limits of the critical points of a polynomial mapping restricted to $\mathcal{H}_t$. The worst-case complexity of our algorithms is polynomial in D^n in terms of arithmetic operations in $\mathbb{Q}$. We prove it improves previous strategies based on the use of infinitesimal arithmetic. Practical experiments confirm these are the first algorithms dealing with this problem mixing practical efficiency and asymptotically optimal complexity.

Key-words: Real solutions, Polynomial systems, Singularities, Complexity and efficient algorithms

* Mohab.Safey@lip6.fr, Univeristé Pierre et Marie Curie, Projet INRIA/LIP6 SALSA

Calcul d'un point par composante connexe sur une hypersurface singulière via le système de Lagrange

Résumé : Soit f un polynôme dans $\mathbb{Q}[X_1, \ldots, X_n]$ de degré borné par D et, pour $t \in \mathbb{Q}$, $\mathcal{H}_t \subset \mathbb{C}^n$ l'hypersurface définie par $f - t = 0$. Considérons un polynôme $\phi \in \mathbb{Q}[X_1, \ldots, X_n]$ et l'application polynomiale $\phi : \mathbb{C}^n \to \mathbb{C}$. Supposons que l'idéal I engendré par $\langle L.\mathbf{grad}(f) - \mathbf{grad}(\phi)\rangle$ est equi-dimensionel, de dimension 1 et que l'idéal $I + \langle f\rangle$ ess zero-dimensionel. Sous ces conditions, on fournit des algorithmes efficaces calculant les limites bornées des points critiques de ϕ restreinte à $\mathcal{H}_t$ quand $t \to 0$.
On prouve ensuite que pour un choix générique d'un point (resp. d'une droite) le résultat précédent s'applique quand ϕ est le carré de la distance euclidienne au point choisi (ou la projection sur la droite choisie). On fournit alors des algorithmes calculant au moins un point par composante connexe de $\mathcal{H}_0 \cap \mathbb{R}^n$ reposant sur le calcul efficace de limites de points critiques. Dans les pires cas, la complexité de nos algorithmes est polynomiale en D^n en terme de nombre d'opérations arithmétiques dans $\mathbb{Q}$. On prouve par ailleurs que leur complexité est meilleure que celle des algorithmes reposant sur l'usage d'une arithmétique infinitésimale. Quelques expérimentations confirment l'efficacité de ces algorithmes qui sont les premiers traitant ces problèmes et mixant à la fois complexité théorique asymptotiquement optimale et performances pratiques.

Mots-clés : Solutions réelles, Systèmes polynomiaux, Singularités, complexité, algorithmes efficaces

1 Introduction

Let f be a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree bounded by D and, for $t \in \mathbb{Q}$, $\mathcal{H}_t \subset \mathbb{C}^n$ be the hypersurface defined by $f - t = 0$.
The core of this paper is to provide an algorithm computing at least one point in each connected component of $\mathcal{H}_0 \cap \mathbb{R}^n$, without smoothness assumptions on $\mathcal{H}_0$, whose theoretical complexity is asymptotically optimal and whose practical behaviour reflects this efficiency.

Motivation and description of the problem. Computing at least one point in each connected component of a real algebraic set defined by a single equation is a basic subroutine to several algorithms of effective real algebraic geometry (see [18, 19, 20, 5, 6, 7] where studying semi-algebraic sets is reduced to study the real counterpart of singular hypersurfaces). Note also that such a subroutine is used in [9] to improve partial Cylindrical Algebraic Decomposition or in [34] to study semi-algebraic sets defined by a single inequality.

Since it has produced asymptotically optimal complexity results, we focus on the critical point method. This method is based on computing the critical locus of a polynomial mapping restricted to $\mathcal{H}_0$ reaching its extrema on each connected component of $\mathcal{H}_0 \cap \mathbb{R}^n$ at a finite number of points. Thus, the problem of computing sampling points in $\mathcal{H}_0 \cap \mathbb{R}^n$ is reduced to solve a polynomial system defining the critical points of the considered polynomial mapping. In the case where $\mathcal{H}_0$ is smooth, a zero-dimensional polynomial system is produced and one has to compute a rational parametrization, also called Rational Univariate Representation (see [27, 28]), or geometric resolution (see [16, 15, 14, 17, 24]) to encode the solution set of this zero-dimensional polynomial system.
Several variants of this method have been provided using either projection functions when $\mathcal{H}_0 \cap \mathbb{R}^n$ is compact and smooth (see [2]) or without assumptions of compactness (see [36, 35] and [5, 6] which reduce the study to a compact real algebraic set) or quadratic mappings (see [29, 1, 4, 3]). When $\mathcal{H}_0$ is smooth, the worst-case complexity of most of these algorithms are polynomial in D^n. Precise analysis show that the best complexity is obtained in [35]. Moreover, in the smooth case, efficient implementations reflecting this nice complexity already exist (see [33]).

In this paper we focus on the situation where $\mathcal{H}_0$ is not smooth. Asymptotically optimal algorithms using an infinitesimal deformation are already provided in [5, 6, 29] but do not lead to efficient implementations. The classical strategy consists in studying the hypersurface defined by $f - \varepsilon = 0$ (where ε is an infinitesimal) which is smooth, compute critical points of a mapping restricted to this hypersurface by means of a rational parametrization with coefficients in the field of rational fractions $\mathbb{Q}(\varepsilon)$ and compute the bounded limits of these critical points from this parametrization (see [29, 7] for developments based on the notion of well-separating elements and [32] for developments based on Puiseux series expansions). Experiments (see [30]) have shown that the intermediate data of such an approach is huge compared to the output. This partially explains the fact it is difficult to obtain an efficient implementation according to the above process of resolution. Moreover, the degree of ε

required to deal with these computations is D^n in the worst-cases which spoils the bit-complexity compared to smooth cases.

An alternative strategy is proposed in [1]. It consists in the recursive study of imbricated singular loci on the one hand, and the computation of critical points of a polynomial mapping restricted to the regular locus of an algebraic variety, on the other hand. This approach has lead to practical improvements (see [30, 33]). Nevertheless, its complexity is not well-controlled.

The goal of this paper is to provide an algorithm whose complexity is asymptotically optimal and whose practical performances reflect this complexity avoiding computations over an infinitesimal arithmetic. More precisely, we aim to design an algorithm whose worst-case bit-complexity is the same when $\mathcal{H}_0$ is smooth or not.

Main contributions. Our approach consists in computing directly the bounded limits (when ε tends to 0) of the critical points of a polynomial mapping restricted to the hypersurface defined by $f - \varepsilon = 0$ without computing an intermediate rational parametrization with coefficients in $\mathbb{Q}(\varepsilon)$.

Given a polynomial $\phi \in \mathbb{Q}[X_1, \ldots, X_n]$, and considering the mapping $\phi : \mathbb{C}^n \to \mathbb{C}$ sending $x \in \mathbb{C}^n$ to $\phi(x)$, consider for $t \in \mathbb{Q}$ the critical locus $K(\phi, \mathcal{H}_t)$ of ϕ restricted to the *regular locus* of $\mathcal{H}_t$.
If $K(\phi, \mathcal{H}_0)$ is zero-dimensional (or empty) and if the ideal I generated by:

$$L.\frac{\partial f}{\partial X_1} - \frac{\partial \phi}{\partial X_1}, \ldots, L.\frac{\partial f}{\partial X_n} - \frac{\partial \phi}{\partial X_n}$$

(where L is a new variable) is equidimensional and has dimension 1, our first result (see Theorem 1 below) states that the bounded limits of $K(\phi, \mathcal{H}_t)$ when t tends to 0 are contained in the algebraic variety associated to the ideal:

$$\langle f \rangle + (I \cap \mathbb{Q}[X_1, \ldots, X_n])$$

which is zero-dimensional. We provide algorithmic tools to perform this computation, based on Gröbner bases and geometric resolution. The latter algorithmic solution does not involve the extra-variable L.
Note that, in the case where $\mathcal{H}_0$ is not smooth the set of bounded limits of $K(\phi, \mathcal{H}_t)$ when t tends to 0 strictly contains $K(\phi, \mathcal{H}_0)$.

Then, we use this result to compute at least one point in each connected component of the real algebraic investigating two variants of the critical point method proposed in [29, 3] (using quadratic mappings) and [35] (using projection functions) without any assumption on the smoothness of $\mathcal{H}_0$.
More precisely, we prove (see Theorem 2 below) that up to a *generic choice* of a point $A = (a_1, \ldots, a_n) \in \mathbb{Q}^n$, the algebraic variety associated to the ideal:

$$\langle f \rangle + \left(\langle L.\frac{\partial f}{\partial X_1} - (X_1 - a_1), \ldots, L.\frac{\partial f}{\partial X_n} - (X_n - a_n) \rangle \cap \mathbb{Q}[X_1, \ldots, X_n] \right)$$

is zero-dimensional and intersects each connected component of the real algebraic set $\mathcal{H}_0 \cap \mathbb{R}^n$. Additionally, given an arbitrary point $(p_1, \ldots, p_{n-1}) \in \mathbb{Q}^{n-1}$ and up to a generic linear change of variables (in the sequel, for $\mathbf{A} \in GL_n(\mathbb{Q})$, $f^{\mathbf{A}}$ denotes the polynomial $f(\mathbf{A}.X)$ where X is the vector of indeterminates), for $i = 1, \ldots, n-2$, the ideals:

$$\langle f^{\mathbf{A}}, X_1 - p_1, \ldots, X_i - p_i \rangle + \langle L.\frac{\partial f^{\mathbf{A}}}{\partial X_{i+1}} - 1, \frac{\partial f^{\mathbf{A}}}{\partial X_{i+2}} \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_n} \rangle \cap \mathbb{Q}[X_1, \ldots, X_n]$$

the ideal $\langle f, X_1 - p_1, \ldots, X_{n-1} - p_{n-1} \rangle$ and the ideal:

$$\langle f^{\mathbf{A}} \rangle + \left(\langle L.\frac{\partial f^{\mathbf{A}}}{\partial X_1} - 1, \frac{\partial f^{\mathbf{A}}}{\partial X_2} \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_n} \rangle \cap \mathbb{Q}[X_1, \ldots, X_n] \right)$$

are zero-dimensional and the union of their associated algebraic varieties intersect each connected component of $\mathcal{H}_0 \cap \mathbb{R}^n$ (see Theorem 3 below).

Then, we provide complexity estimates for the algorithms relying on Theorem 2 and Theorem 3 and the elimination techniques of [17] inspired by [16, 15, 14] and which is generalized in [25]. They do not require the extra variable L appearing in the above statements and are polynomial in n, the complexity $\mathcal{L}$ of evaluation of f and an intrinsic geometric degree δ which is bounded by D^n (where D is the degree of f). We compare precisely the complexity of both algorithms and show the one relying on Theorem 3 is better than the one relying on Theorem 2. At last, we compare the bit-complexity of the algorithm which consists in applying the results of [35] and an infinitesimal arithmetic with the one relying on Theorem 3 and show the latter strategy is better. An implementation of this algorithm is already available in [33]. Experiments have shown it has a practical behaviour at last comparable to the strategy proposed in [1] and sometimes it is better.

Organization of the paper. The next section is devoted to the proof of Theorem 1 stated above. Section 3 is devoted to the design of algorithms computing sampling points on a real algebraic set defined by a single equation and the proofs of Theorems 2 and 3. Section 4 is devoted to the complexity analysis of our algorithms and the comparison of these results with previous works.

2 Computing limits of critical points

Let f be a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree bounded by D. For $t \in \mathbb{R}$, denote by $\mathcal{H}_t \subset \mathbb{C}^n$ the hypersurface defined by $f - t = 0$.
Let $\phi : x \in \mathbb{C}^n \to \phi(x) \in \mathbb{C}$ be a polynomial mapping. For $t \in \mathbb{R}$, $K(\phi, \mathcal{H}_t)$ denotes the critical locus of ϕ restricted to $\mathcal{H}_t$. The following result characterizes the bounded limits of $K(\phi, \mathcal{H}_t)$ when t tends to 0.

Theorem 1 *Let L be a new variable, and $I \subset \mathbb{Q}[L, X_1, \ldots, X_n]$ be the ideal generated by the polynomial family:*

$$L.\frac{\partial f}{\partial X_1} - \frac{\partial \phi}{\partial X_1}, \ldots, L.\frac{\partial f}{\partial X_n} - \frac{\partial \phi}{\partial X_n}$$

Suppose I is equi-dimensional, has dimension 1, and $K(\phi, \mathcal{H}_0)$ is zero-dimensional. Then, the bounded limits of $K(\phi, \mathcal{H}_t)$ when t tends to 0 are contained in the algebraic variety associated to the ideal

$$I_0 = \langle f \rangle + (I \cap \mathbb{Q}[X_1, \ldots, X_n]) \subset \mathbb{Q}[X_1, \ldots, X_n]$$

and I_0 is zero-dimensional.

Proof. Let $C \subset \mathbb{C}^{n+1}$ be the curve defined by I, $\Pi : \mathbb{C}^{n+1} \to \mathbb{C}^n$ be the projection sending $(x_1, \ldots, x_n, \ell)$ to $(x_1, \ldots, x_n)$ and $\mathcal{C} = \Pi(C)$.
Remark that f vanishes at each bounded limit y of $K(\phi, \mathcal{H}_t)$ when $t \to 0$, Let y be such a limit. If y belongs to $K(\phi, \mathcal{H}_0)$, we are done since $K(\phi, \mathcal{H}_0) \subset \mathcal{C}$. Now, suppose $y \notin K(\phi, \mathcal{H}_0)$, then $\mathbf{grad}_y(f) = \mathbf{0}$. Thus, y belongs to the set of non-properness of Π restricted to C which is contained in the Zariski-closure of $\mathcal{C}$ (see [22, Lemma 2 and 3]). This implies y belongs to the Zariski-closure of $\mathcal{C}$ which is the algebraic variety associated to $I \cap \mathbb{Q}[X_1, \ldots, X_n]$. Thus, $\mathcal{V}(I_0) \subset \mathbb{C}^n$ contains the bounded limits of $K(\phi, \mathcal{H}_t)$ when t tends to 0.
Consider a point y in $\mathcal{V}(I_0)$. As above, we distinguish in the sequel the cases where Π restricted to C is proper at y or not. If y is a point of $\mathcal{C} \cap \mathcal{H}_0$ at which Π restricted to C is proper, then y belongs to $K(\phi, \mathcal{H}_0)$ which is supposed to be zero-dimensional. Suppose now y belongs to the set of non-properness of Π restricted to C. From [21], the set of points in $\mathcal{C}$ at which the projection Π restricted to C is not proper is a finite set of points. Then I_0 is zero-dimensional and contains the bounded limits of $K(\phi, \mathcal{H}_t)$ when t tends to 0.
□

Remark 1 *In the case where $\mathcal{H}_0$ is smooth, the set of limits of $K(\phi, \mathcal{H}_t)$ when t tends to 0 is exactly $K(\phi, \mathcal{H}_0)$ while it strictly contains $K(\phi, \mathcal{H}_0)$ when $\mathcal{H}_0$ is not smooth. Thus, the above result is relevant and useful when $\mathcal{H}_0$ is not smooth.*

Corollary 1 *Let D be an integer bounding the degree of f and ϕ. Using the above notation, the degree of I is bounded by $(n-1)(D-1)^{n-1}$ and the degree of I_0 is bounded by $n.D.(D-1)^{n-1}$.*

Proof. Remark that the polynomial system defining I can be bi-homogenized. Then, the announced bound on the degree of I is an immediate consequence of [37, Theorem 1]. Since $\deg(I \cap \mathbb{Q}[X_1, \ldots, X_n]) \leq \deg(I)$ and $I_0 = \langle f \rangle + (I \cap \mathbb{Q}[X_1, \ldots, X_n])$, we are done.
□

Algorithmic procedure using Gröbner bases. Classical results about Gröbner bases (see [10, Chapter 9]) show that computing a Gröbner basis of I with respect to a monomial Degree Reverse Lexicographic block-ordering with $[L] > [X_1, \ldots, X_n]$ and eliminating polynomials having degree greater than 0 in L provides a Gröbner basis G of $I \cap \mathbb{Q}[X_1, \ldots, X_n]$. It is now enough to compute a Gröbner basis for the ideal generated by the polynomial family $G \cup \{f\}$.

Algorithmic procedure using geometric resolution. The algorithm of geometric resolution provided in [25] does not allow to compute elimination ideals. Nevertheless, it allows localization without adding an extra variable. Remark that the ideal

$$I = \langle L.\frac{\partial f}{\partial X_1} - \frac{\partial \phi}{\partial X_1}, \ldots, L.\frac{\partial f}{\partial X_n} - \frac{\partial \phi}{\partial X_n} \rangle \cap \mathbb{Q}[X_1, \ldots, X_n]$$

contains the ideal J generated by the set Δ of all $(2,2)$ minors of the jacobian matrix associated to $\mathrm{Jac}(f, \phi)$. Let $\mathcal{P}$ be a prime ideal associated to $\sqrt{J}$ which is not associated to $\sqrt{I}$ and y be a *generic* point in the algebraic variety associated to $\mathcal{P}$. Remark that if there exists $i \in \{1, \ldots, n\}$ such that $\frac{\partial f}{\partial X_i}(y) \neq 0$, then y belongs to the curve associated to $I \cap \mathbb{Q}[X_1, \ldots, X_n]$ which is not possible. Thus, to compute a geometric resolution of $I \cap \mathbb{Q}[X_1, \ldots, X_n]$ it is sufficient to saturate J by $\frac{\partial f}{\partial X_1}^2 + \cdots + \frac{\partial f}{\partial X_n}$. This can be done by giving as input to the algorithm of [25] the following polynomial system of equations and inequations:

$$\Delta, \quad \frac{\partial f}{\partial X_1}^2 + \cdots + \frac{\partial f}{\partial X_n}^2 \neq 0.$$

An alternative strategy consists in computing for $i = 1, \ldots, n$ geometric resolutions for: $\Delta, \quad \frac{\partial f}{\partial X_i} \neq 0$. This avoids the growth of degree induced by the above one but introduces a combinatorial factor

3 Algorithms

We focus now on the computation of at least one point in each connected component of the real algebraic set $\mathcal{H}_0 \cap \mathbb{R}^n$. In particular, we consider the situation where $\mathcal{H}_0$ has singular points. Our strategy consists in using Theorem 1 and the critical point method using either distance functions (see also [29, 1, 3]) or projection functions (see also [36, 35, 2]).

Using the distance function. Given a point A in $\mathbb{Q}^n$, let ϕ_A be the mapping sending $y \in \mathbb{C}^n$ to the square of the euclidean distance of y to A:

$$\begin{array}{rccc} \phi_A : & \mathbb{C}^n & \rightarrow & \mathbb{C} \\ & (x_1, \ldots, x_n) & \rightarrow & (x_1 - a_1)^2 + \cdots + (x_n - a_n)^2 \end{array}$$

Theorem 2 *There exists a Zariski-closed subset $\mathcal{A}$ of $\mathbb{C}^n$ such that for $A \in \mathbb{Q}^n \setminus \mathcal{A}$ the algebraic variety associated to the ideal*

$$\langle f \rangle + \left(\langle L.\frac{\partial f}{\partial X_1} - (X_1 - a_1), \ldots, L.\frac{\partial f}{\partial X_n} - (X_n - a_n) \rangle \cap \mathbb{Q}[X_1, \ldots, X_n] \right)$$

(where L is a new variable) is zero-dimensional and intersects each connected component of the real algebraic set $\mathcal{H}_0 \cap \mathbb{R}^n$.

The proof is based on both lemmata below. The first one is proved in [29] and ensures that computing the bounded limits of the critical points of the euclidean distance function to a point A restricted to $\mathcal{H}_t$ when t tends to 0 allows to obtain at least one point in each connected component of $\mathcal{H}_0 \cap \mathbb{R}^n$.

Lemma 1 *[29] Let A be a point of $\mathbb{Q}^n$ and ϕ_A be the square of the euclidean distance to A. Each connected component of $\mathcal{H}_0$ contains at least one point which is a bounded limit of $K(\phi_A, \mathcal{H}_t)$ when t tends to 0.*

The following lemma shows that up to a generic choice of A the assumptions of Theorem 1 are satisfied and then we are done.

Lemma 2 *There exists a Zariski-closed subset $\mathcal{A} \subset \mathbb{Q}^n$ such that for $A = (a_1, \ldots, a_n) \in \mathbb{Q}^n \setminus \mathcal{A}$, the ideal I_A generated by:*

$$L.\frac{\partial f}{\partial X_1} - (X_1 - a_1), \ldots, L.\frac{\partial f}{\partial X_n} - (X_n - a_n)$$

is equi-dimensional, has dimension 1 and $K(\phi_A, \mathcal{H}_0)$ is zero-dimensional.

Proof. From Sard's theorem, the set of critical values of the mapping:

$$\begin{array}{rccl} \psi : & \mathbb{C}^n \times \mathbb{C} & \to & \mathbb{C}^n \\ & (x = (x_1, \ldots, x_n), \ell) & \to & \ell.\frac{\partial f}{\partial X_1}(x) - x_1, \ldots, \ell.\frac{\partial f}{\partial X_n}(x) - x_n \end{array}$$

is a proper Zariski-closed subset $\mathcal{A}$ of $\mathbb{C}^n$. It is then enough to choose $A = (a_1, \ldots, a_n) \in \mathbb{Q}^n$ outside $\mathcal{A}$ and remark that this implies at any point $(x, \ell) \in \mathbb{C}^n \times \mathbb{C}$

$$\mathrm{rank}(\mathrm{Jac}_{(x,\ell)}(L.\frac{\partial f}{\partial X_1} - (X_1 - a_1), \ldots, L.\frac{\partial f}{\partial X_n} - (X_n - a_n))) = n$$

to prove that I_A is equi-dimensional and has dimension 1.
Proving that $K(\phi_A, \mathcal{H}_0)$ is zero-dimensional for A chosen outside a Zariski-closed subset of $\mathbb{C}^n$ is done by the same way considering the restriction of ψ to the regular locus of $\mathcal{H}_0$.
□

From Theorem 2, one can deduce an algorithm computing at least one point in each connected component of $\mathcal{H}_0 \cap \mathbb{R}^n$ using either Gröbner bases or geometric resolutions. This is

based on computing the limits of the critical points of ϕ_A restricted to $\mathcal{H}_t$ when t tends to 0.
Compared to the algorithm proposed to [29], our contribution allows to avoid computations over an infinitesimal arithmetic. In section 4, we precisely compare both strategies.
In the next paragraph, we deduce an other algorithm to compute sampling points in $\mathcal{H}_0 \cap \mathbb{R}^n$ adapting the work of [35] to our purpose. Instead of quadratic mappings, we use exclusively projection functions, which are linear.

Using projection functions. Given a matrix $\mathbf{A}$ in $GL_n(\mathbb{C})$, we denote by $f^{\mathbf{A}}$ the polynomial $f(\mathbf{A}.X)$ and by $\mathcal{H}_t^{\mathbf{A}} \subset \mathbb{C}^n$ the hypersurface defined by $f^{\mathbf{A}} - t = 0$ (for $t \in \mathbb{Q}$). We consider canonical projections:

$$\begin{array}{rccc} \Pi_i : & \mathbb{C}^n & \rightarrow & \mathbb{C}^i \\ & (x_1, \ldots, x_n) & \rightarrow & (x_1, \ldots, x_i) \end{array}$$

Given an arbitrary point $(p_1, \ldots, p_{n-1})$ in $\mathbb{Q}^{n-1}$ and a matrix $\mathbf{A} \in GL_n(\mathbb{Q})$, let $I_i^{\mathbf{A}}$ (for $i = 1, \ldots, n-2$) be the ideal:

$$\left(\langle L.\frac{\partial f^{\mathbf{A}}}{\partial X_{i+1}} - 1, \frac{\partial f^{\mathbf{A}}}{\partial X_{i+2}}, \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_n}, X_1 - p_1, \ldots, X_i - p_i \rangle \cap \mathbb{Q}[X_1, \ldots, X_n] \right)$$

$I_{n-1}^{\mathbf{A}}$ be the ideal $\langle X_1 - p_1, \ldots, X_n - p_n \rangle$ and $I_0^{\mathbf{A}}$ be the ideal:

$$\left(\langle L.\frac{\partial f^{\mathbf{A}}}{\partial X_1} - 1, \frac{\partial f^{\mathbf{A}}}{\partial X_2}, \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_n} \rangle \cap \mathbb{Q}[X_1, \ldots, X_n] \right)$$

Theorem 3 *Let $(p_1, \ldots, p_{n-1})$ be an arbitrary point of $\mathbb{Q}^{n-1}$. There exists a Zariski-closed subset $\mathcal{A}$ of $GL_n(\mathbb{C})$ such that for $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, the union of the algebraic varieties associated to the ideals $\langle f^{\mathbf{A}} \rangle + I_i^{\mathbf{A}}$ (for $i = 0, \ldots, n-1$) is zero-dimensional and intersects each connected component of the real algebraic set $\mathcal{H}_0^{\mathbf{A}} \cap \mathbb{R}^n$.*

The proof of this result is based on the following lemmata.

Lemma 3 *Let C be a connected component of $\mathcal{H}_0$ and suppose $\Pi_1(C)$ is closed. Then, either for an arbitrary rational $p_1 \in \mathbb{Q}$, C intersects the hyperplane defined by $X_1 - p_1 = 0$ else it contains a bounded limit of $K(\Pi_1, \mathcal{H}_t)$ when t tends to 0.*

The proof follows the one of Lemma 1 (see also [29]).

Proof. Since $\Pi_1(C)$ is closed, if its boundary is empty for any rational $p_1 \in \mathbb{Q}$, C intersects the hyperplane defined by $X_1 - p_1 = 0$. Suppose now the frontier of $\Pi_1(C)$ is not empty. Choose $p \in \mathbb{R} \notin \Pi_1(C)$, consider H the hyperplane defined by $X_1 - p = 0$ and $\mathcal{M} \subset C$ the set of points in C minimizing the distance from C to H. Let $r > 0$ be such that the set of points $T = \{x \in \mathbb{R}^n \mid \text{dist}(x, \mathcal{M} \leq r\}$ does not meet $(\mathcal{H}_0 \cap \mathbb{R}^n) \setminus C$. Denoting by $T' = \{x \in \mathbb{R}^n \mid \text{dist}(x, \mathcal{M}\}$ and by ε an infinitesimal, remark that the set of points

$(\mathcal{H}_\varepsilon \cup \mathcal{H}_{-\varepsilon}) \cap T'$ is infinitesimally close $\mathcal{H}_0 \cap T'$ and are not at minimal distance to H. Thus the minimal distance from $(\mathcal{H}_\varepsilon \cup \mathcal{H}_{-\varepsilon}) \cap T'$ to H is not obtained on T'. Thus it is obtained at a critical point of the projection Π_1 restricted to $\mathcal{H}_\varepsilon \cup \mathcal{H}_{-\varepsilon}$. Using the transfer principle and remarking the above reasonning is valid for any r small enough ends the proof.

□

The following lemma generalizes the above one. Given an arbitrary point $(p_1, \ldots, p_{n-1}) \in \mathbb{Q}^{n-1}$, for $i \in \{1, \ldots, n-1\}$ denote by $H_i \subset \mathbb{C}^n$ the intersection of the hyperplanes defined by $X_1 - p_1 = \cdots = X_i - p_i = 0$.

Lemma 4 *Let C be a connected component of $\mathcal{H}_0 \cap \mathbb{R}^n$. Suppose for all $i \in \{1, \ldots, n-1\}$ the projection $\Pi_i(C)$ is closed and for any connected component C' of $(\mathcal{H}_0 \cap H_i) \cap \mathbb{R}^n$, $\Pi_{i+1}(C')$ is closed.*
Then, either C contains a limit of $K(\Pi_1, \mathcal{H}_t)$ when t tends to 0 or there exists $i \in \{1, \ldots, n-2\}$ such that $C \cap H_i$ contains a bounded limit of $K(\Pi_{i+1}, \mathcal{H}_t \cap H_i)$ or $\mathcal{H}_t \cap H_{n-1}$.

Proof. Suppose for all $i \in \{1, \ldots, n-1\}$, $\Pi_i(C) = \mathbb{R}^i$. Then C has a non-empty intersection with $\mathcal{H}_0 \cap H_{n-1}$ which is a finite set of points containing the bounded limits of $\mathcal{H}_t \cap H_{n-1}$.

Now, suppose there exists $i \in \{1, \ldots, n-1\}$ such that $\Pi_i(C) \neq \mathbb{R}^i$ and consider the minimum i for which $\Pi_i(C) \neq \mathbb{R}^i$. Remark that $C \cap H_{i-1} \neq \emptyset$. Consider a connected component C' of $C \cap H_i$. Since $C' \subset \mathbb{C}$ and $\Pi_i(C) \neq \mathbb{R}^i$ while $\Pi_{i-1}(C) = \mathbb{R}^{i-1}$, the projection on C' on the X_{i+1}-axis is not $\mathbb{R}$.
From now on, C' is seen as a semi-algebraic set of $\mathbb{R}^{n-i}$ and let π_{i+1} be the canonical projection $\pi_{i+1} : \mathbb{C}^{n-i} \to \mathbb{C}$ sending $(x_{i+1}, \ldots, x_n)$ to x_{i+1}. Moreover, by assumption, $\pi_{i+1}(C')$ is closed. It is now sufficient to apply Lemma 3 and [37, Lemma 10] to C' and $\mathcal{H}_0 \cap H_i$ seen as a hypersurface of $\mathbb{C}^{n-i}$.

□

Lemma 5 *Let $\mathcal{V} \subset \mathbb{C}^n$ be an algebraic variety of dimension d, $\mathrm{Sing}(\mathcal{V})$ be its singular locus and suppose for $i = 1, \ldots, d$ the projections Π_i restricted to the Zariski-closure of $K(\Pi_{i+1}, \mathcal{V}) \setminus \mathrm{Sing}(\mathcal{V})$ to be proper. Let C be a connected component of $\mathcal{V} \cap \mathbb{R}^n$. For $i = 1, \ldots, n-1$ let x be a point in the frontier of $\Pi_i(C)$. Then, either x belongs to $\Pi_i(K(\Pi_{i+1}, \mathcal{V}) \setminus \mathrm{Sing}(\mathcal{V}))$ else x belongs to $\Pi_i(\mathrm{Sing}(\mathcal{V}))$ (where by convention $K(\Pi_{d+1}, \mathcal{V}) = \mathcal{V}$.*

We adapt the proof of [35, Proposition 4] which provides a similar result in the smooth case.
Proof. Let us denote this property by $\mathfrak{Q}_i$. We prove it by decreasing induction on $i = d, \ldots, 1$. First, we prove $\mathfrak{Q}_d$. Let $x \in \mathbb{R}^d$ be in the frontier of $\Pi_d(C)$. By assumption, the restriction of Π_d to $\mathcal{V} \cap \mathbb{R}^n$ is proper, so x is in the image $\Pi_d(C)$. Thus, from the implicit function theorem, either there exists a critical point $y \in C$ of Π_d restricted to $\mathcal{V}$ such that $\pi_d(y) = x$ or there exists a singular point y such that $\Pi_d(y) = x$. This proves $\mathfrak{Q}_d$.
We now assume $\mathfrak{Q}_{i+1}$, and prove $\mathfrak{Q}_i$. Let thus $x \in \mathbb{R}^i$ be in the frontier of $\Pi_i(C) \subset \mathbb{R}^i$.
Let φ be the projection $\varphi : \mathbb{R}^{i+1} \to \mathbb{R}^i$ that maps $(x_1, \ldots, x_{i+1})$ to $(x_1, \ldots, x_i)$; for $r > 0$, we denote by $B_r \subset \mathbb{R}^i$ the closed ball centered at x of radius r, and by $C_r \subset \mathbb{R}^{i+1}$ the preimage $\varphi^{-1}(B_r)$, which is a cylinder.

By definition, for $r > 0$, $\Pi_i^{-1}(B_r)$ meets C, so C_r meets $\Pi_{i+1}(C)$. On the other hand, since x is in the frontier of $\Pi_i(C)$, there exists a point in B_r that is not $\Pi_i(C)$, so there exists a point in C_r that is not in $\Pi_{i+1}(C)$. We deduce that for $r > 0$, C_r meets the frontier of $\Pi_{i+1}(C)$.
By induction hypothesis, there exists $y_r \in (K(\Pi_{i+1}, \mathcal{V}) \cup \mathrm{Sing}(\mathcal{V})) \cap C$ such that $\Pi_{i+1}(y_r) \in C_r$. Applying φ, we deduce that $\Pi_i(y_r) \in B_r$. Since this holds for all $r > 0$, x is in the closure of $\Pi_i(K(\Pi_{i+1}, \mathcal{V}) \cap C) \cup \Pi_i(\mathrm{Sing}(\mathcal{V})$. By assumption, the restriction of Π_i to the Zariski-closure of $K(\Pi_{i+1}, \mathcal{V}) \setminus \mathrm{Sing}(\mathcal{V})$ is proper, so its image by Π_i is closed. Thus either x is in $\Pi_i(K(\Pi_{i+1}, \mathcal{V}) \setminus \mathrm{Sing}(\mathcal{V}) \cap C) \subset \Pi_i(C)$ or it belongs to $\Pi_i(\mathrm{Sing}(\mathcal{V}))$.

□

We identify a linear change of variables to its associated matrix $\mathbf{A} \in GL_n(\mathbb{Q})$ and, given an algebraic variety $\mathcal{V} \subset \mathbb{C}^n$ we denote by $\mathcal{V}^{\mathbf{A}}$ the algebraic variety obtained after the action of $\mathbf{A}$. In the sequel, $\mathrm{Sing}(\mathcal{V})$ denotes the singular locus of $\mathcal{V}$.

Lemma 6 *Let $\mathcal{V} \subset \mathbb{C}^n$ be an algebraic variety. There exists a Zariski-closed subset $\mathcal{A}$ of $GL_n(\mathbb{C})$ such that if any $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, given any connected component $C^{\mathbf{A}}$ of $\mathcal{V}^{\mathbf{A}}$ for all $i \in \{1, \ldots, n-1\}$, $\Pi_i(C^{\mathbf{A}})$ is closed.*

Proof. The proof is done by induction on the dimension d of $\mathcal{V}$. If $\mathcal{V}$ has dimension 0, the conclusion is obvious. Now, suppose the result to be true for any algebraic variety of dimension $d-1$ and let $\mathcal{V} \subset \mathbb{C}^n$ be an algebraic variety of dimension d.
From [35, Theorem 1], given any equi-dimensional algebraic variety $\mathcal{V} \subset \mathbb{C}^n$ of dimension d, there exists a Zariski-closed algebraic subset $\mathcal{A}'$ such that for any $A \in GL_n(\mathbb{Q}) \setminus \mathcal{A}'$ and $i \in \{1, \ldots, d\}$ the projections Π_i restricted to the Zariski closure of $K(\Pi_{i+1}, \mathcal{V}^{\mathbf{A}}) \setminus \mathrm{Sing}(\mathcal{V}^{\mathbf{A}})$ is proper. From Lemma 5, for $i = 1, \ldots, d-1$, if x belongs to the frontier of $\Pi_i(C^{\mathbf{A}})$, then either x belongs to $K(\Pi_{i+1}, \mathcal{V}^{\mathbf{A}}) \setminus \mathrm{Sing}(\mathcal{V}^{\mathbf{A}})$ or x belongs $\mathrm{Sing}(\mathcal{V}^{\mathbf{A}})$ which has dimension less than d.
Thus, one can apply the induction hypothesis on the singular locus of $\mathcal{V}$ and conclude that there exists a Zariski-closed subset of $GL_n(\mathbb{C})$ such that for any $\mathbf{A}' \in GL_n(\mathbb{Q}) \setminus \mathcal{A}'$ and for $i = 1, \ldots, n-1$ the images of the connected components of $\mathrm{Sing}(\mathcal{V})^{\mathbf{A}'}$ by Π_i are closed. It is now sufficient to choose $\mathbf{A}$ such that $\mathbf{A} \notin \mathcal{A} \cup \mathcal{A}'$ to end the proof.

□

Lemma 7 *Let $(p_1, \ldots, p_{n-1})$ be an arbitrary point of $\mathbb{Q}^{n-1}$. There exists a Zariski-closed subset $\mathcal{A}$ of $GL_n(\mathbb{C})$ such that for $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, the ideals $I_i^{\mathbf{A}}$ (for $i = 0, \ldots, n-1$) have dimension 1 and the ideals $\langle f^{\mathbf{A}}, X_1 - p_1, \ldots, X_i - p_i \rangle + I_i^{\mathbf{A}}$ have dimension 0 for $i = 0, \ldots, n$.*

Proof. The fact that $I_{n-1}^{\mathbf{A}}$ is zero-dimensional is obvious.
Given $(p_1, \ldots, p_{n-1})$, for $i = 1, \ldots, n-2$, f_i denotes the polynomial f where the variables $X_1, \ldots, X_j$ are instanciated to $p_1, \ldots, p_i$. Consider the mapping

$$\begin{array}{rccc} \psi : & \mathbb{C}^n \times \mathbb{C} & \to & \mathbb{C}^n \\ & (x = (x_1, \ldots, x_n), \ell) & \to & \left(\ell . \frac{\partial f}{\partial X_1}(x), \ldots, \ell . \frac{\partial f}{\partial X_n}(x)\right) \end{array}$$

and the mappings (for $i = 1, \ldots, n-2$)

$$\begin{array}{rccc} \psi_i : & \mathbb{C}^{n-i} \times \mathbb{C} & \rightarrow & \mathbb{C}^{n-i} \\ & (x = (x_{i+1}, \ldots, x_n), \ell) & \rightarrow & \left(\ell.\frac{\partial f_i}{\partial X_{i+1}}(x), \ldots, \ell.\frac{\partial f_i}{\partial X_n}(x)\right) \end{array}$$

From Sard's theorem, for $i = 0, \ldots, n-2$ there exist Zariski-closed subsets $\mathcal{A}_i$ in $\mathbb{C}^{n-i}$ such that for any vector $(a_{i+1}, \ldots, a_n) \in \mathbb{Q}^{n-i} \setminus \mathcal{A}_i$ the ideal generated by:

$$\left(L.\frac{\partial f}{\partial X_1} - a_1, \ldots, L.\frac{\partial f}{\partial X_n} - a_n\right)$$

and the ideals

$$\left(L.\frac{\partial f_i}{\partial X_{i+1}} - a_{i+1}, \ldots, L.\frac{\partial f_i}{\partial X_n} - a_n\right)$$

are equidimensional and have dimension 1. Considering the same mappings restricted to the regular locus of $\mathcal{H}_0$ allows to prove by the same way that the ideal:

$$\langle f\rangle + \left(\langle L.\frac{\partial f}{\partial X_1} - a_1, \ldots, L.\frac{\partial f}{\partial X_n} - a_n\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]\right)$$

and the ideals

$$\langle f_i\rangle + \left(\langle L.\frac{\partial f_i}{\partial X_{i+1}} - a_{i+1}, \ldots, L.\frac{\partial f_i}{\partial X_n} - a_n\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]\right)$$

have dimension 0 (for $i = 0, \ldots, n-2$).
It is now sufficient to perform a linear change of variables $\mathbf{A}$ sending the vectors $(a_1, \ldots, a_n)$, $\ldots$, $(0, \ldots, 0, a_{i+1}, \ldots, a_n)$, $\ldots$, $(0, \ldots, 0, a_n)$ to the canonical basis to end the proof and to remark for $i = 1, \ldots, n-2$ that if the ideals

$$\left(\langle L.\frac{\partial f_i}{\partial X_{i+1}} - a_{i+1}, \ldots, L.\frac{\partial f_i}{\partial X_n} - a_n\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]\right)$$

(resp. $\langle f_i\rangle + \left(\langle L.\frac{\partial f_i}{\partial X_{i+1}} - a_{i+1}, \ldots, L.\frac{\partial f_i}{\partial X_n} - a_n\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]\right)$) are equidimensional and have dimension 1 (resp. 0) then the same conclusion holds for the ideals $I_i^{\mathbf{A}}$ (resp. $\langle f^{\mathbf{A}}, X_1 - p_1, \ldots, X_i - p_i\rangle + I_i^{\mathbf{A}}$).

□

Proof of Theorem 3. From Lemma 6 applied to $\mathcal{H}_0$ and to each hypersurface $\mathcal{H}_0 \cap H_i$ for $i = 1, \ldots, n-1$ (where H_i is the hyperplane defined by $X_1 = p_1, \ldots, X_i = p_i$, $p_1, \ldots, p_n$ being arbitrary rationals), there exists a Zariski-closed subset $\mathcal{A} \subset GL_n(\mathbb{C})$ such that for $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ the conclusions of Lemmata 4 and 7 and then Theorem 1 hold. Thus, we are done.

□

Remark 2 *From the algorithmic remarks provided in Section 2 and Theorem 3, one deduces an algorithm using either Gröbner bases or geometric resolutions to compute at least one point in each connected component of the real algebraic set* $\mathcal{H}_0 \cap \mathbb{R}^n$.
Given $(p_1, \ldots, p_{n-1}) \in \mathbb{Q}^{n-1}$, *denote by* f_i *(for* $i = 1, \ldots, n-1$*) the polynomial* f *where the indeterminates* $X_1, \ldots, X_i$ *are instantiated to* $p_1, \ldots, p_i$. *Then, remark that the use of geometric resolution can be simplified since it is enough to give as input to the algorithm of [17] the polynomial systems of equalities and inequations:*

$$f_i^{\mathbf{A}} = \frac{\partial f_i^{\mathbf{A}}}{\partial X_{i+2}} = \cdots = \frac{\partial f_i^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f_i^{\mathbf{A}}}{\partial X_{i+1}} \neq 0$$

(for $i = 1, \ldots, n-2$*) and* $f^{\mathbf{A}} = \frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$ *and to isolate the real roots of the univariate polynomial* $f_{n-1}^{\mathbf{A}}$.
At last, note that an alternative strategy can be to introduce an infinitesimal ε, *computing rational parametrizations for the polynomial systems:*

$$f_i^{\mathbf{A}} - \varepsilon = \frac{\partial f_i^{\mathbf{A}}}{\partial X_{i+2}} = \cdots = \frac{\partial f_i^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f_i^{\mathbf{A}}}{\partial X_{i+1}} \neq 0$$

(for $i = 1, \ldots, n-2$*) and*

$$f^{\mathbf{A}} - \varepsilon = \frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$$

and compute the bounded limits of the solution sets of these systems when ε *tends to* 0, *and the real solutions of* $f_{n-1}^{\mathbf{A}} = 0$. *In the following section we show that the above strategy is better.*

4 Complexity estimates

We provide here complexity estimates for the above algorithms computing at least one point in each connected component of a real algebraic set defined by a single equation.
The description of the algorithms relying on Theorem 2 and Theorem 3 given above does not depend on any procedure of algebraic elimination. Following the algorithmic remarks of Section 2, one can use Gröbner bases which allow to compute Rational Univariate Representation following [28] or geometric resolutions. In both bases, the output has the form of the following rational parametrization

$$q(T) = 0, \quad \begin{cases} \frac{\partial q}{\partial T}.X_1 = q_1(T) \\ \qquad \vdots \\ \frac{\partial q}{\partial T}.X_n = q_n(T) \end{cases}$$

from which one can count and isolate the real solutions using variants of Uspensky's algorithm (see [31] and references therein) or Sturm-Habicht sequences (see [7] and references

therein) in time which is polynomial in the degree of the polynomial q in the above rational parametrization.
Thus, the complexity of our algorithms depends on the one of the algebraic elimination procedure we use. We focus on geometric resolutions for which a theoretical complexity result we recall below is provided in [17] and generalized in [25]. Given a system of polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ in generic coordinates

$$g_1 = \cdots = g_n = 0, \quad h \neq 0$$

it computes a rational parametrization of the complex solution set of this system. It is based on an incremental process of lifing and intersection computing at each step a lifted curve, encoded by a parametrized geometric resolution, for the Zariski-closure of the polynomial systems at which $n - i - 1$ generic coordinated are instantiated:

$$g_1 = \cdots = g_i = 0, \quad h \neq 0$$

In the sequel, the quantity $\mathcal{U}(a)$ stands for $a \log^2(a) \log(\log(a))$.

Theorem 4 *[17] Let $(g_1, \ldots, g_s, h)$ be $s+1$ polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree bounded by D, and $\mathcal{L}$ be the complexity of evaluating $(g_1, \ldots, g_s, h)$. Suppose $(g_1, \ldots, g_n)$ defines a regular sequence in the open subset $\{x \in \mathbb{C}^n \mid g \neq 0\}$.*
There exists a probabilistic algorithm computing a geometric resolution of the Zariski-closure of the solution set of $g_1 = \cdots = g_s = 0, \quad h \neq 0$ in a complexity within

$$\mathcal{O}\left(n(n\mathcal{L} + n^4)\mathcal{U}(D.\delta)^2\right)$$

arithmetic operations in $\mathbb{Q}$ where δ is the maximum degree of the Zariski-closure of the complex solution set of the intermediate polynomial systems $g_1 = \cdots = g_i = 0, \quad h \neq 0$ and is dominated by D^n.

Given a parametric geometric resolution encoding a lifted curve, the following result [17, Lemma 16] provides the complexity of computing a geometric resolution of the intersection of this curve and a hypersurface, when this intersection is zero-dimensional.

Lemma 8 *[17] Let C be a geometric resolution of a 1 equi-dimensional ideal I, f be a polynomial of total degree D such that $I + \langle f \rangle$ is zero-dimensional.*
There exists an algorithm computing a geometric resolution of $\sqrt{I + \langle f \rangle}$ whose complexity is in

$$\mathcal{O}\left(n(\mathcal{L} + n^2)\mathcal{U}(\delta)\mathcal{U}(D.\delta)\right)$$

arithmetic operations in $\mathbb{Q}$.

In the sequel, we show how to use these results to provide complexity estimations of the algorithms based on Theorems 2 and 3 to provide at least one point in each connected component of a real algebraic set defined by a single equation.

We first study the algorithm relying on Theorem 2. It consists in choosing a *generic* point $A = (a_1, \ldots, a_n)$ and, for all $i \in \{1, \ldots, n\}$ compute first a lifted curve of the Zariski-closure of the solution set of:

$$\left(\frac{\partial f}{\partial X_i}(X_j - a_j) - \frac{\partial f}{\partial X_j}(X_i - a_i) = 0 \right)_{j \in \{1,\ldots,n\} \setminus \{j\}}, \quad \frac{\partial f}{\partial X_i} \neq 0$$

From [3], these polynomial systems satisfy the requirements needed to apply Theorem 4. It remains to intersect this lifted curve with the hypersurface defined by $f = 0$. Moreover, given a straight-line program of length $\mathcal{L}$, computing a straight-line encoding the gradient of f is linear in $\mathcal{L}$ [8]. Combining this discussion with Theorem 4 and Lemma 8, this leads to the following complexity estimate:

Theorem 5 *Let f be a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree bounded by D, whose complexity of evaluation is bounded by $\mathcal{L}$ and $\mathcal{H} \subset \mathbb{C}^n$ be the hypersurface defined by $f = 0$. The above algorithm computes at least one point in each connected component of $\mathcal{H} \cap \mathbb{R}^n$ within*

$$\mathcal{O}\left(n^2(n\mathcal{L} + n^4)\mathcal{U}(D.\delta)^2\right)$$

arithmetic operations in $\mathbb{Q}$ where δ is the maximal degree of the studied intermediate algebraic varieties and is bounded by D^n.

The algorithm relying on Theorem 3 consists in chosing a *generic* matrix $\mathbf{A} \in GL_n(\mathbb{Q})$, an arbitrary point $(p_1, \ldots, p_{n-1}) \in \mathbb{Q}^{n-1}$ and for $i \in \{1, \ldots, n-2\}$ computing lifted curves encoded by parametrized geometric resolutions for the polynomial systems

$$\frac{\partial f^{\mathbf{A}}}{\partial X_{i+2}} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = X_1 - p_1 = \cdots = X_i - p_i = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_{i+1}} \neq 0$$

and

$$\frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$$

and to intersect each of these lifted curves with the hypersurface defined by $f^{\mathbf{A}} = 0$. Additionally, one has to isolate the real solutions of the univariate polynomial obtained by instantiating in $f^{\mathbf{A}}$ the indeterminates $X_1, \ldots, X_{n-1}$ to $p_1, \ldots, p_{n-1}$. Moreover, given a straight-line program of length $\mathcal{L}$ [8], computing a straight-line encoding the gradient of f is linear in $\mathcal{L}$. This discussion leads to the following complexity estimate.

Theorem 6 *Let f be a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree bounded by D, whose complexity of evaluation is bounded by $\mathcal{L}$ and $\mathcal{H} \subset \mathbb{C}^n$ be the hypersurface defined by $f = 0$. The above algorithm computes at least one point in each connected component of $\mathcal{H} \cap \mathbb{R}^n$ within*

$$\mathcal{O}\left(n^2(n\mathcal{L} + n^4)\mathcal{U}(D.\delta)^2\right)$$

arithmetic operations in $\mathbb{Q}$ where δ is the maximal degree of the intermediate algebraic varieties studied during the incremental process and is bounded by $D.(D-1)^{n-1}$.

Remark 3 *Let $\mathfrak{d}$ be the sum of the degrees of the equi-dimensional components of the singular locus of $\mathcal{H}_0$ having positive dimension. One can refine the above degree bound by remarking that the degree of the curve defined as the Zariski-closure of the solution set of:*

$$\frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$$

is bounded by $(D-1)^{n-1} - \mathfrak{d}$. Thus, while in the smooth case the degree bound $D.(D-1)^{n-1}$ can be reached, it can not in the case where $\mathcal{H}_0$ has a positive dimensional singular locus.

From these results, it appears the strategy based on Theorem 3 than the one based on Theorem 2: degree bounds for the one based on Theorem 3 are better than the ones obtained in Theorem 2.

Comparison with Basu/Pollack/Roy's algorithm. There exist asymptotically optimal algorithm dealing with our problem since [18]. The algorithm which is known to have the best theoretical complexity is the one of Basu, Pollack and Roy provided in [5] (see also [6, 7]) having a complexity within $D^{\mathcal{O}(n)}$ in terms of arithmetic operations in $\mathbb{Q}$. It is important to precise what influences the constant of complexity which is here as exponent. First, the authors reduce their study to a polynomial system having *systematically* $(2D).(2D-1)^{n-1}$ complex solutions. This degree is larger than our degree bound which is D^n. To solve this zero-dimensional system, operations of linear algebra are performed. Thus, a part of the constant of complexity comes from the superfleous factor 2^{3n}. Moreover, in this algorithm, computations are performed over an arithmetic involving two infinitesimals which can appear, in the worst cases, with degree $(2D).(2D-1)^{n-1}$. Then, an other constant in the complexity of [5] comes from this other superfleous factor $\left((2D).(2D-1)^{n-1}\right)^2$. Taking $n=4$ and $D=2$, it is easy to see that even there does not seem to be a difference between the asymptotic complexities of our contribution and [5], our algorithm allows to gain a factor of $2^{12}.(4.3^3)^2$ (which is greater than 47 million) compared to [5] and this gain grows when n and/or D grows.

Comparison with the introduction of infinitesimals. The strategies introducing an infinitesimal deformation using either quadratic mappings or projection functions lead to compute parametric geometric resolutions (where the infinitesimal ε is the parameter). Following [38, 39], this can be done by an asymptotically optimal complexity using the procedure which consists in computing an initial geometric resolution C_0 obtained by instantiating ε to a generic rational value and perform Rational Reconstruction via Padé approximation. The complexity of the computation of C_0 equals the complexity of computing the geometric resolutions we return in the algorithms above. Thus the final step of Rational reconstruction is superfluous. Moreover, the required precision is the maximal of the sum of degree of numerators and denominators of the reconstructed coefficients. This maximal sum is dominated in the worst case by D^n. Once this parametric geometric resolution is computed, one has to compute the bounded limits of the encoded solutions when ε tends to 0. This discussion justifies our approach compared to the one introducing an infinitesimal.

Implementation. A first implementation of the algorithm relying on Theorem 3 is already available in the `RAGLib` Maple package [33]. It is based on Gröbner bases computations using the `Gb` software [11] implemented by J.-C. Faugère and Rational Univariate Representations using the `RS` software [26] implemented by F. Rouillier. This choice is motivated by the fact that, at the time being, the most efficient softwares performing algebraic elimination are based on the algorithms [12, 13] computing Gröbner bases.
Practical experiments show its efficiency compared to previous contributions dealing with the singular case using either infinitesimal deformations (see [29]) or studying recursively singular loci (see [1]). Implementing the algorithm using the `Kronecker` Magma package [23] is a work in progress.

References

[1] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6):543–560, 2002.

[2] 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.

[3] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties and efficient real elimination procedure. *Kybernetika*, 40(5):519–550, 2004.

[4] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties: Geometry and algorithms. *to appear in Journal of complexity*, 2005.

[5] 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.

[6] 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 *Quantifier elimination and cylindrical algebraic decomposition*. Springer-Verlag, 1998.

[7] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*. Springer-Verlag, 2003.

[8] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoret. Comput. Science*, 22:317–330, 1982.

[9] S. Corvez and F. Rouillier. Using computer algebra tools to classify serial manipulators. In F. Winkler, editor, *Automated Deduction in Geometry*, volume 2930 of *Lecture Notes in Artificial Intelligence*, pages 31–43. Springer, 2003.

[10] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties and algorithms : an introduction to computational algebraic geometry and commutative algebra*. Springer-Verlag, 1992.

[11] J.-C. Faugère. Gb/FGb. available at `http://fgbrs.lip6.fr`.

[12] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4).-. *Journal of Pure and Applied Algebra*, 139(1–3):61–88, 1999.

[13] J.-C. Faugère. A new efficient algorithm for computing Gröbner without reduction to zero (F5). In *Proceedings of ISSAC 2002*, pages 75 – 83. ACM Press, 2002.

[14] 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*, number 117, 118 in Journal of Pure and Applied Algebra, pages 277–317, 1997.

[15] 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.

[16] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. When polynomial equation systems can be solved fast? In *Proceedings of AAECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

[17] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.

[18] D. Grigoriev and N. Vorobjov. Solving systems of polynomials inequalities in subexponential time. *Journal of Symbolic Computation*, 5:37–64, 1988.

[19] J. Heintz, M.-F. Roy, and P. Solernò. On the complexity of semi-algebraic sets. In *Proceedings IFIP'89 San Francisco, North-Holland*, 1989.

[20] J. Heintz, M.-F. Roy, and P. Solernò. On the theoretical and practical complexity of the existential theory of the reals. *The Computer Journal*, 36(5):427–431, 1993.

[21] Z. Jelonek. Topological characterization of finite mappings. *Bull. Polish Acad. Sci. Math.*, 49(3):279–283, 2001.

[22] D. Lazard and F. Rouillier. Solving parametric polynomial systems. Technical report, INRIA, 2004.

[23] G. Lecerf. `Kronecker` magma package for solving polynomial systems. available at `http://www.math.uvsq.fr/ lecerf/software/`.

[24] G. Lecerf. *Une alternative aux méthodes de réécriture pour la résolution des systèmes algébriques.* PhD thesis, École polytechnique, 2001.

[25] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *Journal of Complexity*, 19(4):564–596, 2003.

[26] F. Rouillier. RS, RealSolving. available at `http://fgbrs.lip6.fr`.

[27] F. Rouillier. *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux.* PhD thesis, Université de Rennes I, 1996.

[28] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *AAECC Journal*, 9(5):433–461, 1999.

[29] 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.

[30] F. Rouillier, M. Safey, and É. Schost. Solving the birkhoff interpolation problem via the critical point method: An experimental study. In J. Richter-Gebert and D. Wang, editors, *Automated Deduction in Geometry - Third International Workshop ADG 2000, Zurich Switzerland, September 2000, Revised Papers*, number 2061 in Lecture Notes in Artificial Intelligence, pages 26–40. Springer, 2001.

[31] F. Rouillier and P. Zimmermann. Efficient isolation of polynomial real roots. *Journal of Computational and Applied Mathematics*, 162(1):33–50, 2003.

[32] M. Safey El Din. *Résolution réelle des systèmes polynomiaux de dimension positive.* PhD thesis, Université Paris 6, January 2001.

[33] M. Safey El Din. RAGLib (Real Algebraic Geometry Library). available at `http://www-calfor.lip6.fr/~safey/RAGLib`, 2003.

[34] M. Safey El Din. Generalized critical values and solving polynomial inequalities. In *Proceedings of ICPSS, Extended abstract.* Paris 6 University, 2004.

[35] 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 *Proceedings of the 2003 international symposium on Symbolic and algebraic computation*, pages 224–231. ACM Press, 2003.

[36] M. Safey El Din and É. Schost. Properness defects of projections and computation of one point in each connected component of a real algebraic set. *Journal of Discrete and Computational Geometry*, 2004.

[37] M. Safey El Din and P. Trébuchet. Strong bi-homogeneous Bézout theorem and its use in effective real algebraic geometry. *submitted to Journal of complexity*, 2004.

[38] É. Schost. *Sur la résolution des systèmes polynomiaux à paramétres.* PhD thesis, École polytechnique, 2000.

[39] É. Schost. Computing parametric geometric resolutions. *Journal of Applicable Algebra in Engineering, Communication and Computing 13(5): 349 - 393, 2003*, 13(5):349–393, 2003.

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399