

Putting into practice deformation techniques for the computation of sampling points in real singular hypersurfaces

M. Safey El Din*

LIP6 (CalFor), Université Pierre et Marie Curie
INRIA/LIP6 SALSA Project,
Case 168, 4, Place Jussieu,
F-75252 Paris Cedex
France

November 6, 2005

Abstract

Let f be a polynomial in $\mathbb{Q}[X_1, \dots, X_n]$ of degree D and, for $t \in \mathbb{Q}$, $\mathcal{H}_t \subset \mathbb{C}^n$ the hypersurface defined by $f - t = 0$. We provide a probabilistic algorithm computing at least one point in each connected component of $\mathcal{H}_0 \cap \mathbb{R}^n$, without any smoothness assumption on \mathcal{H}_0 whose worst-case complexity is within $\mathcal{O}(n^2(\mathcal{L} + n^3)(\mathcal{U}(D, \delta))^2)$ arithmetic operations in \mathbb{Q} (where $\mathcal{U}(p)$ denotes the cost of multiplying two univariate polynomials of degree p with coefficients in \mathbb{Q} , δ is an intrinsic geometric degree and \mathcal{L} the length of a straight-line program encoding f). This algorithm generalizes the one of Safey El Din and Schost based on critical points of projection functions to compute sampling points in smooth real algebraic sets.

As a by-product, we also prove that given H_1, \dots, H_{n-2} generic hyperplanes of \mathbb{Q}^n , the 0-th Betti number of $\mathcal{H}_0 \cap \mathbb{R}^n$ is bounded by $D(1 + (D - 1) + \dots + (D - 1)^{n-1} - (\mathfrak{d}_0 + \dots + \mathfrak{d}_{n-2}))$ where for $i = 1, \dots, n - 2$, \mathfrak{d}_i (resp. \mathfrak{d}_0) denotes the sum of the degree of the *positive equidimensional components* of the singular locus of $\mathcal{H}_0 \cap (\cap_{j=1}^i H_j)$ (resp. \mathcal{H}_0). This is always less than the classical Thom-Milnor bound in singular situations.

*Mohab.Safey@lip6.fr

1 Introduction

Let f be a polynomial in $\mathbb{Q}[X_1, \dots, X_n]$ of degree D and, for $t \in \mathbb{Q}$, let $\mathcal{H}_t \subset \mathbb{C}^n$ be the hypersurface defined by $f - t = 0$.

The core result of this paper is 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 complexity is polynomial in n , D , the evaluation complexity of f and an intrinsic geometric degree which is proved to be strictly less than the Bézout bound D^n when \mathcal{H}_0 has a positive dimensional singular locus. Such a complexity is asymptotically optimal, and an implementation, whose practical behaviour reflects this efficiency, is provided.

Motivation and description of the problem. Computing at least one point in each connected component of a real algebraic set $\mathcal{H}_0 \cap \mathbb{R}^n$ defined by a single equation $f = 0$ is a question of first importance since it is a basic subroutine used in several algorithms dealing with semi-algebraic sets (see [7]). To tackle this problem, we focus on the critical point method. This is based on reducing the problem to compute the critical points of a polynomial mapping reaching its extrema on each connected component of the studied hypersurface $\mathcal{H}_0 \cap \mathbb{R}^n$.

Critical points are algebraically characterized by the vanishing of some minors of a jacobian matrix. Supposing \mathcal{H}_0 to be smooth forbids rank defects on $\text{Jac}(f)$ and makes easier the problem of computing sampling points in $\mathcal{H}_0 \cap \mathbb{R}^n$. The algorithms provided in [26, 3] have a worst-case complexity within $\mathcal{O}(n^3 D^{3n})$ arithmetic operations in \mathbb{Q} which improves the one of [7] whose complexity is within $\mathcal{O}(n^2 (2D)^{5n})$ arithmetic operations in \mathbb{Q} . A more accurate analysis shows the one of [26] is better and an implementation of this algorithm shows its practical efficiency.

Dealing efficiently with singular situations is the main objective of the algorithms provided in [7, 23, 1]. The contributions in [7, 23] deform infinitesimally \mathcal{H}_0 to retrieve a smooth situation, compute sampling points on the deformed hypersurface, and compute the limits of these points when the introduced infinitesimals tend to 0. This leads to asymptotically optimal algorithms. Nevertheless, to perform such computations one has to compute a rational parametrization with infinitesimal coefficients of the critical points on the deformed hypersurface. Such a representation has in general a degree and coefficients bigger than the size of the result. Moreover, the computation of the limits of the critical points on the deformed hypersurface is not immediate since some of them can tend to ∞ (see [23]).

The strategy developed in [1] consists in studying recursively imbricated singular loci on the one hand and computing critical points of mappings re-

stricted to the regular locus of the considered varieties on the other hand. The complexity of this latter approach is not well-controlled.

The aim of this work is to provide an efficient algorithm computing sampling points in singular hypersurfaces, by adapting the results of [26] to singular situations, and avoiding the explicit introduction of an infinitesimal.

Main contributions. We bring here an algorithm computing sampling points in $\mathcal{H}_0 \cap \mathbb{R}^n$, without smoothness assumptions on \mathcal{H}_0 , whose worst-case complexity is within $\mathcal{O}(n^2(D^n + n^3) \cdot \mathcal{U}(D^2(D-1)^{n-1})^2)$ arithmetic operations in \mathbb{Q} . Moreover, we put the emphasis on the surprising fact, we precise below, that the degree bounds, on which the complexity of our algorithm depend, are better in singular situations than in generic ones. A Gröbner-based implementation is available in [25]. Its practical behaviour is more efficient than the ones obtained with previous strategies. An other implementation using the Magma package `Kronecker`[19] is under development and we report at the end of the paper on some experiments based on this package to illustrate our complexity result.

Our approach goes back to [23] which provides an algorithm computing sampling points by deforming the singular hypersurface, computing critical points on this deformed hypersurface which are encoded by a parametric rational parametrization with coefficients in $\mathbb{Q}(\varepsilon)$ and then, compute the limits of these critical points when ε tends to 0. Our first result shows how to avoid this preliminary computation of a rational parametrization with coefficients in $\mathbb{Q}(\varepsilon)$ to compute *directly* the limits of the considered critical points when ε tends to 0.

Given a polynomial $\phi \in \mathbb{Q}[X_1, \dots, X_n]$, and considering the mapping $\phi : \mathbb{C}^n \rightarrow \mathbb{C}$ 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:

$$L \cdot \frac{\partial f}{\partial X_1} - \frac{\partial \phi}{\partial X_1}, \dots, L \cdot \frac{\partial f}{\partial X_n} - \frac{\partial \phi}{\partial X_n}$$

(where L is a new variable) 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:

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

which is zero-dimensional.

We provide algorithmic tools to perform this computation, based on Gröbner bases [10, 11] or geometric resolutions [14, 13, 12, 15, 20]. 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 can strictly contain $K(\phi, \mathcal{H}_0)$.

Then, we use this result to compute at least one point in each connected component of $\mathcal{H}_0 \cap \mathbb{R}^n$ investigating two variants of the critical point method proposed in [23, 1, 4, 3] (using quadratic mappings) and [26] (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 $A = (a_1, \dots, a_n) \in \mathbb{Q}^n$, the algebraic variety associated to the ideal:

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

is zero-dimensional and has a non-empty intersection with each connected component of the real algebraic set $\mathcal{H}_0 \cap \mathbb{R}^n$.

Additionally, we prove that given an arbitrary point $(p_1, \dots, p_{n-1}) \in \mathbb{Q}^{n-1}$ 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 $i = 1, \dots, n-2$, the ideals:

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

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

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

are zero-dimensional and the union of their associated algebraic varieties has a non-empty intersection with 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 (using quadratic mappings) and Theorem 3 (using projection functions) and the elimination techniques of [15] inspired by [14, 13, 12] and generalized in [20].

Our procedures have a complexity within

$$\mathcal{O}(n^2(n\mathcal{L} + n^4)((1 + h_{\text{sing}})\mathcal{U}(D.\delta)^2 + h_{\text{reg}}\mathcal{U}(\delta)))$$

binary operations where:

- \mathcal{L} is the complexity of evaluating f
- δ is an intrinsic geometric degree bounded by D^n (resp. $D(D-1)^{n-1}$) in the case of the algorithm relying on Theorem 2 (resp. Theorem 3)
- h_{sing} is the maximal bit-size of the coefficients of a geometric resolution encoding singular limits of critical points
- h_{reg} is the maximal bit-size of the coefficients of a geometric resolution encoding singular limits of critical points

Compared to the complexity of the algorithm of [26] one has an overcost coming from $h_{\text{sing}}\delta$. In the case where h_{sing} is proportional to δ one obtains the same complexity than the one we would obtain by introducing an infinitesimal. Nevertheless, h_{sing} is often rather small since in practice it is near the degree of the singular limits of critical points which is less than δ . Note also that degree bounds are better for the algorithm relying on Theorem 3. Moreover, in the case where \mathcal{H}_0 has a positive dimensional singular locus, the intrinsic quantity δ appearing in the solving process of Theorem 3 is bounded by $D(D-1)^{n-1} - (\mathfrak{d}_0 + \dots + \mathfrak{d}_{n-1})$ where, for $i = 1, \dots, n-2$ \mathfrak{d}_i (resp. \mathfrak{d}_0)

We provide complexity estimates for the algorithm relying on Theorem 3). An implementation of this algorithm is already available in [25]. Experiments have shown it has a practical behaviour which is better than the strategy proposed in [1].

Comparison with previous complexity results. Previous contributions [7, 23] dealing with singular hypersurfaces with an asymptotically optimal complexity. We compare here our complexity result with previous ones and show it is exponentially better than the others.

We focus on Basu, Pollack and Roy's algorithm (see [7]) which was known to have the best complexity to compute sampling points on hypersurfaces without any assumption. This algorithm reduces the question to solving a zero-dimensional system with coefficients in a Puiseux series field $\mathbb{Q}\langle\varepsilon, \zeta\rangle$ (where ε and ζ are infinitesimals), which has *always* a degree

$$\mathfrak{D} = \prod_{i=1}^n \max(4, 2 \deg_i(f)) \leq (\max(4, 2D))^n$$

where $\deg_i(f)$ is the partial degree of f in X_i . This resolution is done by means of linear algebra operations in a quotient algebra, so that the complexity is $\mathcal{O}(\mathfrak{D}^3 + n\mathfrak{D}^2)$ arithmetic operations in $\mathbb{Q}(\varepsilon, \zeta)$. In worst cases, the

maximal degree, in ε and ζ , of the coefficients appearing during the computations equals the degree \mathfrak{D} . Thus, the cost of each arithmetic operation in $\mathbb{Q}(\varepsilon, \zeta)$ can at best be bounded by $\mathcal{U}(\mathfrak{D})^2$ (where $\mathcal{U}(p) = p \log^2(p) \log \log(p)$). The complexity of this algorithm is then $\mathcal{O}((\mathfrak{D}^3 + n\mathfrak{D}^2)\mathcal{U}(\mathfrak{D})^2)$ arithmetic operations in \mathbb{Q} . Here, we bring an algorithm computing sampling points in $\mathcal{H}_0 \cap \mathbb{R}^n$, without smoothness assumptions on \mathcal{H}_0 , whose worst-case complexity (which is reached on generic inputs) is within $\mathcal{O}(n^2(D^n + n^3)\mathcal{U}(D^2(D-1)^{n-1})^2)$ arithmetic operations in \mathbb{Q} . On generic inputs, the complexity gain is, up to log factors, equivalent to $(2^{5n}D^{2n})/n^2$ in terms of arithmetic operations in \mathbb{Q} . Taking into account the bit-size of the coefficients which grow linearly in the degree of the studied zero-dimensional ideal on generic inputs, this leads to a complexity gain equivalent to $(2^{6n}D^{2n})/n^2$.

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.

Acknowledgments. We thank J.-C. Faugère and G. Lecerf for helpful comments and suggestions.

2 Computing limits of critical points

Let f be a polynomial in $\mathbb{Q}[X_1, \dots, X_n]$ of degree bounded by D . For $t \in \mathbb{Q}$, denote by $\mathcal{H}_t \subset \mathbb{C}^n$ the hypersurface defined by $f - t = 0$.

Let $\phi : x \in \mathbb{C}^n \rightarrow \phi(x) \in \mathbb{C}$ be a polynomial mapping. For $t \in \mathbb{Q}$, $K(\phi, \mathcal{H}_t)$ 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 $I \subset \mathbb{Q}[L, X_1, \dots, X_n]$ be the ideal generated by the polynomial family:*

$$L \cdot \frac{\partial f}{\partial X_1} - \frac{\partial \phi}{\partial X_1}, \dots, L \cdot \frac{\partial f}{\partial X_n} - \frac{\partial \phi}{\partial X_n}$$

Suppose I 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

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

and I_0 is zero-dimensional.

Proof. Let $C \subset \mathbb{C}^{n+1}$ be the curve defined by I , $\Pi : \mathbb{C}^{n+1} \rightarrow \mathbb{C}^n$ be the projection sending (x_1, \dots, x_n, ℓ) to (x_1, \dots, x_n) and $\mathcal{C} = \Pi(C)$.

Remark that f vanishes at each bounded limit y of $K(\phi, \mathcal{H}_t)$ when $t \rightarrow 0$, Let y be such a limit. If y belongs to $K(\phi, \mathcal{H}_0)$ it is regular and we are done since $K(\phi, \mathcal{H}_0) \subset \mathcal{C}$. Now, suppose $y \notin K(\phi, \mathcal{H}_0)$, which implies $\mathbf{grad}_y(f) = \mathbf{0}$. 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 [18, Lemma 2 and 3] or [17]). This implies y belongs to the Zariski-closure of \mathcal{C} which is the algebraic variety associated to $I \cap \mathbb{Q}[X_1, \dots, X_n]$. Thus, $\mathcal{V}(I_0) \subset \mathbb{C}^n$ contains the bounded limits of $K(\phi, \mathcal{H}_t)$ when t tends to 0.

We prove now that the variety $\mathcal{V}(I_0)$ associated to I_0 is zero-dimensional. 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 [17], the set of points in the Zariski-closure of \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 *The above result is relevant and useful when \mathcal{H}_0 is not smooth since, in this case, the set of bounded limits of $K(\phi, \mathcal{H}_t)$ when $t \rightarrow 0$ can strictly contain $K(\phi, \mathcal{H}_0)$.*

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

Proof. Remark that the polynomial system defining I can be bihomogenized considering L and X_1, \dots, X_n independantly. Then, the announced bound on the degree of I is an immediate consequence of [28, Theorems 1 and 2] which bounds the sum of the degrees of all the equidimensional components of a radical bihomogeneous ideal. Since $\deg(\sqrt{I} \cap \mathbb{Q}[X_1, \dots, X_n]) \leq \deg(\sqrt{I})$ and $\sqrt{I_0} = \sqrt{\langle f \rangle + (\sqrt{I} \cap \mathbb{Q}[X_1, \dots, X_n])}$, we are done.

□

Algorithmic procedure using Gröbner bases. Classical results about Gröbner bases (see [8, Chapter 9]) show that computing a Gröbner basis of I with respect to a monomial Degree Reverse Lexicographic block-ordering

with $[L] > [X_1, \dots, X_n]$ and eliminating polynomials having degree greater than 0 in L provides a Gröbner basis G of $I \cap \mathbb{Q}[X_1, \dots, X_n]$. 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 [20] does not allow us to compute elimination ideals. Nevertheless, it allows localization without adding an extra variable. Remark that the ideal

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

contains the ideal J generated by the set Δ of all $(2, 2)$ minors of the jacobian matrix associated to $\text{Jac}(f, \phi)$. 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 $i \in \{1, \dots, n\}$ such that $\frac{\partial f}{\partial X_i}(y) \neq 0$, then y belongs to the curve associated to $I \cap \mathbb{Q}[X_1, \dots, X_n]$ which is not possible by assumption. Thus, to compute a geometric resolution of $I \cap \mathbb{Q}[X_1, \dots, X_n]$ it is sufficient to saturate J by $\left(\frac{\partial f}{\partial X_1}\right)^2 + \dots + \left(\frac{\partial f}{\partial X_n}\right)^2$. This can be done by giving as input to the algorithm of [20] the following polynomial system of equations and inequations:

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

An alternative strategy consists in computing for $i = 1, \dots, n$ geometric resolutions for: $\Delta, \frac{\partial f}{\partial X_i} \neq 0$. 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 [23, 1, 3]) or projection functions (see also [27, 26, 2]).

Using the distance function. Given a point $A = (a_1, \dots, a_n)$ 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 :

$$\begin{aligned} \phi_A : \quad \mathbb{C}^n &\rightarrow \mathbb{C} \\ (x_1, \dots, x_n) &\rightarrow (x_1 - a_1)^2 + \dots + (x_n - a_n)^2 \end{aligned}$$

Theorem 2 *There exists a Zariski-closed subset \mathcal{A} of \mathbb{C}^n such that for $A = (a_1, \dots, a_n) \in \mathbb{Q}^n \setminus \mathcal{A}$ the algebraic variety associated to the ideal*

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

(where L is a new variable) is zero-dimensional and has a non-empty intersection with 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 [23] 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 us to obtain at least one point in each connected component of $\mathcal{H}_0 \cap \mathbb{R}^n$.

Lemma 1 [23] *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 $A = (a_1, \dots, a_n) \in \mathbb{Q}^n \setminus \mathcal{A}$, the ideal I_A generated by:*

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

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:

$$\begin{aligned} \psi : \quad \mathbb{C}^n \times \mathbb{C} &\rightarrow \mathbb{C}^n \\ (x = (x_1, \dots, x_n), \ell) &\rightarrow \ell \cdot \frac{\partial f}{\partial X_1}(x) - x_1, \dots, \ell \cdot \frac{\partial f}{\partial X_n}(x) - x_n \end{aligned}$$

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

$$\text{rank}(\text{Jac}_{(x, \ell)}(L \cdot \frac{\partial f}{\partial X_1} - (X_1 - a_1), \dots, L \cdot \frac{\partial f}{\partial X_n} - (X_n - a_n))) = n$$

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 in [23], our contribution allows us to avoid computations over an infinitesimal arithmetic.

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 [26] 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:

$$\begin{aligned} \Pi_i : \quad \mathbb{C}^n &\rightarrow \mathbb{C}^i \\ (x_1, \dots, x_n) &\rightarrow (x_1, \dots, x_i) \end{aligned}$$

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

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

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

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

Theorem 3 *Let (p_1, \dots, 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 $i = 0, \dots, n-1$) 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 $\mathcal{H}_0 \cap \mathbb{R}^n$ and suppose $\Pi_1(C)$ is closed. Suppose there exists $t_0 \in]0, +\infty[$ such that for all $t \in]0, t_0[$ and all connected component C_t of $(\mathcal{H}_t \cup \mathcal{H}_{-t}) \cap \mathbb{R}^n$, $\Pi_1(C_t)$ is closed. Then, either for an arbitrary rational $p_1 \in \mathbb{Q}$, C intersects the hyperplane defined by $X_1 - p_1 = 0$ or 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 [23]).

Proof. Since $\Pi_1(C)$ is closed, if its frontier 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 $p \in \mathbb{R} \setminus \Pi_1(C)$, 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 . Since $\Pi_1(C)$ is closed, \mathcal{M} is not empty. 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 $T' = \{x \in \mathbb{R}^n \mid \text{dist}(x, \mathcal{M}) = r\}$ and by ε an infinitesimal, remark that the set of points $(\mathcal{H}_\varepsilon \cup \mathcal{H}_{-\varepsilon}) \cap T'$ is infinitesimally close to $\mathcal{H}_0 \cap T'$ 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' . Since for t small enough, each connected component of $\mathcal{H}_t \cap \mathbb{R}^n$ is supposed to have a closed image by Π_1 , the minimal distance of $(\mathcal{H}_\varepsilon \cup \mathcal{H}_{-\varepsilon}) \cap T$ to H 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 reasoning is valid for any r small enough ends the proof. \square

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

Lemma 4 *Let C be a connected component of $\mathcal{H}_0 \cap \mathbb{R}^n$. Suppose for all $i \in \{1, \dots, n-1\}$ 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. Suppose also that there exists $t_0 \in]0, +\infty[$ such that for all $t \in]0, t_0[$, all connected component C_t of $(\mathcal{H}_t \cup \mathcal{H}_{-t}) \cap \mathbb{R}^n$ and all $i \in \{1, \dots, n-1\}$ the projection $\Pi_i(C_t)$ is closed and for any connected component C'_t of $(\mathcal{H}_t \cup \mathcal{H}_{-t}) \cap H_i \cap \mathbb{R}^n$, $\Pi_{i+1}(C'_t)$ is closed. Then, either C contains a limit of $K(\Pi_1, \mathcal{H}_t)$ when t tends to 0 or there exists $i \in \{1, \dots, n-2\}$ such that $C \cap H_i$ contains a bounded limit of either $K(\Pi_{i+1}, \mathcal{H}_t \cap H_i)$ or $\mathcal{H}_t \cap H_{n-1}$ when t tends to 0.*

Proof. Suppose for all $i \in \{1, \dots, n-1\}$, $\Pi_i(C) = \mathbb{R}^i$. 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 $i \in \{1, \dots, n-2\}$ 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 $C' \subset C$ 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 $\pi_{i+1} : \mathbb{C}^{n-i} \rightarrow \mathbb{C}$ sending (x_{i+1}, \dots, x_n) to x_{i+1} . Moreover, by assumption, $\pi_{i+1}(C')$ is closed. It is now sufficient to apply Lemma 3 to C' and $\mathcal{H}_0 \cap H_i$ seen as a hypersurface of \mathbb{C}^{n-i} . \square

Lemma 5 *Let $\mathcal{V} \subset \mathbb{C}^n$ be an algebraic variety of dimension d , $\text{Sing}(\mathcal{V})$ be its singular locus and suppose for $i = 1, \dots, d$ the projections Π_i restricted to the Zariski-closure of $K(\Pi_{i+1}, \mathcal{V}) \setminus \text{Sing}(\mathcal{V})$ to be proper.*

Consider a connected component C of $\mathcal{V} \cap \mathbb{R}^n$. For $i = 1, \dots, n-1$ let x be a point in the frontier of $\Pi_i(C)$. Then, either x belongs to $\Pi_i(K(\Pi_{i+1}, \mathcal{V}) \setminus \text{Sing}(\mathcal{V}))$ else x belongs to $\Pi_i(\text{Sing}(\mathcal{V}))$ (where by convention $K(\Pi_{d+1}, \mathcal{V}) = \mathcal{V}$).

We adapt the proof of [26, 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 $i = d, \dots, 1$. 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 $\varphi : \mathbb{R}^{i+1} \rightarrow \mathbb{R}^i$ be the projection that maps (x_1, \dots, x_{i+1}) to (x_1, \dots, 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 in $\Pi_i(C)$, 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 $y_r \in (K(\Pi_{i+1}, \mathcal{V}) \cup \text{Sing}(\mathcal{V})) \cap C$ 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 $\Pi_i(K(\Pi_{i+1}, \mathcal{V}) \cap C) \cup \Pi_i(\text{Sing}(\mathcal{V}))$. By assumption, the restriction of Π_i to the Zariski-closure of $K(\Pi_{i+1}, \mathcal{V}) \setminus \text{Sing}(\mathcal{V})$ is proper, so its image by Π_i is closed. Thus either x is in $\Pi_i(K(\Pi_{i+1}, \mathcal{V}) \setminus \text{Sing}(\mathcal{V}) \cap C) \subset \Pi_i(C)$ or it belongs to $\Pi_i(\text{Sing}(\mathcal{V}))$. \square

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, $\text{Sing}(\mathcal{V})$ 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 $i \in \{1, \dots, n-1\}$, $\Pi_i(C^{\mathbf{A}})$ 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 [26, 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 $i \in \{1, \dots, d\}$ the projections Π_i restricted to the Zariski closure of $K(\Pi_{i+1}, \mathcal{V}^{\mathbf{A}}) \setminus \text{Sing}(\mathcal{V}^{\mathbf{A}})$ is proper. From Lemma 5, for $i = 1, \dots, d-1$, if x belongs to the frontier of $\Pi_i(C^{\mathbf{A}})$, then either x belongs to $K(\Pi_{i+1}, \mathcal{V}^{\mathbf{A}}) \setminus \text{Sing}(\mathcal{V}^{\mathbf{A}})$ or x belongs $\text{Sing}(\mathcal{V}^{\mathbf{A}})$ 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 $i = 1, \dots, n-1$ the images of the connected components of $\text{Sing}(\mathcal{V})^{\mathbf{A}'}$ 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 *There exists a Zariski-closed subset $\mathcal{A} \subset GL_n(\mathbb{C})$ and $t_0 \in \mathbb{R}$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ and all $t \in]0, t_0[\cap \mathbb{Q}$, each connected component of \mathcal{H}_t has a closed image by the projection Π_1 .*

Proof. Let $\theta \in \mathbb{Q}$ be generic enough so that \mathcal{H}_θ is smooth. From [26, Theorem 1 and Proposition 4], there exists a Zariski-closed subset $\mathcal{A} \subset GL_n(\mathbb{Q})$ such that the image of any connected component of $\mathcal{H}_\theta^{\mathbf{A}}$ is closed by Π_1 . Remark now that the set of t such that this property is not true for $\mathcal{H}_t^{\mathbf{A}}$ is Zariski-closed since it is contained in the set of reals for which one of the projections (x_1, \dots, x_i) restricted to the critical locus of the projection on (x_1, \dots, x_{i+1}) restricted to the hypersurface defined by $f^{\mathbf{A}} - t$ where $f^{\mathbf{A}}$ is seen as a polynomial with coefficients in $\mathbb{Q}(t)$. □

Lemma 8 *Let (p_1, \dots, 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 $i = 0, \dots, n-1$) have dimension 1 and the ideals $\langle f^{\mathbf{A}}, X_1 - p_1, \dots, X_i - p_i \rangle + I_i^{\mathbf{A}}$ have dimension 0 for $i = 0, \dots, n$.*

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

$$\begin{aligned} \psi : \quad \mathbb{C}^n \times \mathbb{C} &\rightarrow \mathbb{C}^n \\ (x = (x_1, \dots, x_n), \ell) &\rightarrow \left(\ell \cdot \frac{\partial f}{\partial X_1}(x), \dots, \ell \cdot \frac{\partial f}{\partial X_n}(x) \right) \end{aligned}$$

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

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

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

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

and the ideals

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

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

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

and the ideals

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

have dimension 0 (for $i = 0, \dots, n-2$).

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

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

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

□

Proof of Theorem 3. From Lemma 6 and Lemma 7 applied to \mathcal{H}_0 and to each hypersurface $\mathcal{H}_0 \cap H_i$ for $i = 1, \dots, n-1$ (where H_i is the hyperplane defined by $X_1 = p_1, \dots, X_i = p_i$, (p_1, \dots, p_{n-1}) 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 8 (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 $(p_1, \dots, p_{n-1}) \in \mathbb{Q}^{n-1}$, denote by f_i (for $i = 1, \dots, n-1$) the polynomial f where the indeterminates X_1, \dots, X_i are instantiated to p_1, \dots, 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 [15] the polynomial systems of equalities and inequations:

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

(for $i = 1, \dots, n-2$) and $f^{\mathbf{A}} = \frac{\partial f^{\mathbf{A}}}{\partial X_2} = \dots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$ 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:

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

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

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

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 only provide complexity estimates for the algorithm computing at least one point in each connected component of a real algebraic set defined by a single equation relying on Theorem 3 since degree bounds are better for this one than the degree bounds of the one relying on Theorem 2.

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 [22] or geometric resolutions [14, 13, 12, 15, 20]. In both cases, the output has the form of the following rational parametrization

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

from which one can count and isolate the real solutions using variants of Uspensky's algorithm (see [24] 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 [15] and generalized in [20]. Given a system of polynomials in $\mathbb{Q}[X_1, \dots, X_n]$ in generic coordinates

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

it computes a rational parametrization of the complex solution set of this system. It is based on an incremental process of lifting 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 coordinates are instantiated:

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

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

Theorem 4 [15] *Let (g_1, \dots, g_s, h) be $s + 1$ polynomials in $\mathbb{Q}[X_1, \dots, X_n]$ of degree bounded by D , and \mathcal{L} be the complexity of evaluating (g_1, \dots, g_s, h) . Suppose (g_1, \dots, 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 $g_1 = \cdots = g_s = 0$, $h \neq 0$ in a complexity within

$$\mathcal{O}(n(n\mathcal{L} + n^3)\mathcal{U}(D.\delta)^2)$$

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 $g_1 = \cdots = g_i = 0$, $h \neq 0$ and is dominated by D^n .

From Theorem 3, the problem of computing sampling points in $\mathcal{H}_0 \cap \mathbb{R}^n$ is reduced to choosing a random linear change of variables $\mathbf{A} \in GL_n(\mathbb{Q})$, isolate the real solutions of $\mathcal{H}_0^{\mathbf{A}} \cap V(X_1, \dots, X_n)$ and compute the limits of the critical points

$$K(\pi_1, \mathcal{H}_t^{\mathbf{A}}), K(\pi_2, \mathcal{H}_t^{\mathbf{A}} \cap V(X_1)), \dots, K(\pi_{n-1}, \mathcal{H}_t^{\mathbf{A}} \cap V(X_1, \dots, X_{n-2}))$$

when t tends to 0. We describe below a procedure based on the computation of geometric resolutions to compute the limits of critical points of a projection on a line restricted to a hyperurface:

1. Compute a geometric resolution G encoding a generic point in the Zariski-closure of the curve defined by:

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

2. Get the image of G modulo a randomly chosen prime number, compute the intersection with $f^{\mathbf{A}} = 0$, remove the obtained points at which $\frac{\partial f^{\mathbf{A}}}{\partial X_1}$ vanish, and lift the integers using the lifting system:

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

Thus, one gets the regular limits of $K(\Pi_1, \mathcal{H}_t^{\mathbf{A}})$ when t tends to 0.

3. Then compute the intersection of the curve encoded by G with the hypersurfaces defined by $\frac{\partial f^{\mathbf{A}}}{\partial X_1} = 0$ and $f^{\mathbf{A}} = 0$ modulo prime numbers and recover the final result using the Chinese remainder theorem and Rational Reconstruction.

We estimate the complexity of each above step. Let \mathcal{L} be the length of the Straight-Line Program encoding the system:

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

and n be the number of variables. The first step is performed in $\mathcal{O}(n^2(\mathcal{L} + n^2)(\mathcal{U}(D\delta)^2 + h\mathcal{U}(\delta)))$ bit operations, where h is the maximal bit-size of the coefficients of G and δ is the maximal degree of the closure of the algebraic sets:

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

for $i = 2, \dots, n$. Remark that δ is dominated by $(D - 1)^{n-1}$.

The second step has a cost which is $\mathcal{O}(n(\mathcal{L} + n^2)\mathcal{U}(D\delta)(h_{\text{reg}} + \mathcal{U}(D\delta)))$ bit operations where h_{reg} is the bit-size of the maximum of the bit-size of the coefficients of the geometric resolution encoding the regular limits of critical points (see the section about lifting integers and intersecting a lifted curve with a hypersurface in [15]). At last, each computation of the third step has a complexity $\mathcal{O}(n(\mathcal{L} + n^2)h_{\text{sing}}\mathcal{U}(D\delta))$ (see the section about intersecting a lifting curve and a hypersurface in [15]). The number of these computations is h_{sing} , where h_{sing} is the maximal bit-size of the geometric resolution encoding the singular limits of the critical points. Thus, one deduces from this discussion the following complexity result.

Theorem 5 *Let f be a polynomial in $\mathbb{Q}[X_1, \dots, X_n]$ 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*

$$\mathcal{O}(n^2(n\mathcal{L} + n^2)((1 + h_{\text{sing}})\mathcal{U}(D.\delta)^2 + h_{\text{reg}}\mathcal{U}(\delta)))$$

bit-operations 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 equidimensional components of the singular locus of \mathcal{H}_0 having positive dimension. One can refine the above degree bound $D(D - 1)^{n-1}$ dominating δ by remarking that the degree of the curve defined as the Zariski-closure of the solution set of:*

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

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 cannot in the case where \mathcal{H}_0 has a positive dimensional singular locus.

Taking into account the above discussion and performing a careful analysis of degree bounds for the algorithm relying on Theorem 3, this leads to the following result.

Theorem 6 *Let H_1, \dots, H_{n-2} be generic hyperplanes of \mathbb{Q}^n . The number of connected components of the real counterpart of \mathcal{H}_0 is bounded by*

$$D(1 + (D - 1) + \dots + (D - 1)^{n-1} - (\mathfrak{d}_0 + \dots + \mathfrak{d}_{n-2})),$$

where \mathfrak{d}_i (resp. \mathfrak{d}_0) denotes the sum of the degree of the positive-dimensional components of the singular locus of $\mathcal{H}_0 \cap (\cap_{j=1}^i H_j)$ (resp. \mathcal{H}_0).

Comparison with Basu/Pollack/Roy’s algorithm. There exist asymptotically optimal algorithm dealing with our problem since [16]. 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 superfluous 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 superfluous factor $((2D).(2D - 1)^{n-1})^2$. 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 us 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. In worst cases, i.e. when h_{sing} is equivalent to the bit-size of the coefficients of the input multiplied by the degree of the output, our strategy has the same complexity than the one which consists in studying the hypersurface defined by $f - \varepsilon = 0$. Nevertheless, this case does not often occur in practice. Moreover, our strategy avoids the growth of degrees induced by the presence of critical points in the deformed hypersurface which tend to ∞ . This partly explains the good behaviour of our approach.

Implementation. A first implementation of the algorithm relying on Theorem 3 is already available in the `RAGLib` Maple package [25]. It is based on Gröbner bases computations using the `Gb` software [9] implemented by J.-C. Faugère and Rational Univariate Representations using the `RS` software [21]

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 [10, 11] computing Gröbner bases.

Practical experiments show its efficiency compared to previous contributions dealing with the singular case using either infinitesimal deformations (see [23]) or studying recursively singular loci (see [1]).

We present here some experiments using the `Kronecker` Magma package [19] which illustrate our complexity results. The hypersurfaces we study are all singular. The computations have been performed using `Magma V2.10` on a PC Pentium 4 3.2 GHz with 1024 KB of Cache size and 1024 MB of RAM. We provide below the timings (in seconds) for the computation of the limits on a projection on a line which is randomly chosen. The first column contains the number of variables, the second one the degree of the polynomial f defining the studied hypersurface, the third one the degree of the curve being the Zariski-closure of the complex solution set of:

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

the fourth one indicates the number of regular limits, the fifth one the number of singular limits, the sixth one indicates the number of iteration required to recover the singular limits, and the last column indicates the Memory usage. The polynomials are downloadable at:

<http://www-calfor.lip6.fr/~safey/slp/>

	#vars	Deg	DegCurve	DegReg	DegSing	#Iter	Timing	Mem
H1	3	11	3	0	3	3	48sec.	5 MB
H2	5	4	60	60	22	5	97sec.	6.9 MB
H3	3	11	39	8	51	24	2844sec.	10.4MB
H4	5	10	118	198	28	11	1757sec.	14.4MB

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] D. Cox, J. Little, and D. O’Shea. *Ideals, varieties and algorithms : an introduction to computational algebraic geometry and commutative algebra*. Springer-Verlag, 1992.
- [9] J.-C. Faugère. Gb/FGb. available at <http://fgbrs.lip6.fr>.
- [10] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4).- *Journal of Pure and Applied Algebra*, 139(1–3):61–88, 1999.
- [11] 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.
- [12] 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.
- [13] 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.
- [14] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. When polynomial equation systems can be solved fast? In *Proceedings of AAEECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

- [15] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.
- [16] D. Grigoriev and N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. *Journal of Symbolic Computation*, 5:37–64, 1988.
- [17] Z. Jelonek. Topological characterization of finite mappings. *Bull. Polish Acad. Sci. Math.*, 49(3):279–283, 2001.
- [18] D. Lazard and F. Rouillier. Solving parametric polynomial systems. Technical report, INRIA, 2004.
- [19] G. Lecerf. **Kronecker** magma package for solving polynomial systems. available at <http://www.math.uvsq.fr/lecerf/software/>.
- [20] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *Journal of Complexity*, 19(4):564–596, 2003.
- [21] F. Rouillier. RS, RealSolving. available at <http://fgbrs.lip6.fr>.
- [22] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *AAECC Journal*, 9(5):433–461, 1999.
- [23] 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.
- [24] F. Rouillier and P. Zimmermann. Efficient isolation of polynomial real roots. *Journal of Computational and Applied Mathematics*, 162(1):33–50, 2003.
- [25] M. Safey El Din. RAGLib (Real Algebraic Geometry Library). available at <http://www-calfor.lip6.fr/~safey/RAGLib>, 2003.
- [26] 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.
- [27] 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.

- [28] M. Safey El Din and P. Trébuchet. Strong bi-homogeneous Bézout theorem and its use in effective real algebraic geometry. *in preparation*, 2005.