Testing Sign Conditions on a Multivariate Polynomial and Applications

Mohab Safey El Din.

Abstract. Let f be a polynomial in $\mathbb{Q}[X_1, \dots, X_n]$ of degree D. We focus on testing the emptiness and computing at least one point in each connected component of the semi-algebraic set defined by $f > 0$ (or $f < 0$ or $f \neq 0$). To this end, the problem is reduced to computing at least one point in each connected component of a hypersurface defined by $f - e = 0$ for $e \in \mathbb{Q}$ *positive and small enough*. We provide an algorithm allowing us to determine a positive rational number e which is small enough in this sense. This is based on the efficient computation of the set of *generalized critical values* of the mapping $f : y \in \mathbb{C}^n \to f(y) \in \mathbb{C}$ which is the union of the classical set of critical values of the mapping f and the set of *asymptotic critical values* of the mapping f. Then, we show how to use the computation of generalized critical values in order to obtain an efficient algorithm deciding the emptiness of a semi-algebraic set defined by a single inequality or a single inequation. At last, we show how to apply our contribution to determining if a hypersurface contains real regular points. We provide complexity estimates for probabilistic versions of the latter algorithms which are within $\mathcal{O}(n^7 D^{4n})$ arithmetic operations in $\mathbb{Q}$. The paper ends with practical experiments showing the efficiency of our approach on real-life applications.

Mathematics Subject Classification (2000). Primary 14Q20; Secondary 14P10.

Keywords. Polynomial Systems, Real Solutions, Inequalities, Optimization, Complexity.

1. Introduction

Let f be a polynomial in $\mathbb{Q}[X_1, \dots, X_n]$ of degree D and $\mathcal{S}_+ \subset \mathbb{R}^n$ (resp. $\mathcal{S}_-$ and $\mathcal{S}$) be the semi-algebraic set defined by $f > 0$ (resp. $f < 0$ and $f \neq 0$). The aim of this paper is to provide an efficient algorithm *in practice* which computes at least one point in each connected component of $\mathcal{S}_+$ (resp. $\mathcal{S}_-$ and $\mathcal{S}$).

This question is of first importance since solving parametric polynomial systems of equations and inequalities is reduced to compute at least one point in each connected component of the complementary of a real hypersurface (see [30]). This question also appears as a black box used in algorithms solving quantifier elimination problems (see [7]).

Algorithms computing a Cylindrical Algebraic Decomposition (see [11]) allow us to produce one point in each connected component of $\mathcal{S}_+$, $\mathcal{S}_-$ or $\mathcal{S}$. Nevertheless the complexity of such algorithms is doubly exponential in the number of variables and their implementations are limited to problems having 3 or 4 variables.

Algorithms based on the critical point method are provided in [5, 6], [23], [24, 25], and [36]. The classical strategy is based on introducing an infinitesimal deformation. Suppose first that there exists $x \in \mathbb{R}^n$ such that $f(x) = 0$. Then, if $\mathcal{S}_+$ is not empty, by the mean value theorem, there exists $e \in]0, +\infty[$ *small enough* such that each connected component of $\mathcal{S}_+$ contains a connected component of the real counterpart of the hypersurface defined by $f - e = 0$. If $\mathcal{S}_+$ is empty, for all $e \in]0, +\infty[$, the real counterpart of the hypersurface defined by $f - e = 0$ is empty. Suppose now that for all $x \in \mathbb{R}^n$, $f(x) \neq 0$. Then, f has a constant sign on $\mathbb{R}^n$ and evaluating the sign of f at any point of $\mathbb{R}^n$ is sufficient to determine if $\mathcal{S}_+$ is empty or not. Finally, providing at least one point in each connected component of the semi-algebraic set defined by $f > 0$ consists in picking up a point x in $\mathbb{R}^n$ at which $f(x) \neq 0$ and returning:

- at least one point in each connected component of the real counterpart of a hypersurface defined by $f - e = 0$ for $e \in]0, +\infty[$ small enough.
- and x if and only if $f(x) > 0$.

Rephrasing the above shape of resolution in terms of infinitesimals leads to study the real counterpart hypersurface of the hypersurface defined by $f - \varepsilon = 0$ where ε is an infinitesimal.

Computing at least one point in each connected component of a real hypersurface. Consider a hypersurface $\mathcal{H} \subset \mathbb{C}^n$. We focus now on the state of the art on algorithms computing at least one point in each connected component (i.e. sampling points) of $\mathcal{H} \cap \mathbb{R}^n$. This problem is tackled by the critical point method. Its principle is the following: choose a polynomial mapping $\phi : \mathcal{H} \cap \mathbb{R}^n \to \mathbb{R}$ reaching its extrema in each connected component of $\mathcal{H} \cap \mathbb{R}^n$ and such that its critical locus is zero-dimensional or empty. When $\mathcal{H}$ is smooth, ϕ can be the square of the euclidean distance to a generically chosen point of $\mathbb{Q}^n$. When, additionally, $\mathcal{H} \cap \mathbb{R}^n$ is known to be compact, ϕ can be the projection on a line.

In [5], computing sampling points in $\mathcal{H} \cap \mathbb{R}^n$ is reduced to computing sampling points of a smooth hypersurface whose real counterpart is compact by introducing several infinitesimals. Thus, projection functions are used. The algorithms are deterministic and their complexity is $(2D)^{\mathcal{O}(n)}$ arithmetic operations in $\mathbb{Q}$. Algebraic manipulations are performed to avoid a computation of Gröbner bases and lead to encode critical points as solutions of a zero-dimensional polynomial system

generating an ideal having *always* a degree $2D(2D-1)^n$. Moreover, all the computations are performed over either a field of rational fractions (the infinitesimals being manipulated here as parameters) or over an arithmetic of truncated series allowing to increase the precision if required. Thus, there is no hope to obtain an efficient practical behaviour of these algorithms.
In [1], [3, 4], and [39], the authors use the square of the euclidean distance to a generically chosen point A in $\mathbb{Q}^n$. Algorithms dealing with the case where $\mathcal{H}$ is not smooth are provided in [1, 39]. The one of [39] uses infinitesimal deformations. The one of [1] processes by performing a recursive study of the singular locus until it has dimension 0 or is empty. Because of the choice of A, the deterministic complexity of the algorithm of [39] is $D^{\mathcal{O}(n^2)}$. Nevertheless, in practice, the first choice is suitable to obtain zero-dimensional critical loci, so that under this assumption, *which is satisfied in practice*, the complexity of [39] is $D^{\mathcal{O}(n)}$. The complexity of [1] is not well-controlled even if in singular situations it behaves better than the ones based on infinitesimal deformations. The algorithms of [3, 4] use the geometric resolution algorithm which is probabilistic. Their complexity is polynomial in n, the evaluation complexity of the input polynomial and an intrinsic geometric degree δ which is dominated by D^n.
In the smooth case, these contributions are improved in [43]: generic projection functions are used even in non-compact situations instead of distance functions to a generic point. The genericity of the choice of projection functions is necessary to ensure properness properties. As in the case of algorithms using distance functions, in practice, the first choices are suitable. Using elimination algorithms based on the geometric resolution, this leads to a probabilistic algorithm whose arithmetic complexity is polynomial in n, the evaluation complexity of the input polynomial, and an intrinsic geometric degree δ which is dominated by $D(D-1)^{n-1}$. One can also use Gröbner bases. Making the assumptions that the first choice of projections is suitable, the complexity becomes $D^{\mathcal{O}(n)}$. This work is generalized to the case of singular hypersurfaces in [45]. The algorithms relying on [43] are the most efficient in practice and are implemented in [42].
The output of all these algorithms are critical points encoded by a rational parameterization:

$$\left\{\begin{array}{ccc} X_n & = & \frac{q_n(T)}{q_0(T)} \\ & \vdots & \\ X_1 & = & \frac{q_1(T)}{q_0(T)} \\ q(T) & = & 0 \end{array}\right.$$

where T is a new variable, and $q, q_0, q_1, \ldots, q_n$ are univariate polynomials in $\mathbb{Q}[t]$. Such a rational parametrization can be obtained either by linear algebra computations in a quotient-algebra (see [38]) or directly by the geometric resolution algorithm (see [19, 20], [21], [22], and [34]).

As recalled above, the classical strategy to compute at least one point in each connected component implies to apply the aforementioned algorithms in the case of a hypersurface defined by a polynomial with coefficients in $\mathbb{Q}(\varepsilon)$. Thus, the output is a rational parameterization with coefficients in $\mathbb{Q}(\varepsilon)$. Once it is obtained, a small enough specialization for ε is obtained by computing the discriminant of q with respect to T and choosing a specialization less than the smallest absolute value of the union of the real roots of this discriminant and the leading coefficient of q. Thus, the final output is smaller than the rational parameterization with coefficients in $\mathbb{Q}(\varepsilon)$. Moreover, computing rational parameterizations with coefficients in $\mathbb{Q}(\varepsilon)$ is hard in practice: infinitesimal arithmetics spoil the practical behaviour of elimination algorithms due to problems appearing in memory management and the over-cost of arithmetic operations (see [40]).

Substituting infinitesimal deformations by a pre-computation of generalized critical values. Remark that in order to obtain one point in each connected component in $\mathcal{S}_+$ (resp. $\mathcal{S}_-$ or $\mathcal{S}$), it is sufficient to substitute *a priori* the infinitesimal ε appearing in $f-\varepsilon$ by a small enough positive rational number $e \in \mathbb{Q}$. The problem is to ensure that the chosen rational number is small enough which means here that for each connected component S of $\mathcal{S}_+$, there exists a connected component of the real counter part of the hypersurface defined by $f-e=0$ which is contained in S. This can be done by determining $e_0 \in \mathbb{R}$ such that for all $e \in]0, e_0[$, there exists a diffeomorphism φ such that the following diagram commutes:

$$\begin{tikzcd}
f^{-1}(e)\times]0,e_0[\arrow[r, "\varphi"] \arrow[dr, "\pi"'] & f^{-1}(]0,e_0[) \arrow[d, "f"] \\
&]0,e_0[
\end{tikzcd}$$

where π is the canonical projection on the second member of the cartesian product $f^{-1}(e)\times]0,e_0[$.
Such a topological property is obtained by ensuring that the interval $I =]0, e_0[$ has an empty intersection with the set of *generalized critical values* of the polynomial mapping $\widetilde{f} : x \in \mathbb{R}^n \to f(x) \in \mathbb{R}$ (see [35, Theorem 3.1]). This set of generalized critical values is denoted by $K(f)$ in the sequel. This set is defined and studied in [35]. A real number $c \in \mathbb{R}$ is a generalized critical value of a mapping $\widetilde{f}$ if and only if it is either a critical value of $\widetilde{f}$ or there exists a sequence of points $(z_\ell)_{\ell\in\mathbb{N}}$ such that $f(z_\ell)$ tends to c when ℓ tends to ∞, $||z_\ell||$ tends to ∞ when ℓ tends to ∞ and $||z_\ell||.||d_{z_\ell} f||$ tends to 0 when ℓ tends to ∞. In the latter case, c is said to be an *asymptotic critical value*. Degree bounds are provided in [28]. An algorithm computing them is described in [35]. This algorithm works as follows: denoting by I the ideal

$$I = \langle f - T, \left(\frac{\partial f}{\partial X_i} - a_i\right)_{i\in\{1,\ldots,n\}}, \left(X_i\frac{\partial f}{\partial X_j} - a_{i,j}\right)_{(i,j)\in\{1,\ldots,n\}^2}\rangle$$

where $a_1, \ldots, a_{1,1}, \ldots, a_{n,n}$ and T are new variables, compute

$$J = I \cap \mathbb{Q}[T, a_1, \ldots, a_n, a_{1,1}, \ldots, a_{n,n}].$$

Generalized critical values are solutions of

$$J + \langle a_1, \ldots, a_n, a_{11}, a_{n,n} \rangle.$$

Thus, this algorithm requires to perform algebraic elimination of variables on the ideal I defined with polynomials involving $n^2 + 2n + 1$ variables. Moreover, the degree of I can equal D^n (where D is the degree of f). Practical experiments done at the end of paper show that its practical behaviour is inefficient.
We provide here an algorithm computing efficiently the set of generalized critical values of a polynomial mapping from $\mathbb{R}^n$ to $\mathbb{R}$. A probabilistic version of this algorithm has a complexity within $D^{\mathcal{O}(n)}$ arithmetic operations in $\mathbb{Q}$ which is polynomial in the size of the output in worst-cases.
This allows us to substitute the use of infinitesimal deformations by a pre-computation of generalized critical values in order to compute at least one point in each connected component of a semi-algebraic set defined by a single inequality. The algorithm we obtain is efficient in practice and its probabilistic versions have a complexity within $\mathcal{O}(n^7 D^{4n})$ arithmetic operations in $\mathbb{Q}$. We also show how to apply our contribution to the problem of deciding if a hypersurface contains real regular points. Our algorithmic contributions have been implemented in the RAGlib Maple package [42] and we describe at the end of the paper how they have been applied on concrete applications which are unreachable with anterior methods.

Plan of the paper. The paper is organized as follows. In Section 2, we recall the definition and basic properties of *generalized critical values* which can be found in [35]. In Section 3, we provide geometric results which, up to a generic linear change of the variables $X_1, \ldots, X_n$, characterize *generalized critical values* as the set of non-properness of a projection on a line restricted to a 1-dimensional polar variety. In Section 4, we show how to obtain a algorithm computing generalized critical values which is directly based on the geometric results of Section 3. In Section 5, we describe an algorithm computing at least one point in each connected component of a semi-algebraic set defined by a single inequality, which is based on the computation of *generalized critical values*. In Section 6, we show how to apply our contributions to determining if a hypersurface contains real regular points. Finally, Section 7 contains some benchmarks illustrating the practical efficiency of our algorithms and showing these methods are already promising to deal with problems having more than 4 variables.

Acknowledgments. The author thanks E. Schost for fruitful discussions and comments about this work.

2. Definition and first properties of generalized critical values

In this section, we recall the definitions and basic properties of generalized critical values which can be found in [35].

Definition 2.1. A complex number $c \in \mathbb{C}$ is a critical value of the mapping $f : y \in \mathbb{C}^n \to f(y)$ if and only if there exists $z \in \mathbb{C}^n$ such that $f(z) = c$ and $\frac{\partial f}{\partial X_1}(z) = \cdots = \frac{\partial f}{\partial X_n}(z) = 0$.
A complex number $c \in \mathbb{C}$ is an asymptotic critical value of the mapping $f : y \in \mathbb{C}^n \to f(y)$ if and only if there exists a sequence of points $(z_\ell)_{\ell \in \mathbb{N}} \subset \mathbb{C}^n$ such that:

- $f(z_\ell)$ tends to c when ℓ tends to ∞.
- $||z_\ell||$ tends to $+\infty$ when ℓ tends to ∞.
- for all $(i, j) \in \{1, \dots, n\}$ $||X_i(z_\ell)||.||\frac{\partial f}{\partial X_j}(z_\ell)||$ tends to 0 when ℓ tends to ∞.

In the sequel, we denote by $K_0(f)$ the set of critical values of f, by $K_\infty(f)$ the set of asymptotic critical values of f, and by $K(f)$ the set of generalized critical values of f (i.e. $K(f) = K_0(f) \cup K_\infty(f)$).

Remark 2.2. Remark that any statement of the following kind: *given a semi-algebraic (resp. constructible) set $\mathcal{S} \subset \mathbb{R}^n$ (resp. $\mathcal{S} \subset \mathbb{C}^n$ and a polynomial mapping $\varphi : \mathcal{S} \subset \mathbb{R}^n \to \mathbb{R}^q$ (resp. $\mathcal{S} \subset \mathbb{C}^n \to \mathbb{C}^q$) and a point $y \in \mathbb{R}^q$ (resp $\mathbb{C}^q$), there exists a sequence of points $(z_\ell)_\ell$ lying in $\mathcal{S}$ and a point $y \in \mathbb{R}^q$ (resp. $y \in \mathbb{C}^q$) such that:*

- *$||z_\ell||$ tends to ∞ when ℓ tends to ∞;*
- *$\varphi(y_\ell)$ tends to y when ℓ tends to ∞;*

implies that y belongs to the closure of the image of the semi-algebraic map φ. Note that since $||z_\ell||$ is supposed to tend to ∞, the graph of φ is not compact and, using the curve selection Lemma, the sequence of points in the above statement can be substituted by the existence of a semi-algebraic curve $\gamma :]0, 1[\to \mathbb{R}^n$ (resp. $\gamma :]0, 1[\to \mathbb{C}^n$) such that $||\gamma(t)||$ tends to ∞ when $t \to 1$ and $\varphi(\gamma(t))$ tends to y when $t \to 1$.

Example. Consider the following polynomial in $Q[X_1, X_2]$

$$f = X_1(X_1X_2 - 1)$$

and the mapping $\widetilde{f} : (x_1, x_2) \to f(x_1, x_2)$. This mapping has obviously no critical value since $\langle f - T, \frac{\partial f}{\partial X_1}, \frac{\partial f}{\partial X_2} \rangle = \mathbb{Q}[X_1, X_2, T]$. Suppose now that there exists a sequence of points z_ℓ such that:

- $||z_\ell||$ tends to $+\infty$ when ℓ tends to ∞.
- for all $(i, j) \in \{1, 2\}$ $||X_i(z_\ell)||.||\frac{\partial f}{\partial X_j}(z_\ell)||$ tends to 0 when ℓ tends to ∞.

This implies that $X_1^2(z_\ell)$ tends to 0 when ℓ tends to ∞, which implies that $X_1(z_\ell)$ tends to 0 when ℓ tends to ∞, and $X_2X_1^2(z_\ell)$ tends to 0 when ℓ tends to ∞. Finally, $f(z_\ell)$ tends to 0 when ℓ tends to ∞. Thus, 0 is an asymptotic critical value of the mapping $\widetilde{f}$. We will see further that it is the only one.

Consider now the following example in 3 variables:

$$f = X_1 + X_1^2X_2 + X_1^4X_2X_3$$

In [35], the authors prove that the set of generalized critical values of the mapping sending $x \in \mathbb{C}^n$ to $f(x)$ is $\{0\}$ by using a similar reasoning as the above.

In [35], the authors prove the following result which can be seen as a generalized Sard's theorem for generalized critical values.

Theorem 2.3. *Let f be a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree D. The set of generalized critical values $K(f)$ of the mapping $\widetilde{f} : x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$ is Zariski-closed in $\mathbb{C}$.*
Moreover, $D\sharp K_\infty(f) + \sharp K_0(f) \leq D^n - 1$

Given $f \in \mathbb{Q}[X_1, \ldots, X_n]$, consider a mapping $f_\mathbb{C} : x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$ and an open subset $F_\mathbb{C}$ of $\mathbb{C}$. We say that $f_\mathbb{C}$ realizes a locally trivial fibration on $\mathbb{C}^n \setminus f_\mathbb{C}^{-1}(F_\mathbb{C})$ if for all connected open set (for the euclidean topology) $U_\mathbb{C} \subset \mathbb{C} \setminus F_\mathbb{C}$, for all $e \in U_\mathbb{C}$ denoting by $\pi_\mathbb{C}$ the projection on the second member of the cartesian product $f_\mathbb{C}^{-1}(e) \times U_\mathbb{C}$, there exists a diffeomorhism φ such that the following diagram

$$\begin{tikzcd} f_\mathbb{C}^{-1}(e) \times U_\mathbb{C} \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & f_\mathbb{C}^{-1}(U_\mathbb{C}) \arrow[d, "f"] \\ & U_\mathbb{C} \end{tikzcd}$$

is commutative.
The above definition is also used for polynomial mappings from $\mathbb{R}^n$ to $\mathbb{R}$. Consider a mapping $f_\mathbb{R} : \mathbb{R}^n \to \mathbb{R}$ and an open subset $F_\mathbb{R}$ of $\mathbb{R}$. We say that $f_\mathbb{R}$ realizes a locally trivial fibration on $\mathbb{R}^n \setminus f_\mathbb{R}^{-1}(F_\mathbb{R})$ if for all connected open set (for the euclidean topology) $U_\mathbb{R} \subset \mathbb{C} \setminus F_\mathbb{R}$, for all $e \in U_\mathbb{R}$ denoting by $\pi_\mathbb{R}$ the projection on the second member of the cartesian product $f_\mathbb{R}^{-1}(e) \times U_\mathbb{R}$, there exists a diffeomorphism φ such that the following diagram

$$\begin{tikzcd} f_\mathbb{R}^{-1}(e) \times U_\mathbb{R} \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & f_\mathbb{R}^{-1}(U_\mathbb{R}) \arrow[d, "f"] \\ & U_\mathbb{R} \end{tikzcd}$$

is commutative.
The main interest of the set of *generalized critical values* relies on its topological properties which are summarized below and proved in [35].

Theorem 2.4. *The mapping $f_\mathbb{C}$ realizes a locally trivial fibration in $\mathbb{C}^n \setminus f_\mathbb{C}^{-1}(K(f_\mathbb{C}))$. The mapping $f_\mathbb{R}$ realizes a locally trivial fibration in $\mathbb{R}^n \setminus f_\mathbb{R}^{-1}(K(f_\mathbb{R}))$.*

Example. Consider the examples given above. We have proved that for both examples 0 is an asymptotic critical value. Remark that the fiber of both considered mappings above 0 is reducible while a generic fiber is irreducible. This is characteristic to a change of topology and is easily visualized on Figure 1 illustrating the example $f = X_1(X_1X_2 - 1)$.

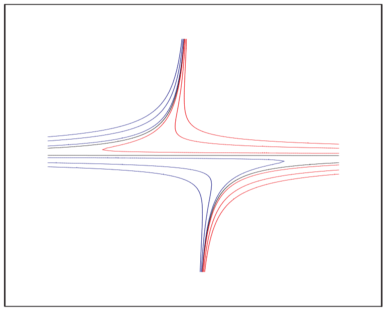

FIGURE 1. Existence of generalized critical values and change in topology

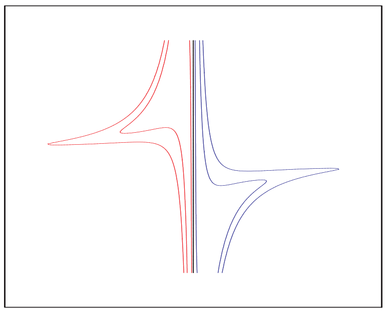

FIGURE 2. Existence of generalized critical values and no change in topology

Nevertheless, note that a mapping can realize a locally trivial fibration even if there exists a generalized critical value in I. To illustrate this fact, consider the following example:

$$f = -X_2(2X_1^2X_2^2 - 9X_1X_2 + 12)$$

which realizes a locally trivial fibration around 0 as shown in Figure 2 but is such that $K(f) = \{0\}$.

Thus, $K(f)$ is Zariski-closed, degree bounds on $K(f)$ are Bézout-like degree bounds and its topological properties ensure that there is no topological change in the fibers of f taken above any interval of $\mathbb{R}$ which has an empty intersection with $K(f)$.

Denote by $GL_n(\mathbb{C})$ the set of n-square invertible matrices with coefficients in $\mathbb{C}$. Consider now $\mathbf{A} \in GL_n(\mathbb{C})$ and denote by $f^{\mathbf{A}}$ the polynomial $f(\mathbf{AX})$ where $\mathbf{X}$ denotes $(X_1, \ldots, X_n)$. Moreover, given $\{f_1, \ldots, f_s\}$ in $\mathbb{Q}[X_1, \ldots, X_n]$ and an algebraic variety $\mathcal{V} \subset \mathbb{C}^n$ defined by $f_1 = \cdots = f_s = 0$, we denote by $\mathcal{V}^{\mathbf{A}}$ the algebraic variety defined by $f_1^{\mathbf{A}} = \cdots = f_s^{\mathbf{A}} = 0$.

The following lemma is an immediate consequence of Definition 2.1 and will be used in the sequel.

Lemma 2.5. *For all $\mathbf{A} \in GL_n(\mathbb{Q})$, $K(f)$ equals $K(f^{\mathbf{A}})$, $K_0(f)$ equals $K_0(f^{\mathbf{A}})$ and $K_\infty(f)$ equals $K_\infty(f^{\mathbf{A}})$.*
If c is a critical value (resp. an asymptotic critical value) of f, then for all $e \in \mathbb{Q}$, $c + e$ is a critical value (resp. an asymptotic critical value) of $f + e$.

Using Remark 2.2, the following lemma is also immediate and is used further.

Lemma 2.6. *Let f be a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$. Consider $c \in \mathbb{C}$ and $(z_\ell)_{\ell\in\mathbb{N}} \subset \mathbb{C}^n$ be a sequence of points such that:*

- *$f(z_\ell)$ tends to c when ℓ tends to ∞;*
- *$||z_\ell||$ tends to ∞ when ℓ tends to ∞;*
- *$||z_\ell||.||d_{z_\ell} f||$ tends to 0 when ℓ tends to ∞.*

Denote by $\mathbf{X}$ the vector $X_1, \ldots, X_n$. There exists a Zariski-closed subset $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, $||\mathbf{A}\mathbf{X}(z_\ell)||$ tends to ∞ when ℓ tends to ∞.

In the sequel, for the sake of simplicity, we identify a polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ with the mapping $f_{\mathbb{C}} : x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$.

3. Geometric results

Let f be a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$, $\mathcal{H} \subset \mathbb{C}^{n+1}$ be the hypersurface defined by $f - T = 0$ (where T is a new variable). Given $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$, we denote by $F_i : \mathbb{C}^n \to \mathbb{C}^{n+1}$ the polynomial mapping sending x to:

$$((\partial f/\partial X_i)(x), (X_1 \partial f/\partial X_i)(x), \ldots, (X_n \partial f/\partial X_i)(x))$$

and by $\widetilde{F}_i : \mathbb{C}^n \to \mathbb{C}^{in+i+1}$ the polynomial mapping sending x to:

$$(F_1(x), F_2(x), \ldots, F_i(x), f(x)).$$

We consider in the sequel the polynomial mapping $\phi : \mathbb{C}^n \to \mathbb{C}^{n^2+n+1}$ sending $x = (x_1, \ldots, x_n)$ to

$$(F_1(x), \ldots, F_n(x), f(x))$$

which coincides with $\widetilde{F}_n$. For any polynomial mapping ψ, we denote by Γ_ψ the image of ψ and by $\overline{\Gamma}_\psi$ its Zariski-closure. For $(i, j) \in \{1, \ldots, n\}^2$, we introduce new variables a_i, and $a_{i,j}$ such that $\overline{\Gamma}_\phi$ is defined by a set of generators of the ideal:

$$\langle f - T, (\partial f/\partial X_i - a_i)_{i\in\{1,\ldots,n\}}, (X_i.\partial f/\partial X_j - a_{i,j})_{(i,j)\in\{1,\ldots,n\}^2}\rangle$$

intersected with the polynomial ring $\mathbb{Q}[T, a_1, \ldots, a_n, a_{1,1}, \ldots, a_{n,n}]$.
Let $L_i \subset \mathbb{C}^{in+i+1}$ be the coordinate axis of T, i.e. the line defined by:

$$a_1 = \cdots = a_i = a_{1,1} = \cdots = a_{n,1} = \cdots = a_{1,i} = \cdots = a_{n,i} = 0.$$

The line L_n is denoted by L in the sequel.

Kurdyka and its collaborators prove that $\overline{\Gamma}_\phi \cap L$ equals the set of generalized critical values of f (see [28, 35]). The set of *asymptotic critical values* of f, denoted by $K_\infty(f)$, is characterized as the intersection of the set of non-properness of ϕ with L.
The main result of this section is the following one:
There exists a Zariski-closed subset $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ the set $K_\infty(f)$ of asymptotic critical values of f is contained in the set of non-properness of the projection $\pi_T : (x_1, \dots, x_n, t) \in \mathbb{C}^{n+1} \to t \in \mathbb{C}$ restricted to the Zariski-closure of the constructible set defined by:

$$f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0.$$

To prove this, in the sequel, for $i = n, \dots, 2$, we consider projections:

$$\begin{array}{cccc} \Pi_i : & \mathbb{C}^{n+1} & \to & \mathbb{C}^i \\ & (x_1, \dots, x_n, t) & \mapsto & (x_{n-i+2}, \dots, x_n, t) \end{array}$$

and the algebraic varieties $W^{\mathbf{A}}_{n-i} \subset \mathbb{C}^{n+1}$ denotes the Zariski-closure of the constructible set defined by:

$$f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_i} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_{i+1}} \neq 0.$$

For simplicity, $W^{\mathbf{A}}_n$ denotes $\mathcal{H}^{\mathbf{A}}$.
In the sequel, we consider maps between complex or real algebraic varieties. The notion of properness of such maps will be relative to the topologies induced by the metric topologies of $\mathbb{C}$ or $\mathbb{R}$. A map $\phi : V \to W$ of topological spaces is said to be proper at $w \in W$ if there exists a neighborhood B of w such that $f^{-1}(\overline{B})$ is compact (where $\overline{B}$ denotes the closure of B). The map ϕ is said to be proper if it is proper at all $w \in W$.

Given $\mathbf{A} \in GL_n(\mathbb{Q})$ and $j \in \{2, \dots, n\}$, we say that the property $\mathcal{P}_j(\mathbf{A})$ is satisfied if and only if for all $i \in \{j, \dots, n\}$, the mapping Π_i restricted to $W^{\mathbf{A}}_i$ is proper. By convention, we set $\mathcal{P}_{n+1}(\mathbf{A})$ to be always true for all $\mathbf{A} \in GL_n(\mathbb{Q})$.

Remark 3.1. Remark that from the algebraic Bertini-Sard theorem [49], if $\mathcal{P}_i(\mathbf{A})$ is true, Π_i restricted to W_i is a finite map and then $W^{\mathbf{A}}_i$ has dimension i.

We first show below that if $\mathcal{P}_2(\mathbf{A})$ is satisfied, then the result stated above is true (see Proposition 3.2 below). Then, we prove that there exists a Zariski-closed subset $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, $\mathcal{P}_2(\mathbf{A})$ holds.

3.1. Geometric characterization of generalized critical values under properness assumptions

In the sequel, we do the following hypothesis:
Assumption (H): there exists a Zariski-closed subset $\mathcal{A} \subsetneq GL_n(\mathbb{Q})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ and $j \in \{2, \dots, n+1\}$, the property $\mathcal{P}_j(\mathbf{A})$ is satisfied.

We prove in the sequel (see Proposition 3.2) that if $\mathcal{P}_2(\mathbf{A})$ is satisfied, given $c \in K_\infty(f)$, there exists a sequence of points $(z_\ell)_{\ell\in\mathbb{N}}$ in $W_1^{\mathbf{A}}$ such that:

- $f^{\mathbf{A}}(z_\ell)$ tends to c when ℓ tends to ∞
- $||z_\ell||$ tends to ∞ when ℓ tends to ∞
- $||z_\ell||.||d_{z_\ell} f^{\mathbf{A}}||$ tends to 0 when ℓ tends to ∞

so that the existence of asymptotic critical values can be read off in $W_1^{\mathbf{A}}$ which has dimension 1.

Proposition 3.2. *Consider $c \in K_\infty(f)$. There exists a a Zariski-closed subset $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ such that for all $A \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, there exists a sequence of points $(z_\ell)_{\ell\in\mathbb{N}}$ such that:*

- *for all $\ell \in \mathbb{N}$, $z_\ell \in W_1^{\mathbf{A}}$;*
- *$f^{\mathbf{A}}(z_\ell) \to c$ when $\ell \to \infty$;*
- *$||z_\ell||$ tends to ∞ when ℓ tends to ∞;*
- *$||z_\ell||.||d_{z_\ell} f^{\mathbf{A}}|| \to 0$ when $\ell \to \infty$.*

Proof. Given an integer j in $\{n+1, \ldots, 2\}$ and $\mathbf{A} \in GL_n(\mathbb{Q})$, we say that property $\mathfrak{P}_j(\mathbf{A})$ is satisfied if and only if the following assertion is true: *let $c \in K_\infty(f^{\mathbf{A}})$, if the property $\mathcal{P}_j(\mathbf{A})$ is satisfied, then there exists a sequence of points $(z_\ell)_{\ell\in\mathbb{N}}$ such that:*

- *for all $\ell \in \mathbb{N}$, $z_\ell \in W_{j-1}^{\mathbf{A}}$;*
- *$f^{\mathbf{A}}(z_\ell) \to c$ when $\ell \to \infty$;*
- *$||z_\ell||$ tends to ∞ when ℓ tends to ∞;*
- *$||z_\ell||.||d_{z_\ell} f^{\mathbf{A}}|| \to 0$ when $\ell \to \infty$.*

Suppose now $\mathfrak{P}_{j+1}(\mathbf{A})$ is true and $\mathcal{P}_j(\mathbf{A})$ is satisfied. We show below that this implies $\mathfrak{P}_j(\mathbf{A})$.

Since $\mathfrak{P}_{j+1}(\mathbf{A})$ is supposed to be true and $\mathcal{P}_{j+1}(\mathbf{A})$ holds, then there exists a sequence of points $(z_\ell)_{\ell\in\mathbb{N}}$ such that:

- for all $\ell \in \mathbb{N}$, $z_\ell \in W_j^{\mathbf{A}}$;
- $f^{\mathbf{A}}(z_\ell) \to c$ when $\ell \to \infty$;
- $||z_\ell||$ tends to ∞ when ℓ tends to ∞;
- $||z_\ell||.||d_{z_\ell} f^{\mathbf{A}}|| \to 0$ when $\ell \to \infty$.

We prove below that one can choose such a sequence $(z_\ell)_{\ell\in\mathbb{N}}$ in $W_{j-1}^{\mathbf{A}}$.
Consider the mapping $\phi^{\mathbf{A}} : W_j^{\mathbf{A}} \subset \mathbb{C}^{n+1} \to \mathbb{C}^{2j+1}$ which associates to a point $x = (x_1, \ldots, x_n, t) \in W_j^{\mathbf{A}}$ the point:

$$\left(x_{n-j+2}, \ldots, x_n, t, \frac{\partial f}{\partial X_{n-j+1}}(x), \left(x_{n-j+r} \frac{\partial f}{\partial X_{n-j+1}}(x) \right)_{r=1,\ldots,j} \right)$$

Denote by

$$(a_{n-j+2}, \ldots, a_n, a_{n+1}, a_{0,n-j+1}, a_{n-j+1,n-j+1}, \ldots, a_{n,n-j+1})$$

the coordinates of the target space of $\phi^{\mathbf{A}}$.

Note that since $\mathcal{P}_j(\mathbf{A})$ holds, the restriction of Π_j to $W_j^{\mathbf{A}}$ has finite fibers. Then, there exists a Zariski-closed subset $\mathcal{Z} \subsetneq \mathbb{C}^{2j+1}$ such that specializing the coordinates $(a_{n-j+2}, \dots, a_n, a_{0,n-j+1}, a_{n-j+1,n-j+1})$ of the target space of $\phi^{\mathbf{A}}$ to a point

$$\alpha_{n-j+2}, \dots, \alpha_n, \alpha_{0,n-j+1}, \alpha_{n-j+1,n-j+1}$$

outside $\mathcal{Z}$ defines a finite set of points in the image of $\phi^{\mathbf{A}}$. Indeed, these points are the images of the points in $W_j^{\mathbf{A}}$ such that their X_i coordinate (for $i = n-j+2, \dots, n$) equals α_i and $X_{n-j+1}\frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}}$ equals $\alpha_{n-j+1,n-j+1}$.

Given a point $\underline{\alpha} = (\alpha_{n-j+2}, \dots, \alpha_n) \in \mathbb{C}^{j-1}$ and a couple of complex numbers $\theta = (\eta_1) \in \mathbb{C}$, such that $(\alpha_{n-j+2}, \dots, \alpha_n, \eta_1) \notin \mathcal{Z}$, we denote by $y(\underline{\alpha}, \beta)$ a point in the image of $\phi^{\mathbf{A}}$ obtained by specializing the first $(n-j-1)$ coordinates (corresponding to $x_{n-j+2}, \dots, x_n$) to $\underline{\alpha}$ and the $j+2$-th coordinate (corresponding to $x_{n-j+1}\frac{\partial f}{\partial X_{n-j+1}}$). We also denote by $x(\underline{\alpha}, \theta)$ a point in the pre-image of $y(\underline{\alpha}, \theta)$ by $\phi^{\mathbf{A}}$.

Consider $c \in K_\infty(f^{\mathbf{A}})$. Then, since $\mathfrak{P}_{j+1}(\mathbf{A})$ is supposed to be true, there exists a sequence of points $(z_\ell)_{\ell \in \mathbb{N}} \subset \mathbb{C}^n$ in the Zariski-closure of the constructible set defined by:

$$\frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-j}} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}} \neq 0$$

such that:

- $f^{\mathbf{A}}(z_\ell)$ tends to c when ℓ tends to ∞
- $||z_\ell||$ tends to ∞ when ℓ tends to ∞.
- $||z_\ell||.||d_{z_\ell} f^{\mathbf{A}}||$ tends to 0 when ℓ tends to ∞.

Consider the images by ϕ of the points $(z_\ell, f^{\mathbf{A}}(z_\ell))$ and their first $j-1$ coordinates $\underline{\alpha_\ell}$ and θ_ℓ of their $j+2$-th coordinate.

Remark that without loss of generality, we can do the assumption (H'): for all $(i,j) \in \mathbb{N} \times \mathbb{N}$, $x(\underline{\alpha}_i, \theta_\ell)$ is not a root of $\frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+2}}$ and $(\underline{\alpha}_i, \theta_\ell) \notin \mathcal{Z}$.

If for all $\ell \in \mathbb{N}$, $\frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}}(z_\ell) = 0$ the result is obtained. Else, one can suppose that for all $\ell \in \mathbb{N}$, $\frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}}(z_\ell) \neq 0$.

Note θ_ℓ tends to 0 when ℓ tends to ∞ and that the last $j+1$ coordinates of $y(\underline{\alpha}_{i_0}, \theta_\ell)$ tend to zero when i_0 is fixed and ℓ tends to ∞.

Remark that $X_{n-j+1}(x(\underline{\alpha}, \theta))$ is a root of a univariate polynomial with coefficients depending on $\underline{\alpha}$ and θ. Then, for a fixed integer i_0, since θ_ℓ tends to (0) when ℓ tends to ∞, $X_{n-j+1}(x(\underline{\alpha}_{i_0}, \theta_\ell))$ has either a finite limit or tends to ∞ when ℓ tends to ∞.

In the sequel, we prove that for $i_0 \in \mathbb{N}$, $y(\underline{\alpha}_{i_0}, \theta_\ell)$ has a finite limit in $\mathbb{C}^{2n+1}$ when ℓ tends to ∞.

Suppose first that $X_{n-j+1}(x(\underline{\alpha}_{i_0}, \theta_\ell))$ has a finite limit when ℓ tends to ∞. Then, $f^{\mathbf{A}}(x(\underline{\alpha}_{i_0}, \theta_\ell))$ remains bounded (since $X_{n-j+1}(x(\underline{\alpha}_{i_0}, \theta_\ell))$ has a finite limit and since $\frac{\partial f^{\mathbf{A}}}{\partial X_1}, \dots, \frac{\partial f^{\mathbf{A}}}{\partial X_{n-j}}$ vanish at $x(\underline{\alpha}_{i_0}, \theta_\ell))$. Thus, it has consequently a finite limit.

Moreover, without loss of generality, one can suppose that $X_{n-j+1}(x(\underline{\alpha}_{i_0}, \theta_\ell))$ does not tend to 0 which implies that $\frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}}(x(\underline{\alpha}_{i_0}, \theta_\ell))$ tends to 0 when ℓ tends to ∞.

Suppose now that $X_{n-j+1}(x(\underline{\alpha}_{i_0}, \theta_\ell))$ tends to ∞ when ℓ tends to ∞. This immediately implies that $\frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}}(x(\underline{\alpha}_{i_0}, \theta_\ell))$ tends to 0 when ℓ tends to ∞.
Since $X_{n-j+1}(x(\underline{\alpha}_{i_0}, \theta_\ell))$ tends to ∞ when ℓ tends to ∞, and

$$\left(X_k \frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}} \right) (x(\underline{\alpha}_{i_0}, \theta_\ell))$$

tends to 0 when ℓ (for $k \in \{n-j+1, \ldots, n\}$) tends to ∞, using Remark 2.2 and the curve selection Lemma at infinity (see [35, Lemma 3.3, page 9], this implies there exists a semi-algebraic arc $\gamma_{i_0} : [0, 1[\to \mathbb{R}^n$ such that:

- $\gamma_{i_0}([0, 1[)$ is included in the intersection of $W_j^{\mathbf{A}}$ and of the linear subspace defined by $X_k = X_k(\underline{\alpha}_{i_0})$ for $k = n-j+2, \ldots, n$, which implies that
$$\sum_{p=1}^{n} \left(X_p \frac{\partial f^{\mathbf{A}}}{\partial X_p} \right) (\gamma_{i_0}(\rho)) = \left(X_{n-j+1} \frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}} \right) (\gamma_{i_0}(\rho))$$
- and
$$||\gamma_{i_0}(\rho)|| \to \infty \quad \text{and} \quad ||X_{n-j+1}(\gamma_{i_0}(\rho))||.||\frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}}(\gamma_{i_0}(\rho))|| \to 0$$
when ρ tends to 1.

From Lojasiewicz's inequality at infinity [9, 2.3.11, p. 63], this implies that there exists an integer $N \geq 1$ such that:

$$\forall \rho \in [0, 1[, \quad ||\frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}}(\gamma_{i_0}(\rho)))|| \leq ||X_{n-j+1}(\gamma_{i_0}(\rho))||^{-1-\frac{1}{N}}$$

Following the same reasoning as in [35, Lemma 3.4, page 9], one can re-parameterize γ_{i_0} such that γ_{i_0} becomes a semi-algebraic function from $[0, +\infty[$ to $\mathbb{R}^n$ and $\lim_{\rho \to 1} ||\dot{\gamma}_{i_0}(\rho)|| = 1$. Thus, the following yields:

$$\forall p \in [0, +\infty[, \quad ||\frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}}(\gamma_{i_0}(\rho))||.||\dot{\gamma}_{i_0}(\rho)|| \leq ||X_{n-j+1}(\gamma_{i_0}(\rho))||^{-1-\frac{1}{N}}.||\dot{\gamma}_{i_0}(\rho)||$$

and there exists $B \in \mathbb{R}$ such that

$$\int_0^\infty ||\gamma_{i_0}(\rho)||^{-1-\frac{1}{N}}.||\dot{\gamma}_{i_0}(\rho)|| d\rho \leq B.$$

Since

$$\int_0^\infty ||\gamma_{i_0}(\rho)||^{-1-\frac{1}{N}}.||\dot{\gamma}_{i_0}(\rho)|| d\rho \geq \int_0^\infty ||X_{n-j+1}(\gamma_{i_0}(\rho))||^{-1-\frac{1}{N}}.||\dot{\gamma}_{i_0}(\rho)|| d\rho$$

and

$$\int_0^\infty ||\frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}}(\gamma_{i_0}(\rho))||.||\dot{\gamma}_{i_0}(\rho)|| d\rho \geq || \int_0^\infty \frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}}(\gamma_{i_0}(\rho)).\dot{\gamma}_{i_0}(\rho) d\rho||$$

one has finally

$$||\int_0^\infty \frac{\partial f^{\mathbf{A}}}{\partial X_{n-j+1}}(\gamma_{i_0}(\rho)).\dot{\gamma}_{i_0}(\rho)d\rho|| \leq B$$

Thus, the restriction of $f^{\mathbf{A}}$ is bounded along γ_{i_0}.
Finally, we have proved that $y(\underline{\alpha}_{i_0}, \theta_\ell)$ tends to a point whose last $j+1$ coordinates are null.

By assumption, there exists a Zariski-closed $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, $\mathcal{P}_j(\mathbf{A})$ is satisfied.
For the sake of simplicity, we omit, in the sequel, to indicate the change of variables $\mathbf{A}$ performed on f.

Let $y_{i_0} = (\underline{\alpha}_{i_0}, c_{i_0}, 0, \ldots, 0)$ be the limit of $y(\underline{\alpha}_{i_0}, \theta_\ell)$ and let $p_{i_0} \in \mathbb{C}^n$ be $(\underline{\alpha}_{i_0}, c_{i_0})$ and $p_\ell \in \mathbb{C}^n$ be the point whose coordinates are the j-first coordinates of $y(\underline{\alpha}_{i_0}, \theta_\ell)$.
We prove now that y_{i_0} belongs to the image of ϕ.
Since the restriction to W_j of Π_j is supposed to be proper, for all $\ell \in \mathbb{N}$, $\Pi_j^{-1}(p_\ell) \cap W_j \neq \emptyset$ and there exists a ball centered at p_{i_0} such that $\Pi_j^{-1}(\mathcal{B})$ is compact. Moreover, remark that $x(\underline{\alpha}_{i_0}, \theta_\ell)$ belongs to $\Pi_j^{-1}(p_\ell)$.
Thus, one can extract a converging subsequence from $(x(\underline{\alpha}_{i_0}, \theta_\ell))_{\ell \in \mathbb{N}}$ and let x_{i_0} be the limit of the chosen converging subsequence.
It remains to prove that:

- $(f(x_{i_0}))_{i_0 \in \mathbb{N}}$ tends to c when i_0 tends to ∞
- $\left(X_i \frac{\partial f}{\partial X_j}\right)(x_{i_0})$ for $(i,j) \in \{1, \ldots, n\}$ tends to 0 when i_0 tends to ∞.

This is done by continuity of the polynomials f and $X_i \frac{\partial f}{\partial X_j}$ for $i = 2, \ldots, n$, proving that:

- by definition of $x(\underline{\alpha}_{i_0}, \theta_{i_0})$, $\left(f(x(\underline{\alpha}_{i_0}, \theta_{i_0}))\right)_{i_0 \in \mathbb{N}}$ tends to c when i_0 tends to ∞,
- by definition of $x(\underline{\alpha}_{i_0}, \theta_{i_0})$, $\left(X_i \frac{\partial f}{\partial X_j}\right)(x(\underline{\alpha}_{i_0}, \theta_{i_0})$ for $(i,j) \in \{1, \ldots, n\}$ tends to 0 when i_0 tends to ∞,

To this end, we show that for all $k \in \{1, \ldots, n\}$ and for all $\varepsilon \in]0, +\infty[$ there exists $M \in \mathbb{N}$ such that for all $i_0 > M$, $||X_k(x_{i_0}) - X_k(x(\underline{\alpha}_{i_0}, \theta_{i_0}))|| \leq \varepsilon$.
Indeed, we have

$$\begin{aligned} ||X_k(x_{i_0}) - X_k(x(\underline{\alpha}_{i_0}, \theta_{i_0}))|| = \\ ||X_k(x_{i_0}) - X_k(x(\underline{\alpha}_{i_0}, \theta_\ell)) + X_k(x(\underline{\alpha}_{i_0}, \theta_\ell)) - X_k(x(\underline{\alpha}_{i_0}, \theta_{i_0}))|| \leq \\ ||X_k(x_{i_0}) - X_k(x(\underline{\alpha}_{i_0}, \theta_\ell))|| + ||X_k(x(\underline{\alpha}_{i_0}, \theta_\ell)) - X_k(x(\underline{\alpha}_{i_0}, \theta_{i_0}))|| \end{aligned}$$

Moreover, $||X_k(x_{i_0}) - X_k(x(\underline{\alpha}_{i_0}, \theta_\ell))||$ tends to 0 when ℓ tends to ∞ so that for all ε' there exists N_1 such that for all $\ell > N_1$, $||X_k(x_{i_0}) - X_k(x(\underline{\alpha}_{i_0}, \theta_\ell))|| < \varepsilon'$.

At last, remark that since $\left(x(\underline{\alpha}_{i_0},\theta_\ell)\right)_{\ell\in\mathbb{N}}$ converges to a point in $\mathbb{C}^n$, the sequence $\left(X_k(x(\underline{\alpha}_{i_0},\theta_\ell))\right)_{\ell\in\mathbb{N}}$ is a Cauchy-sequence which implies that for all ε'' there exists $N_2 \in \mathbb{N}$ such that for all $(\ell',\ell'') \in \mathbb{N}^2$ satisfying $\ell' > N_2$ and $\ell'' > N_2$, $||X_k(x(\underline{\alpha}_{i_0},\theta'_\ell)) - X_k(x(\underline{\alpha}_{i_0},\theta_{\ell''}))||$. In particular when, $i_0 > N_2$, and $\ell > N_2$, $||X_k(x(\underline{\alpha}_{i_0},\theta_\ell)) - X_k(x(\underline{\alpha}_{i_0},\theta_{i_0}))|| < \varepsilon''$.
Now choosing $\varepsilon' + \varepsilon'' < \varepsilon$ ends the proof.

□

3.2. Ensuring properness properties

We prove now that there exists a Zariski-closed subset $\mathcal{A} \in GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, the property $\mathcal{P}_1(\mathbf{A})$ holds, which is summarized in the following proposition.

Proposition 3.3. *There exists a Zariski-closed subset $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ and for all $j \in \{1,\ldots,n-1\}$:*

- *Π_j restricted to $W_j^{\mathbf{A}}$ is proper.*

In [43], the authors prove that given a hypersurface $\mathcal{H} \subset \mathbb{C}^{n+1}$, there exists a Zariski-closed subset $\mathcal{A} \subsetneq GL_{n+1}(\mathbb{C})$ such that for $j \in \{1,\ldots,n-1\}$ and for all $\mathbf{A} \in GL_{n+1}(\mathbb{Q}) \setminus \mathcal{A}$, Π_j restricted to $W_j^{\mathbf{A}}$ is proper and satisfies a Nœther normalization property.
This result can not be used as stated in [43], since we consider here the hypersurface defined by $f - T = 0$ and allow only change of variables on $X_1,\ldots,X_n$. Nevertheless, the incremental intersection process, originate from [19, 20, 21], which is used in the proof of [43] allows us to state:

Proposition 3.4. *For $i = 1,\ldots,n$, denote by $\Delta_i^{\mathbf{A}}$ the ideals associated to the Zariski-closure of the constructible set defined by:*

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

There exists a Zariski-closed subset $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ such that:

- *for all $i \in \{1,\ldots,n\}$ and for all prime $P_i^{\mathbf{A}}$ associated to $\Delta_i^{\mathbf{A}}$, the extension $\mathbb{C}[\mathbf{X}_{\geq i+1}] \to \mathbb{C}[\mathbf{X}]/P_i^{\mathbf{A}}$ is integral, where $\mathbf{X}_{\geq i+1}$ denotes $X_{i+1},\ldots,X_n$ and $\mathbf{X}$ denotes $X_1,\ldots,X_n$.*

Using *mutatis mutandis* the proof of [43, Proposition 3, Section 2.5], which is based on [26, Lemma 3.10] relating the properness of π_i to the fact that the above extensions are integral yields the following result:

Lemma 3.5. *Denote by π_{i+1} the projection $(x_1,\ldots,x_n) \in \mathbb{C}^n \to (x_{i+1},\ldots,x_n) \in \mathbb{C}^{n-i}$. There exists a Zariski-closed subset $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ and for all $i \in \{1,\ldots,n\}$, π_{i+1} restricted to the algebraic variety defined by $\Delta_i^{\mathbf{A}}$ is proper.*

Now, remark that there exists a Zariski-closed subset $\mathcal{Z} \subsetneq \mathbb{C}$ such that for all $t \in \mathbb{C} \setminus \mathcal{Z}$, choosing $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ yields the properness of π_{n-i+1} restricted to $W_i^{\mathbf{A}} \cap \{T = t\}$. Now, iterating the above reasoning for each $\theta \in \mathcal{Z}$ yields Zaiski-closed subsets $\mathcal{A}_1, \ldots, \mathcal{A}_p$ such that for all $\mathbf{A} \in GL_n(\mathbb{C}) \setminus (\mathcal{A} \cup_{k=1}^{p} \mathcal{A}_k)$, π_{n-i+1} restricted to $W_i^{\mathbf{A}} \cap \{T = \theta\}$ is proper. This finally shows that for all $t \in \mathbb{C}$, π_i restricted to $W_i^{\mathbf{A}} \cap \{T = t\}$ is proper which ends the proof of Proposition 3.3.

We are now ready to state our main geometric result which characterizes the set of *generalized critical values* of f.

3.3. Main geometric result

The combination of Proposition 3.2, Proposition 3.3 and Lemma 2.6 leads to the following result.

Theorem 3.6 (Geometric characterization of generalized critical values). *There exists a Zariski-closed subset $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ the set $K_\infty(f)$ of asymptotic critical values of f is contained in the set of non-properness of the projection $\pi_T : (x_1, \ldots, x_n, t) \in \mathbb{C}^{n+1} \to t \in \mathbb{C}$ restricted to the Zariski-closure of the constructible set defined by:*

$$f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0.$$

Remark 3.7. Remark that the above result only states that $K_\infty(f)$ is contained in the set of non-properness $\mathcal{Z}$ of the projection $\Pi : (x_1, \ldots, x_n, t) \in \mathbb{C}^{n+1} \to t \in \mathbb{C}$ restricted to W_1. The latter set is zero-dimensional (see [26]). Nevertheless, this inclusion can be strict since some points in $\mathcal{Z}$ can depend on $\mathbf{A}$.

Example. In [44], the authors use [26, Lemma 3.10] to compute the set of non-properness of a projection restricted to an algebraic variety. Denoting by $I^{\mathbf{A}}$ the ideal associated to $W_1^{\mathbf{A}}$, this algorithm specializes in our case to computing the characteristic polynomial of the multiplication by X_1 in $\mathbb{Q}(T)[X_1, \ldots, X_n]/I^{\mathbf{A}}$. The set of non-properness of the projection on T is the union of the zero-sets of the denominators of this characteristic polynomial seen as univariate in X_1.
Consider the polynomial which is already studied in Section 2

$$f = X_1 + X_1^2 X_2 + X_1^4 X_2 X_3$$

Performing the linear change of variables below

$$\begin{array}{rcl} X_1 & \leftarrow & X_1 + X_2 + X_3 \\ X_2 & \leftarrow & X_1 + 2X_2 + 3X_3 \\ X_3 & \leftarrow & X_1 + 4X_2 + 9X_3 \end{array}$$

one finds as a set of non-properness for the projection on T the zero-set of the univariate polynomial below

$$256\,T^2\,(20\,T + 1)$$

whose set of roots contains *strictly* $K_\infty(f)$.

Remark that Theorem 3.6 does not allow here to compute *exactly* $K_\infty(f)$ but only a Zariski-closed subset containing it.

4. The algorithm and its complexity

Given $f \in \mathbb{Q}[X_1, \ldots, X_n]$, we show now how to compute the set of generalized critical values $K(f)$ of the mapping $x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$. Since $K(f) = K_0(f) \cup K_\infty(f)$, we focus first on the computation of $K_0(f)$ and then we deal with the computation of $K_\infty(f)$.
Our algorithms rely on tools coming from polynomial system solving. We use Gröbner bases and the Geometric resolution algorithm. Gröbner bases are a standard tool in polynomial system solving since it allows to test the membership of a polynomial to an ideal, to compute elimination ideals, and to reduce the computation of rational parameterizations of the roots of a zero-dimensional ideal to linear algebra computations in a polynomial ring quotiented by the considered ideal. Gröbner bases have a complexity within $D^{\mathcal{O}(n)}$ arithmetic operations in $\mathbb{Q}$ when the input polynomial family generates a zero-dimensional ideal (see [32]).

The geometric resolution algorithm [22, 34] is more recent and goes back to [19, 20, 21]. The input is a polynomial system of equations and inequations encoded by a straight-line program and defining a constructible set. It returns generic points in each equi-dimensional component of the Zariski-closure of the constructible set defined by the input. These generic points are encoded by rational parameterizations

$$\left\{ \begin{array}{ccc} X_n & = & \frac{q_n(T)}{q_0(T)} \\ & \vdots & \\ X_1 & = & \frac{q_1(T)}{q_0(T)} \\ q(T) & = & 0 \end{array} \right.$$

where T is a new variable. Thus, the output of the geometric resolution algorithm is a list of $n+2$-tuples of univariate polynomials $(q, q_0, q_1, \ldots, q_n)$. This algorithm is probabilistic, but its complexity is well-controlled. We denote by $M(x)$ the cost of multiplying univariate polynomials of degree x and the notation $p \in \mathcal{O}_{\log}(x)$ means that $p \in \mathcal{O}(x \log x^a)$ for some constant a.

Theorem 4.1 (Complexity result for geometric resolution). [34] *Let $g_1, \ldots, g_S$ and g be polynomials of degree bounded by D in $\mathbb{Q}[X_1, \ldots, X_n]$, represented by a straight-line program of length $\mathcal{L}$. There exists an algorithm computing a geometric resolution of the Zariski-closure $V(g_1, \ldots, g_S) \setminus V(g)$ whose arithmetic complexity is:*

$$\mathcal{O}_{\log}(Sn^4(n\mathcal{L} + n^4)M(D\mathfrak{d}))^3$$

where $\mathfrak{d}$ is the maximum among the sums of the algebraic degrees of the irreducible components of the intermediate varieties defined as the Zariski-closures of the constructible sets $g_1 = \cdots = g_i = 0, g \neq 0$ for i in $1, \ldots, S$.

Remark 4.2. In [34], the author proves that the bit complexity of his algorithm is

$$\tau \mathcal{O}_{\log}\left(Sn^4(n\mathcal{L}+n^4)M(D\mathfrak{d})\right)^4$$

where τ bounds the bit-size of the coefficients of the input polynomial system.

In practice, Gröbner bases techniques remain, in general, the fastest tool to solve symbolically polynomial systems, in particular when the algorithms given in [16, 17] are used. The geometric resolution algorithm is implemented as a `Magma` package by G. Lecerf (see [31]).
Hereafter, we describe how to compute $K_0(f)$ and $K_\infty(f)$ using Gröbner bases techniques and the geometric resolution algorithm. When using Gröbner bases, one obtains a deterministic algorithm and an efficient behaviour in practice (see Section 7). When using the geometric resolution algorithm, we obtain a probabilistic algorithm whose complexity is well-controlled.

Computation of $K_0(f)$. The first step of an algorithm computing $K(f)$ is obviously the computation of the set of critical values $K_0(f)$ of f. This is encoded as the set of roots of a univariate polynomial. Denote by I the ideal

$$\langle f-T, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\rangle.$$

Sard's Theorem ensures that there exists a univariate polynomial $P \in \mathbb{Q}[T]$ such that: $\langle P\rangle = I \cap \mathbb{Q}[T]$ and, by definition, the set of roots of P is $K_0(f)$.
Gröbner bases allow such computations of elimination ideals.

Algorithm computing $K_0(f)$ using Gröbner bases

- **Input:** a polynomial f in $\mathbb{Q}[X_1, \ldots, X_n]$.
- **Output:** a univariate polynomial $P \in \mathbb{Q}[T]$ such that its zero-set is $K_0(f)$.
- Compute a Gröbner basis G for an elimination ordering $[X_1, \ldots, X_n] > [T]$ of the ideal generated by:

$$\langle f-T, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\rangle.$$

- Return the element of G belonging to $\mathbb{Q}[T]$.

Remark that $\sharp K_0(f) \leq (D-1)^n$ since it is defined as the values taken by a polynomial on each isolated primary component of an ideal defined by n polynomials of degree $D-1$. So, one could expect to obtain an algorithm computing $K_0(f)$ having a complexity within $(D-1)^{\mathcal{O}(n)}$. This aim can be reached by using the geometric resolution Algorithm. The first step is the computation of rational parameterizations of generic points in each equi-dimensional component of the algebraic variety defined by:

$$\frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0.$$

Once they are obtained, one can obtain the values taken by f at these points which are encoded by a univariate polynomial.

Probabilistic Algorithm computing $K_0(f)$ using the Geometric Resolution Algorithm

- **Input:** a polynomial f in $\mathbb{Q}[X_1, \ldots, X_n]$.
- **Output:** a univariate polynomial $P \in \mathbb{Q}[T]$ such that its zero-set is $K_0(f)$.
- Let G be the rational parameterizations returned by the geometric resolution algorithm taking as input $\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}$.
- For each element $g = (q, q_0, q_1, \ldots, q_n)$ of G, substitute for $i = 1, \ldots, n$ in $f - T$ the variables X_i by $\frac{q_i}{q_0}$. Put the result to the same denominator and compute the resultant of the obtained polynomial with respect to the variable T.
- Return the product of the computed polynomials.

The complexity of the above algorithm is dominated by the cost of computing a geometric resolution of the algebraic variety defined by:

$$\frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0$$

Computation of $K_\infty(f)$. It remains to show how to compute $K_\infty(f)$. Following Remark 3.7 and Example 3.3, this task can be achieved by linear algebra computations in the quotient ring $\mathbb{Q}(T)[X_1, \ldots, X_n]/I^{\mathbf{A}}$ where $I^{\mathbf{A}}$ is the ideal associated to $W_1^{\mathbf{A}}$.

Deterministic Algorithm. In order to obtain a deterministic algorithm, we must check that the chosen linear change of variables $\mathbf{A}$ is generic enough. This will be always possible since the bad choices of $\mathbf{A}$ are contained in a Zariski-closed subset of $GL_n(\mathbb{C})$. Given $f \in \mathbb{Q}[X_1, \ldots, X_n]$, denote by $\deg(f, [X_1, \ldots, X_i])$ the degree of f when it is seen as a polynomial in $\mathbb{Q}(X_{i+2}, \ldots, X_n)[X_1, \ldots, X_i]$ and denote by ϕ_i the mapping sending $f \in \mathbb{Q}[X_1, \ldots, X_n]$ to

$$X_0^{\deg(f,[X_1,\ldots,X_{i+1}])} f(\frac{X_1}{X_0}, \ldots, \frac{X_{i+1}}{X_0}, X_{i+2}, \ldots, X_n).$$

From [30, 44], the properness of Π_i restricted to the Zariski-closure of

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

can be tested by computing the intersection of the projective closure of $W_{n-i}^{\mathbf{A}}$ in $\mathbb{P}^{i+1}(\mathbb{C}) \times \mathbb{C}^{n-i}$ and the hyperplane at infinity. This can be done by Gröbner bases computations (see [13]). A preliminary test consists in applying ϕ_i to the system defining $W_{n-i}^{\mathbf{A}}$, instantiating X_0 to 1 and check that when substituting X_k by 1 (for $k = 1, \ldots, i-1$), the obtained polynomial system generates $\langle 1 \rangle$. Using Gröbner bases, such computations are particularly efficient when the choice of $\mathbf{A}$ is a correct one. Modular computations can also be used to perform some preliminary tests on sparse matrices $\mathbf{A} \in GL_n(\mathbb{Q})$.

In the sequel we denote by `SetOfNonProperness` a subroutine taking as input a polynomial system of equations and inequations and a set of variables and computes a Zariski-closed strict subset containing the set of non-properness of the projection on the variables given as input restricted to the Zariski-closure of the constructible set defined by the input polynomial system. Such a procedure is described in [30, 44]. Using Gröbner bases, such a procedure works as follows. Consider a polynomial family F, a polynomial g, U a new variable and G a Gröbner basis of the ideal $\langle Ug-1, F\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]$ (which is supposed to have dimension d) with respect to a DRL block ordering $[X_1, \ldots, X_d] < [X_{d+1}, \ldots, X_n]$. The set of non-properness of the projection on $X_1, \ldots, X_d$ restricted to the set of common complex zeroes of F is contained as the union of the complex zero sets of the leading coefficients of the polynomials of G seen in $\mathbb{Q}(X_1, \ldots, X_d)[X_{d+1}, \ldots, X_n]$ whom leading monomials are the smallest pure powers of X_i for $i \in \{d+1, \ldots, n\}$.

Algorithm computing $K_\infty(f)$ using Gröbner bases

- **Input:** a polynomial f in $\mathbb{Q}[X_1, \ldots, X_n]$.
- **Output:** a univariate polynomial $P \in \mathbb{Q}[T]$ such that its zero-set contains $K_\infty(f)$.
- Choose randomly $\mathbf{A} \in GL_n(\mathbb{C})$ and check if it is generic enough until this test returns true.
- Return `SetOfNonProperness`($[f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}} = 0, \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0], \{T\}$)

Probabilistic Algorithm. As in the case of the computation of $K_0(f)$, Gröbner bases do not allow to obtain complexity results even if the first choice of $\mathbf{A}$ is supposed to be correct. To reach this aim, one also uses extensions of the geometric resolution algorithms allowing to lift the parameter. Here, in the input polynomial system

$$f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}} = 0, \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0$$

T is considered as the parameter. From [2], if $\mathbf{A}$ is generic enough, this defines a zero-dimensional system generating a radical ideal in $\mathbb{Q}(T)[X_1, \ldots, X_n]$. The output is a geometric resolution

$$\left\{ \begin{array}{ccc} X_n & = & \frac{q_n(X_1,T)}{q_0(X_1,T)} \\ & \vdots & \\ X_2 & = & \frac{q_2(X_1,T)}{q_0(X_1,T)} \\ q(X_1,T) & = & 0 \end{array} \right.$$

The set of non properness of the projection on T restricted to the Zariski-closure of the constructible set defined by the input polynomial system is contained the least commun multiple of the denominators of the coefficients of q.

Probabilistic Algorithm computing $K_\infty(f)$ using the Geometric Resolution Algorithm

- **Input:** a polynomial f in $\mathbb{Q}[X_1, \ldots, X_n]$.
- **Output:** a univariate polynomial $P \in \mathbb{Q}[T]$ such that its zero-set contains $K_\infty(f)$.
- Consider T as a parameter in the polynomial system $f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}} = 0, \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0$ and compute a geometric resolution.
- Lift the parameter.
- Return the least common multiple of the denominators in the coefficients of the polynomial q.

Complexity estimates. Using Theorem 4.1 (see [34]), the probabilistic versions of the algorithms computing $K_0(f)$ and $K_\infty(f)$ allow to perform a complexity analysis. Indeed, using strong versions of Bézout theorems (see [18]), the sum of the degrees of the primary components of the ideal generated by :

$$\frac{\partial f}{X_1} = \cdots = \frac{\partial f}{X_n} = 0$$

is bounded by $(D-1)^n$ (where D is the degree of f). Thus, the polynomial returned by the probabilistic algorithm computing $K_0(f)$ has a degree bounded by $(D-1)^n$. We focus now on the computation of $K_\infty(f)$. Our algorithm computed a polynomial encoding the set of non-properness of a projection restricted to the curve defined as the Zariski-closure of the solution set:

$$f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}}, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0$$

which has a degree bounded by $(D-1)^{n-1}$ since, from Bézout's theorem the Zariski-closure of the complex solution set of .

$$f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}}, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0$$

has degree at most $(D-1)^{n-1}$. From [47], the lifting of the parameter T has a complexity which is log-linear in the evaluation complexity of the above system and quadratic in the degree of the studied curve.
Bounding the evaluation complexity of f by D^n, this discussion leads to the following complexity result.

Theorem 4.3 (Complexity result). *The above probabilistic algorithm computing $K_0(f)$ performs at most $\mathcal{O}(n^7 D^{4n})$ arithmetic operations in $\mathbb{Q}$.*

The above probabilistic algorithm computing $K_\infty(f)$ performs at most $\mathcal{O}(n^7D^{4n})$ arithmetic operations in $\mathbb{Q}$.

Remark 4.4. Using Remark 4.2, the bit-complexity of the probabilistic versions of our algorithms is $\mathcal{O}(\tau n^7 D^{5n})$ where τ bounds the bit-size of the coefficients in f.

5. Application I: testing the emptiness of a semi-algebraic set defined by a single inequality

In this section, we show how to use the above algorithm to compute at least one point in each connected component of a semi-algebraic set defined by a single inequality.

Remark that, given $f \in \mathbb{Q}[X_1,\ldots,X_n]$, if there does not exist $x \in \mathbb{R}^n$ such that $f(x)=0$, it is sufficient to evaluate f at a point $x \in \mathbb{R}^n$ at which it does not vanish and return x if $f(x)>0$. We focus now on the case where there exists $x \in \mathbb{R}^n$ such that $f(x)=0$.

Theorem 5.1 (Semi-algebraic sets). *Let f be a polynomial in $\mathbb{Q}[X_1,\ldots,X_n]$ and $\mathcal{S}$ be the semi-algebraic set defined by $f>0$. Suppose that there exists $x \in \mathbb{R}^n$ such that $f(x)=0$ and let $e \in \mathbb{Q}$ be such that $0<e<\min(|r|, r \in K(f)\cap\mathbb{R})$.*
Consider the hypersurface $\mathcal{H}_e$ defined by $f-e=0$. Then, for each connected component S of $\mathcal{S}$, there exists a connected component C of $\mathcal{H}_e \cap \mathbb{R}^n$ such that $C \subset S$.

Proof. Let ε be an infinitesimal and $\mathcal{H}_\varepsilon \subset \mathbb{C}\langle\varepsilon\rangle^n$ be the hypersurface defined by $f-\varepsilon=0$. Since, by assumption, there exists $x \in \mathbb{R}^n$ such that $f(x)=0$, from the intermediate value theorem, each connected component S of $\mathcal{S}$ contains a point x_S such that $f(x_S)=\varepsilon$. The connected component $C_{x_S} \subset \mathbb{R}\langle\varepsilon\rangle^n$ of $\mathcal{H}_\varepsilon \cap \mathbb{R}\langle\varepsilon\rangle^n$ is contained in S since f does not vanish on C_{x_S}.
From the transfer principle, this implies that there exist $e_0>0$ such that for all $0<e'<e_0$ and for all connected component S of $\mathcal{S}$ there exists a connected component $C_{e'}$ of the real locus of the hypersurface defined by $f-e'=0$ such that $C_{e'} \subset S$. Consider such a rational number e' and a positive rational number e such that $0<e<\min(|r|, r\in K(f))$. We prove now that there exists a connected component C_e of the real locus of the hypersurface defined by $f-e=0$ such that $C_e \subset S$ for all connected component S of $\mathcal{S}$.
Suppose that e' is chosen small enough such that $K(f)\cap]0,e'[=\emptyset$. If $0<e<e'$, the assertion follows immediately.
Suppose now that $e>e'$. From [35, Theorem 3.1], f realizes a locally trivial fibration on $\mathbb{R}^n \setminus f^{-1}(K(f))$. This implies that there exists a diffeomorphism φ such that, for all $e_1 \in]e', e[$, denoting by π the projection on the second member

of the cartesian product $f^{-1}(e_1)\times]e,e'[$ the following diagram is commutative

$$\begin{tikzcd} f^{-1}(e_1)\times]e,e'[\arrow[r, "\varphi"] \arrow[dr, "\pi"'] & f^{-1}(]e,e'[) \arrow[d, "f"] \\ &]e,e'[\end{tikzcd}$$

This implies that one can link any point $x_{e'}$ of $C_{e'}$ to a point x_e in $\mathcal{H}_e \cap \mathbb{R}^n$ via a continuous path on which f does not vanish. Then, x_e belongs to S and if C_e denotes the connected component of $\mathcal{H}_e \cap \mathbb{R}^n$ containing x_e, one has $C_e \subset S$ since f is constant on C_e. □

Remark 5.2. From Theorem 5.1, deciding the emptiness of the semi-algebraic set defined by $f > 0$ is reduced to decide if a hypersurface defined by a polynomial with coefficients in $\mathbb{Q}$ contains real points.
Substituting f by $-f$ one can deal with semi-algebraic sets defined by $f < 0$. Finally, computing at least one point in each connected component of the semi-algebraic set defined by $f \neq 0$ is done by computing at least one point in each connected component of the semi-algebraic sets defined by $f > 0$ and $f < 0$.

The Algorithm. The algorithm relies on Theorem 5.1. Given a polynomial f in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree D, the algorithm computes at least one point in each connected component of the semi-algebraic set defined by $f > 0$. The first step is the computation of the set of generalized critical values of the mapping $f : x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$. Using the probabilistic version of the algorithm provided in Section 4, this can be done within $\mathcal{O}(n^7 D^{4n})$ arithmetic operations in $\mathbb{Q}$.
We have seen in the preceeding section that the degree of the polynomials encoding generalized critical values is bounded by $\mathcal{O}(D^n)$. Their coefficients have a bit-size which is bounded by $\mathcal{O}(\tau D^n)$ if τ bounds the bit-size of the input polynomial system (see [10]). Thus, isolating the real solutions of the polynomial encoding the set of generalized critical values of f is done within $\mathcal{O}(\tau D^{4n})$ arithmetic operations in $\mathbb{Q}$ using the variant of Uspensky's algorithm designed in [41]. Choosing a positive rational number e between 0 and the smallest positive real generalized critical value is immediate.
It remains to compute at least one point in each connected component of the real counterpart of the hypersurface defined by $f - e = 0$. This can be done using the algorithm designed in [43] within $\mathcal{O}(n^7 D^{3n})$ arithmetic operations in $\mathbb{Q}$. This algorithm is based on computations of critical loci of generic projections.
If this step does not return any point, then one has to evaluate f at a point x of $\mathbb{R}^n$ at which it does not vanish and return this point if $f(x) > 0$.
The above discussion leads to the following theorem.

Theorem 5.3 (Complexity result). *Let f be a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree D and $\mathcal{S}$ be the semi-algebraic set defined by $f > 0$. The probabilistic version of the above algorithm computes at least one point in each connected component of $\mathcal{S}$ with a complexity within $\mathcal{O}(n^7 D^{4n})$ arithmetic operations in $\mathbb{Q}$.*

6. Application II: determining the existence of real regular points in a hypersurface

In this section, we focus on the following problem: given a polynomial $f \in \mathbb{Q}[X_1, \dots, X_n]$ of degree D, decide if the hypersurface $\mathcal{H}$ defined by $f = 0$ contains real regular points. Hence, the problem consists in deciding if the real dimension of $\mathcal{H} \cap \mathbb{R}^n$ equals the complex dimension of $\mathcal{H}$. This problem appears in many applications (in particular in automated geometric reasoning or in computational geometry [14]) studying generic geometric situations.

This can be solved using the Cylindrical Algebraic Decomposition but the complexity of this method is doubly exponential in the number of variables and, in practice, this method is limited to problems having 3 or 4 variables.

Such a problem can also be tackled by computing the *real radical* of the ideal $\langle f \rangle \subset \mathbb{Q}[X_1, \dots, X_n]$ (which is the radical ideal of $\mathbb{Q}[X_1, \dots, X_n]$ whose associated algebraic variety is the smallest one – for the inclusion ordering – containing $\mathcal{H} \cap \mathbb{R}^n$). This can be done by using the algorithms designed in [8]. These algorithms perform a recursive study on imbricated singular loci of the studied varieties. Up to our knowledge, bounding the degree of the singular locus of a variety, the degree of the singular locus of the singular locus and so on yields doubly exponential bounds in the number of variables. Thus, the complexity of such methods seems to be doubly exponential in the number of variables and no efficient implementation have been obtained from these works.

The real dimension of $\mathcal{H}$ can be computed using [7, Chapter 14]. The complexity of this algorithm is $D^{\mathcal{O}(n^2)}$. Nevertheless, this algorithm does not provide satisfactory results in practice due to the use of several infinitesimals and some growth of degree which are difficult to manage in practical implementations and lead to a high complexity constant (which is here as an exponent).

All the methods above compute exactly the real dimension of $\mathcal{H} \cap \mathbb{R}^n$ which is stronger than the expected output. In the case where f is square-free, the problem in which we are interested can be tackled by deciding if all the semi-algebraic sets $\mathcal{S}_i \subset \mathbb{R}^n$ defined by $f = 0, \frac{\partial f}{\partial X_i} \neq 0$ (for $i = 1, \dots, n$) are empty or not. Each semi-algebraic set $\mathcal{S}_i$ is studied by studying the real algebraic sets of $\mathbb{R}\langle\varepsilon\rangle^n$ defined by $f = \frac{\partial f}{\partial X_i} - \varepsilon = 0$ and $f = \frac{\partial f}{\partial X_i} + \varepsilon = 0$. The complexity of this method is $D^{\mathcal{O}(n)}$ but we are lead here to study n distinct semi-algebraic sets defined by an equation (of degree D) and an inequation (of degree $D-1$).

In the sequel, we show how to reduce the problem of determining the existence of real regular points in a hypersurface defined by $f = 0$ to the problem of deciding if there exist $(x, x') \in \mathbb{R}^n \times \mathbb{R}^n$ such that $f(x) > 0$ and $f(x') < 0$. The probabilistic version of our algorithm has a complexity within $\mathcal{O}(n^7 D^{4n})$ arithmetic operations in $\mathbb{Q}$.

Theorem 6.1 (Existence of regular real points). *Let f be a square-free polynomial in $\mathbb{Q}[X_1, \dots, X_n]$ and $\mathcal{H} \subset \mathbb{C}^n$ be the hypersurface defined by $f = 0$. There exist* *regular real points in $\mathcal{H}$ if and only if there exist $(x, x') \in \mathbb{R}^n \times \mathbb{R}^n$ such that $f(x) > 0$ and $f(x') < 0$.*

Proof. Suppose first that $\mathcal{H}$ contains real regular points and let y be such a point. Since f is square-free, one has $\mathbf{grad}_y(f) \neq \mathbf{0}$. Now, considering the line passing through y and supported by the vector $\mathbf{grad}_y(f)$ and a Taylor development of f along this line near y, it is clear that f is positive and negative along this line.
Suppose now that $\mathcal{H}$ does not contain a real regular zero. Then, the real locus of $\mathcal{H}$ (which may be empty) is contained in the singular locus of $\mathcal{H}$. Since the co-dimension of the singular locus of $\mathcal{H}$ is greater than 1, the complementary of $\mathcal{H} \cap \mathbb{R}^n$ in $\mathbb{R}^n$ is connected. This implies that either the semi-algebraic set defined by $f > 0$ is empty or the semi-algebraic set defined by $f < 0$ is empty. □

The Algorithm. The algorithm based on Theorem 6.1 works as follows. The input of the algorithm is a polynomial f in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree D. Compute the square-free part of f.
Determine the sign of f on a randomly chosen point at which f does not vanish. In practice, this step is immediate while in theory, one has to test each point in a grid of size D^{n^2} to be sure to find a point at which f does not vanish. Since our complexity estimates are based on probabilistic algorithms, we suppose that the cost of this step is the one of the evaluation of f, i.e. $\mathcal{O}_{\log}(D^n)$ arithmetic operations in $\mathbb{Q}$.
If f is found to be positive on the test-point, test the emptiness of the semi-algebraic defined by $f < 0$, else test the emptiness of the semi-algebraic set defined by $f > 0$. Using the algorithm designed in Section 5 using the computation of generalized critical values, this is done within $\mathcal{O}(n^7 D^{4n})$ arithmetic operations in $\mathbb{Q}$.

7. Practical results

We have implemented the algorithms presented in Sections 4, 5 and 6 using Gröbner bases.
The Gröbner engine which is used is FGb [15] which is implemented in `C` by J.-C. Faugère. Computing rational parametrizations of the complex roots of a zero-dimensional ideal from a Gröbner basis is done by RS [37] which is implemented in `C` by F. Rouillier. Isolation of real roots of univariate polynomials with rational coefficients is done by RS using the algorithm provided in [41].
The resulting implementation is a part of the RAGLib Maple library (release 2.21) [42]. We do not describe implementation details allowing us to avoid an *explicit* linear change of variables by using a choice of generic projections. We also don't describe modular tests which allow us to test if the chosen projections are good. However, we observe that the first choices have always been correct.
All the computations have been performed on a PC Intel Pentium Centrino Processor 1.86 GHz with 2048 Kbytes of Cache and 1024 MB of RAM.

7.1. Description of the test-suite.

The following polynomial appears in a problem of algorithmic geometry studying the Voronoi Diagram of three lines in $\mathbb{R}^3$. In [14], the authors focus on determining topology changes of the Voronoi diagram of three lines in $\mathbb{R}^3$. The question was first reduced to determining if the zero-set of discriminant of the following polynomial with respect of the variable u contains real regular points. This discriminant has degree 30. This discriminant is the product of a polynomial of degree 18 and several polynomials up to an odd power whom zero-set could not contain a real regular point since they are sums of squares. The polynomial of degree 18 is **Lazard II**. D. Lazard and S. Lazard have also asked to determine if the following polynomial which is denoted by **Lazard I** in the sequel is always positive.

$$\begin{aligned}
&16\,a^2\left(\alpha^2+1+\beta^2\right)u^4+16\,a\left(-\alpha\,\beta\,a^2+ax\alpha+2\,a\alpha^2+2\,a+2\,a\beta^2+ay\beta-\alpha\,\beta\right)u^3+\\
&\left(\left(24\,a^2+4\,a^4\right)\alpha^2+\left(-24\,\beta\,a^3-24\,a\beta-8\,ya^3+24\,xa^2-8\,ay\right)\alpha+24\,a^2\beta^2+4\,\beta^2-\right.\\
&\left.8\,\beta\,xa^3+4\,y^2a^2+24\,y\beta\,a^2-8\,ax\beta+16\,a^2+4\,x^2a^2\right)u^2+\left(-4\,\alpha\,a^3+4\,ya^2-\right.\\
&\left.4\,ax-8\,a\alpha+8\,\beta\,a^2+4\,\beta\right)\left(\beta-a\alpha+y-ax\right)u+\left(a^2+1\right)\left(\beta-a\alpha+y-ax\right)^2
\end{aligned}$$

In the sequel, we denote by **Lazard I** the above polynomial and by **Lazard II** the discriminant of **Lazard I** with respect to the variable u.

The following polynomial appears in [29]. The problem consists in determining the conditions on a, b, c and d such that the ellipse defined by:

$$\frac{(x-c)^2}{a^2}+\frac{(y-d)^2}{b^2}=1$$

is inside the circle defined by $x^2+y^2-1=0$. The problem is reduced to compute at least one point in each connected component of the semi-algebraic set defined as the set of points at which the polynomial below (which is called in the sequel **Ellipse-Circle**) does not vanish.

$$\begin{aligned}
&4\,a^6c^2d^2+2\,a^2b^2d^6-6\,a^2b^2d^4+a^4c^4+2\,a^4c^2d^6-6\,a^2b^2c^4-6\,a^4b^2c^4+4\,a^6b^2d^2+\\
&a^8b^4+6\,b^4c^2d^2-2\,b^6c^4d^2+a^8d^4+6\,a^2b^6d^2-8\,a^4b^4d^2-4\,a^4b^2d^6-6\,b^4c^4d^2-8\,a^4b^4c^2+\\
&6\,a^6b^2c^2-8\,a^2b^4c^2+6\,a^4b^4d^4-2\,b^4c^2d^4-4\,a^2b^4c^6-4\,a^6b^4c^2-6\,a^2b^4d^4-2\,a^4c^4d^2+\\
&10\,a^4b^2d^4-2\,a^2b^8c^2-6\,a^2b^6c^4+a^4b^8+6\,a^2b^2d^2+6\,a^6b^4d^2-4\,a^4b^6d^2+b^4d^4+b^4c^8+\\
&10\,a^2b^4c^4+6\,a^2b^2c^2+4\,a^2b^6c^2+a^4d^8+4\,b^6c^2d^2+6\,a^4b^6c^2-8\,a^4b^2d^2+\\
&4\,a^4b^2c^2-2\,a^8b^2d^2+6\,a^4c^2d^2+4\,a^2b^4d^2-6\,a^6b^2d^4+6\,a^4b^4c^4-2\,a^6c^2d^4+\\
&2\,b^4c^6d^2+2\,a^2b^2c^6-6\,a^4c^2d^4+b^8c^4+2\,a^4b^2-4\,a^4d^2+a^4-2\,b^6-2\,a^6+a^8+\\
&b^8+b^4+2\,a^2b^4+2\,b^6c^6-2\,b^8c^2-6\,b^6c^4+2\,a^6b^4-2\,a^2b^2-2\,a^6b^6+2\,a^4b^6-\\
&2\,a^2b^8-6\,a^4b^2c^4d^2+2\,a^2b^4c^4d^2+2\,a^4b^2c^2d^4-6\,a^2b^4c^2d^4-6\,a^4b^2c^2d^2-6\,a^2b^4c^2d^2+\\
&4\,a^2b^2c^4d^4+2\,a^2b^2c^2d^6+2\,a^2b^2c^4d^2+2\,a^2b^2c^2d^4-10\,a^2b^2c^2d^2+6\,a^2b^6c^2d^2-\\
&6\,a^4b^4+2\,a^2b^6-2\,a^8b^2+2\,a^6b^2+6\,a^6b^2c^2d^2-10\,a^4b^4c^2d^2-4\,b^4c^6+6\,b^4c^4+6\,b^6c^2-\\
&2\,a^6c^2+2\,a^2b^2c^6d^2+a^4c^4d^4-2\,a^4c^2-2\,b^6d^2-4\,a^4d^6+2\,a^6d^6-\\
&2\,a^8d^2-6\,a^6d^4+6\,a^6d^2+b^4c^4d^4-4\,b^4c^2+6\,a^4d^4-2\,b^4d^2
\end{aligned}$$

The following polynomials which is called in the sequel $\mathbf{LL}_n$ are studied in [33]. They are used as a benchmark for algorithms decomposing polynomials in sums of squares (see also [48]).

$$\sum_{i=1}^{n} \prod_{j \neq i} (X_i - X_j)$$

In the sequel we consider **LL5** (which has degree 4 and contains 5 variables) and **LL6** (which has degree 5 and contains 6 variables).
The following polynomial, which is called **Cusp** in the sequel, appears in [12] for the study of cuspidal robots.

$$\begin{aligned}
-4\, d_4\, {d_3}^3 X^4 - 2\, \rho^2 {d_3}^2 X^4 + 2\, \rho^2 z^2 X^4 + {d_3}^4 X^4 + 4\, d_4\, d_3\, z^2 X^4 + \\
4\, X^4 + z^4 X^4 - 4\, \rho^2 X^4 + \rho^4 X^4 + {d_4}^4 X^4 - 4\, {d_4}^3 d_3\, X^4 + 6\, {d_4}^2 {d_3}^2 X^4 + \\
4\, d_4\, d_3\, \rho^2 X^4 - 2\, z^2 {d_3}^2 X^4 - 2\, \rho^2 {d_4}^2 X^4 - 2\, z^2 {d_4}^2 X^4 + \\
8\, d_4\, {d_3}^2 X^3 - 16\, d_3\, {d_4}^2 X^3 - 8\, d_4\, z^2 X^3 + 8\, {d_4}^3 X^3 - 8\, d_4\, \rho^2 X^3 + 16\, d_4\, X^3 + \\
2\, \rho^4 X^2 - 4\, z^2 {d_3}^2 X^2 + 2\, z^4 X^2 - 4\, z^2 {d_4}^2 X^2 - 8\, \rho^2 X^2 - 4\, {d_4}^2 {d_3}^2 X^2 + \\
32\, {d_4}^2 X^2 - 4\, \rho^2 {d_3}^2 X^2 + 8\, X^2 + 2\, {d_4}^4 X^2 + 2\, {d_3}^4 X^2 + 4\, \rho^2 z^2 X^2 - \\
4\, \rho^2 {d_4}^2 X^2 - 8\, d_4\, \rho^2 X + 8\, {d_4}^3 X + 16\, d_3\, {d_4}^2 X + 8\, d_4\, {d_3}^2 X - 8\, d_4\, z^2 X + \\
16\, d_4\, X - 2\, z^2 {d_3}^2 - 2\, \rho^2 {d_3}^2 + 4\, {d_4}^3 d_3 - 2\, \rho^2 {d_4}^2 + 6\, {d_4}^2 {d_3}^2 - \\
4\, \rho^2 - 2\, z^2 {d_4}^2 - 4\, d_4\, d_3\, z^2 + {d_4}^4 + 4\, d_4\, {d_3}^3 + \rho^4 + {d_3}^4 + \\
4 - 4\, d_4\, d_3\, \rho^2 + z^4 + 2\, \rho^2 z^2
\end{aligned}$$

7.2. Practical Results

Below, in the column **JK** we give the timings for computing generalized critical values by using the algorithm of [35]. We obviously use the same Gröbner engine `FGb` for both algorithms. The column **AlgoHyp** corresponds to the maximum of the timings obtained by

- our algorithm computing at least one point in each connected component of the semi-algebraic set defined by the positivity of our input;
- our algorithm computing at least one point in each connected component of the semi-algebraic set defined by the negativity of our input.

The column **CAD** contains the timings of an implementation of the open CAD algorithm in Maple which is due to G. Moroz and F. Rouillier. It outputs a set of rational points in each cell homeomorphic to $]0,1[^n$ (where n is the number of variables) of a CAD adapted to the input polynomial. The symbol ∞ means that the computations have been stopped after 2 days of computations without getting a result.
For all the examples we consider, the implementation of the algorithms provided in [7, Chapter 13] either do not end after 2 days of computation or require too much memory.
On problems having at most 4 variables, the open CAD algorithm behaves well (except on polynomials having a big degree) and our implementation has comparable timings even if it is sometimes slower. On problems having more variables, our implementation ends with reasonnable timings while open CAD either does not end after 2 days of computations or requires too much memory. This is mainly due to the highest degrees appearing in the projection step of CAD while the

degrees of the polynomials appearing during the execution of our algorithms is better controlled.

Concerning our algorithm, on all these examples, the execution time of the computation of generalized critical values is neglictible compared to the time spent in the computation of sampling points in a hypersurface.

Note also that our algorithm is now implemented using a Gröbner basis engine which can be strongly improved for problems having 3 or 4 variables. In these situations, we expect to obtain strong improvements. Finally, remark that the generic choice of projections to compute generalized critical values induces a growth of coefficients which reduces the practical performances of our contribution. We plan now to investigate how to compute generalized critical values without any change of variables. This could strongly speed up our contribution. That's why we are convinced that our method is a promising one.

Pbm	**♯vars**	**Degree**	**JK**	**AlgoHyp**	**CAD**
Lazard I	6	8	∞	60 sec.	∞
Lazard II	5	18	∞	10 hours.	∞
Ellipse-Circle	4	12	∞	90 sec.	5 min.
LL5	5	4	∞	10 sec.	20 sec.
LL6	6	5	∞	7 min.	∞
Cusp	5	8	∞	10 sec.	20 min.

Computation time obtained on a PC Intel Pentium Centrino Processor 1.86 GHz with 2048 Kbytes of Cache and 1024 MB of RAM.

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. *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] E. Becker and R. Neuhaus *Computation of real radicals for polynomial ideals*. Computational Algebraic Geometry, Vol. 109 of Progress in Mathematics, pp. 1–20, Birkhaüser, 1993.

[9] R. Benedetti, J.-J. Risler *Real algebraic and semi-algebraic sets*. Actualités Mathématiques, Hermann, 1990.

[10] J.-B. Bost, H. Gillet and C. Soulet, Heights of projective varieties and positive Green forms, *J. Amer. Math. Soc.*, **7**(4):903-1027, 1994.

[11] G.E. Collins, Quantifier elimination for real closed fields by cylindrical algebraic decomposition. *Lecture notes in computer science*, 33:515-532, 1975.

[12] Corvez, Solen and Rouillier, Fabrice, Using computer algebra tools to classify serial manipulators, *Proceedings of Automated Deduction in Geometry*, F. Winkler (eds), Lecture Notes in Artificial Intelligence, **2930**:31–43, 2003,

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

[14] H. Everett, D. Lazard, S. Lazard, and M. Safey El Din. The topology of the Voronoi diagram of three lines in $\mathbb{R}^3$. Proceedings of Symposium on Computational Geometry, ACM Press, South-Korea, 2007.

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

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

[17] 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.

[18] W. Fulton, Intersection Theory. *Ergebnisse der Mathematik und ihrer Grenzgebiete*, 2. Springer-Verlag, 1984.

[19] 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.

[20] 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.

[21] 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.

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

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

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

[25] 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.

[26] Z. Jelonek. Testing sets for properness of polynomial mappings. *Mathematische Annalen*, 315(1):1–35, 1999.

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

[28] Z. Jelonek, K. Kurdyka. On asymptotic critical values of a complex polynomial. *Journal für die Reine und Angewandte Mathematik*, 565:1–11, 2003.

[29] D. Lazard. Quantifier elimination: optimal solution for two classical examples. Journal of Symbolic Computation, 5(1-2):261-266, 1988.

[30] D. Lazard and F. Rouillier. Solving parametric polynomial systems. Journal of Symbolic Computation, 42:636-667, 2007.

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

[32] Y.N. Lakshman. A single exponential bound of the complexity of computing Gröbner bases of zero-dimensional ideals. In C. Traverso T. Mora, editor, *Proc. Effective Methods in Algebraic Geometry*, MEGA, vol. 94 of Progress in Mathematics, pages 227–234. Birkhäuser, 1991.

[33] A. Lax and P. Lax, On sums of squares, Linear Algebra App., **20**, 71-75, 1978.

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

[35] K. Kurdyka, P. Orro, S. Simon, *Semi-algebraic Sard's theorem for generalized critical values.* Journal of Differentiable Geometry **56** (2000), 67–92.

[36] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. *Journal of Symbolic Computation*, 13(3):255–352, 1992.

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

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

[39] 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.

[40] F. Rouillier, M. Safey El Din., and E. Schost. Solving the Birkhoff Interpolation Problem via the Critical Point Method : an Expermiental Study, Lecture Notes in Computer Science, Automated deduction in geometry, ADG'2000, Zurich, Switzerland, September 25-27, revised papers, Editors: J. Richter-Gebert, D. Wang, Springer-Verlag, Heidelberg, 2000..

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

[42] M. Safey El Din. RAGLib (Real Algebraic Geometry Library). available at `http://www-spiral.lip6.fr/∼safey/RAGLib`, June, 2007.

[43] 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.

[44] 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*, 32(3):417–430, 2004.

[45] M. Safey El Din, Finding sampling points on real hypersurfaces is easier in singular situations. *Electronic proceedings of MEGA*, 2005.

[46] M. Safey El Din, *Generalized critical values and solving polynomial inequalities.* Proceedings of International Conference on Polynomial Systems (2004).

[47] E. Schost, Computing Parametric Geometric Resolutions. *Journal of Applicable Algebra in Engineering, Communication and Computing*, 13(5): 349 - 393, 2003.

[48] M. Schweighofer, Global optimization of polynomials using gradient tentacles and sums of squares, *SIAM Journal on Optimization*, **17**, No 3, 920–942, 2006.

[49] I. Shafarevich, *Basic Algebraic Geometry I*, Springer-Verlag, (1977).

Mohab Safey El Din.
University Pierre et Marie Curie
LIP6 SPIRAL Team,
INRIA/LIP6/UPMC SALSA Project
104, avenue du Président Kennedy
75016 Paris FRANCE
e-mail: `Mohab.Safey@lip6.fr`