Computing the Global Optimum of a Multivariate Polynomial over the Reals

Mohab Safey El Din
INRIA, Paris-Rocquencourt Center, SALSA Project
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingéniérie 919, LIP6 Passy-Kennedy,
Case 169, 4, Place Jussieu, F-75252 Paris Cedex
Mohab.Safey@lip6.fr

ABSTRACT

Let f be a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree D. We provide an efficient algorithm in practice to compute the global supremum $\sup_{x\in\mathbb{R}^n} f(x)$ of f (or its infimum $\inf_{x\in\mathbb{R}^n} f(x)$). The complexity of our method is bounded by $D^{\mathcal{O}(n)}$. In a probabilistic model, a more precise result yields a complexity bounded by $\mathcal{O}(n^7 D^{4n})$ arithmetic operations in $\mathbb{Q}$. Our implementation is more efficient by several orders of magnitude than previous ones based on quantifier elimination. Sometimes, it can tackle problems that numerical techniques do not reach. Our algorithm is based on the computation of generalized critical values of the mapping $x \to f(x)$, i.e. the set of points $\{c \in \mathbb{C} \mid \exists (x_\ell)_{\ell\in\mathbb{N}} \subset \mathbb{C}^n \; f(x_\ell) \to c, \quad ||x_\ell||||d_{x_\ell} f|| \to 0 \text{ when } \ell \to \infty\}$. We prove that the global optimum of f lies in its set of generalized critical values and provide an efficient way of deciding which value is the global optimum.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algorithms*; G.1.6 [**Mathematics of computing**]: Numerical Analysis—*Optimization*; F.2.2 [**Theory of Computation**]: Analysis of algorithms and problem complexity—*Non numerical algorithms and problems: Geometrical problems and computation*

General Terms

Algorithms

Keywords

Global optimization, Polynomial system solving, real solutions, complexity

1. INTRODUCTION

Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be a multivariate polynomial of degree D. We consider below the problem of computing the global supremum of f, i.e. $\sup_{x\in\mathbb{R}^n} f(x)$.

Motivation and description of the problem. Global optimization of multivariate polynomials is a classical problem of scientific computing which appears in numerous applications from various fields (control theory, chemistry, economics, etc.). Hence, obtaining certified and efficient algorithms in practice solving this problem is a question of first importance.

Recently, numerical methods have been developed to tackle this problem. The algorithm of [32] is designed for unconstrained optimization and solves in fact an LMI (Linear Matrix Inequality) relaxation of the polynomial optimization problem. The algorithm of [26] is designed for polynomial constraint optimization and constructs also, in a different way, an LMI relaxation of the initial problem. The problem is that, according to [21, 13], a lot of LMI problems are ill-conditioned. In general, mixing numerical instability and ill-conditioning provides bad results in terms of quality of the output. As far as we know, in the context of global polynomial optimization, the conditioning of LMI problems and their numerical stability is a subject which has not been intensively investigated.

In this paper, we focus on symbolic methods to compute $\sup_{x\in\mathbb{R}^n} f(x)$ without assumption on f. Our aim is to design an efficient algorithm in practice which can be complementary to numerical methods when they fail. We focus on certified algorithms, but we also consider probabilistic ones, for complexity estimates.

The first way of computing $\sup_{x\in\mathbb{R}^n} f(x)$ by computer algebra techniques is to rewrite this problem as a quantifier elimination problem: $\exists e \in \mathbb{R} \; \forall x \in \mathbb{R}^n \quad f(x) \leq e$ and $\forall \varepsilon \in \mathbb{R} \; \exists x \in \mathbb{R}^n \varepsilon > 0 \; f(x) > e - \varepsilon$. This problem can be solved using the cylindrical algebraic decomposition algorithm [9]. Nevertheless, it has a complexity which is doubly exponential in the number of variables and polynomial in the degree of f. The best implementations of this algorithm are limited to problems having 3 or 4 variables. Quantifier elimination problems can also be solved using the critical point method (see [6] and [7, Chapter 14]). The complexity of these methods is doubly exponential in the number of quantifiers. Thus, in the case of global polynomial optimization, this yields an algorithm (see [7, Chapter 14, Section 14.4])

ISSAC'08, July 20–23, 2008, Hagenberg, Austria.

whose complexity is $D^{\mathcal{O}(n)}$ since the number of quantifiers is fixed. Nevertheless, the reduction of global optimization problems to quantifier elimination induces a growth of the complexity constant. Moreover, the algorithms in [7, Chapter 14] are exclusively designed to obtain deterministic complexity results. Algebraic manipulations and infinitesimals which are introduced to obtain complexity results spoil practical computations. This explains why no efficient implementations have been derived from these algorithms. Finally, note that obtaining algorithms for the computation of the global supremum of a polynomial without reducing this problem to a quantifier elimination one was an open problem in the scope of computer algebra.

Main results. The main result of this paper is an efficient algorithm computing the global supremum of a polynomial without reduction to quantifier elimination.

It is well known that computing $\sup_{x\in B} f(x)$ where B is compact can be tackled by computing the critical values of the mapping $x \to f(x)$ and studying the values taken by f over the boundary of B. These techniques are not sufficient to compute $\sup_{x\in\mathbb{R}^n} f(x)$. Indeed, consider the polynomial $f = X^2 + (XY-1)^2$. It is always positive and considering its values at the sequence of points $(\frac{1}{\ell}, \ell)$, it is easy to see that $\sup_{x\in\mathbb{R}^n}(-f(x)) = 0$, while $\{x \in \mathbb{R}^n \mid f(x) = 0\}$ is obviously empty. The phenomenon which occurs here is that the polynomial f tends to a supremum "at infinity", i.e. each sequence of points $(x_\ell)_{\ell\in\mathbb{N}} \subset \mathbb{R}^n$ such that $f(x_\ell) \to 0$ when ℓ tends to ∞ is such that $||x_\ell||$ tends to ∞ when ℓ tends to ∞. On the other hand, it is well known that if, for such a sequence of points, $||\mathbf{grad}_{x_\ell} f||$ does not tend to 0 when ℓ tends to ∞, $f(x_\ell)$ can't have a finite limit. This leads to consider the notion of *generalized critical values* of a polynomial mapping $x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$ introduced in [23]. The set of generalized critical values is defined as the set of complex numbers c such that there exists a sequence of points $(x_\ell)_{\ell\in\mathbb{N}} \subset \mathbb{C}^n$ satisfying $f(x_\ell) \to c$ and for all $(i,j) \in \{1,\ldots,n\}^2$, $\left(X_i \frac{\partial f}{\partial X_j}\right)(x_\ell) \to 0$ when ℓ tends to ∞.

The first result (see Theorem 5 below) relates $\sup_{x\in\mathbb{R}^n} f(x)$ to the set of asymptotic critical values of the mapping $x \in \mathbb{R}^n \to f(x)$. More precisely, the statement of Theorem 5 is: *Let $f \in \mathbb{Q}[X_1,\ldots,X_n]$ and $\mathcal{E} = \{e_1,\ldots,e_\ell\}$ (with $e_1 < \ldots < e_\ell$) be the set of real generalized critical values of the mapping $x \in \mathbb{R}^n \to f(x)$. Then $\sup_{x\in\mathbb{R}^n} f(x) < \infty$ if and only if there exists $1 \le i_0 \le \ell$ such that $\sup_{x\in\mathbb{R}^n} f(x) = e_{i_0}$.*

It remains to show how to determine if the supremum of f over $\mathbb{R}^n$ is finite and, in this case, which of the generalized critical values is $\sup_{x\in\mathbb{R}^n} f(x)$. This is the aim of Theorem 6 whose statement is: *Let $\mathcal{E} = \{e_1,\ldots,e_\ell\}$ be the set of real generalized critical values of the mapping $x \in \mathbb{R}^n \to f(x)$ such that $e_1 < \ldots < e_\ell$. Consider $\{r_0,\ldots,r_\ell\}$ a set of rationals such that $r_0 < e_1 < r_1 < \ldots < e_\ell < r_\ell$. The supremum of f over $\mathbb{R}^n$ is finite if and only if there exists $i_0 \in \{1,\ldots,\ell\}$ such that $\{x \in \mathbb{R}^n \mid f(x) = r_{i_0-1}\} \neq \emptyset$ and $\forall j \ge i_0$ $\{x \in \mathbb{R}^n \mid f(x) = r_j\} = \emptyset$ if and only if $\sup_{x\in\mathbb{R}^n} f(x) = e_{i_0}$ (in this case $\sup_{x\in\mathbb{R}^n} f(x) = e_{i_0}$).*

Hence, the algorithm we obtain consists first in computing the set of generalized critical values of the mapping $x \in \mathbb{R}^n \to f(x)$. Then, it tests the emptiness of the real counterpart of smooth hypersurfaces defined by $f - r_j = 0$. This allows us to compute $\sup_{x\in\mathbb{R}^n} f(x)$ without any reduction to a quantifier elimination problem. The computations are based on algebraic elimination and finding the real solutions of zero-dimensional polynomial systems. Our implementation uses Gröbner bases. At the end of the paper, we present some experiments showing the efficiency of this strategy compared to the ones reducing global optimization problems to a quantifier elimination one.

The complexity of the algorithm of [7, Chapter 14] reducing global optimization problems to quantifier elimination is $D^{\mathcal{O}(n)}$. It is thus important to ensure that the algorithm which is designed here is in the same complexity class.

We make the distinction between algorithms whose probability of success depends on the entries (this is the case of some numerical algorithms running with fixed precision), algorithms whose probability of success depend on random choices done during the computation, and certified algorithms (the result is always correct but the complexity of such algorithms can depend on random choices done during the computation).

Substituting the computations of Gröbner bases by the geometric resolution algorithm designed in [30], one gets a probabilistic algorithm whose complexity is $\mathcal{O}(n^7 D^{4n})$ arithmetic operations in $\mathbb{Q}$. As far as we know, such a complexity bound had never been obtained previously.

The running of our algorithms depend on some random choices of matrices and points which are valid outside a proper Zariski-closed subset. This is a first obstacle to get a complexity result in a deterministic framework. An other problem comes from the computation of critical values of a polynomial using Gröbner bases. We show how to compute the critical values using Gröbner bases with a complexity bounded by $D^{\mathcal{O}(n)}$. The deformation technique we use is interesting in itself. Indeed, by generalizing the strategy developed in [39] (which had lead to practical improvements), it can be used to real solve general singular polynomial systems. Finally, we prove that, under the assumption that the first random choices are valid, the complexity of this algorithm is $D^{\mathcal{O}(n)}$.

Related works. In the scope of numerical techniques, looking for the global supremum of a polynomial is tackled by looking for the smallest $\varepsilon > 0$ such that $\varepsilon - f > 0$. In general, the strategy consists in rewriting $\varepsilon - f$ as a sum of squares via LMI relaxations (see the works of Parillo-Sturmfels [32, 33] and the works of Lasserre [26] for methods based on moment theory), while it is well-known that a polynomial can be positive without being a sum of squares. More recently, Nie, Demmel and Sturmfels [31] proposed a method based on computations over the ideal generated by the partial derivatives of the studied polynomial (when this ideal is zero-dimensional and radical). In particular, this technique seems to be more numerically stable than the previous ones. Lasserre developed an other approach for computing the real radical of zero-dimensional systems [27]. In any case, computing over the gradient ideal does not allow us to obtain the supremum of the considered polynomial. In [45], Schweighofer introduces the use of asymptotic critical values to obtain a numerical procedure computing the global supremum (or infimum) of a polynomial. Nevertheless, the conditioning and the numerical stability of this method is not studied.

The notion of generalized critical values we use in this paper was introduced in [23]. A first algorithm computing them is given. Efficient algorithms are given in [42, 40]. This computation is used in algorithms solving polynomial systems

of inequalities in the RAGLIB maple package [41].
An other ingredient of this paper is the emptiness test of the real counterpart of a smooth hypersurface. Single exponential algorithms in the number of variables are given in [18, 19, 20, 35]. They are based on computations of critical points and have not lead to efficient implementations. Algorithms given in [43, 44] and some of their variants are implemented in RAGLIB [41]. A particular study leading to efficient algorithms dealing with the case of singular hypersurfaces is done in [39]. Algorithms relying on the critical point method and using evaluation and lifting techniques to encode polar varieties are given in [3, 2, 5, 4].

Conclusions and perspectives. We provide the first certified algorithm based on computer algebra techniques computing the supremum of polynomials over the reals without using quantifier elimination. This leads to an efficient implementation which allows us to deal with problems which are intractable by previous methods. The complexity of the method is singly exponential in the number of variables. We plan to extend these results in two ways. The first question which arises is to decide if the computed global supremum is reached and provide at least one point at which it is reached if it is. The second one is: given a singular point of a polynomial, decide if it is a local optimum. Finally, solving global optimization problems under some constraints is an area where the techniques we develop here can be used.

Plan of the paper. Section 2 provides the definition, useful properties and an algorithm for the computation of the set of generalized critical values of a polynomial mapping. In Section 3, we recall the basics of an efficient algorithm computing sampling points in the real counterpart of a smooth hypersurface which is used to test the emptiness of the considered real hypersurfaces. Then, in Section 4, we give the algorithm computing $\sup_{x\in\mathbb{R}^n} f(x)$ and its proof. Section 5 is devoted to complexity results. Section 6 presents some practical results we obtained with the algorithm designed here.

2. PROPERTIES AND COMPUTATION OF GENERALIZED CRITICAL VALUES

In this section, we recall the definitions and basic properties of generalized critical values which can be found in [23].

DEFINITION 1. *[23] A complex number $c \in \mathbb{C}$ is a* critical value *of the mapping $\widetilde{f} : y \in \mathbb{C}^n \to f(y)$ 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 $\widetilde{f} : y \in \mathbb{C}^n \to f(y)$ if and only if there exists a sequence of points $(z_\ell)_{\ell\in\mathbb{N}} \subset \mathbb{C}^n$ such that:*
a) $f(z_\ell)$ tends to c when ℓ tends to ∞.
b) $||z_\ell||$ tends to $+\infty$ when ℓ tends to ∞.
c) for all $(i,j) \in \{1,\dots,n\}^2$ $||X_i(z_\ell)||.||\frac{\partial f}{\partial X_j}(z_\ell)||$ tends to 0 when ℓ tends to ∞. The set of generalized critical values *is the union of the sets of critical values and asymptotic critical values of $\widetilde{f}$.*

In the sequel, we denote by $K_0(f)$ the set of critical values of $\widetilde{f}$, by $K_\infty(f)$ the set of asymptotic critical values of $\widetilde{f}$, and by $K(f)$ the set of generalized critical values of $\widetilde{f}$ (i.e. $K(f) = K_0(f) \cup K_\infty(f)$). In [23], the authors prove the following result which can be seen as a generalized Sard's theorem for generalized critical values. Bounds on the number of generalized critical values can be found also in [22].

THEOREM 1. *Let f be a polynomial in $\mathbb{Q}[X_1,\dots,X_n]$ 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 two topological spaces V and W, a polynomial mapping $F : V \to W$, and a subset $\mathcal{W}$ of W, we say that F realizes a locally trivial fibration on $V \setminus F^{-1}(\mathcal{W})$ if for all connected open set $U \subset W \setminus \mathcal{W}$, for all $e \in U$, denoting by π the projection on the second member of the cartesian product $F^{-1}(e) \times U$, there exists a diffeomorphism φ such that the following diagram

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

is commutative. The main interest of the set of *generalized critical values* relies on its topological properties which are summarized below and proved in [23].

THEOREM 2. *[23] The mapping $f_{\mathbb{C}} : x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$ realizes a locally trivial fibration in $\mathbb{C}^n \setminus f_{\mathbb{C}}^{-1}(K(f_{\mathbb{C}}))$.*
The mapping $f_{\mathbb{R}} : x \in \mathbb{R}^n \to f(x) \in \mathbb{R}$ realizes a locally trivial fibration in $\mathbb{R}^n \setminus f_{\mathbb{R}}^{-1}(K(f_{\mathbb{R}}))$.

The set of critical values of f can be computed by the routine CRITICALVALUES given below. It takes as input $f \in \mathbb{Q}[X_1,\dots,X_n]$ and returns a univariate polynomial whose set of roots is the set of critical values of $\widetilde{f}$.

CRITICALVALUES
Input: a polynomial $f \in \mathbb{Q}[X_1,\dots,X_n]$. Output: a univariate polynomial whose set of roots is the set of critical values of the mapping $x \to f(x)$.
• Compute a Gröbner basis for a monomial ordering eliminating $[X_1,\dots,X_n]$ of the ideal generated by $f - T, \frac{\partial f}{\partial X_1},\dots,\frac{\partial f}{\partial X_n}$ (where T is a new variable). • Let G be the Gröbner basis previously computed, return the element of G lying in $\mathbb{Q}[T]$.

We show now how to compute the set of asymptotic critical values of $\widetilde{f}$. 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 $\phi^{-1}(\overline{B})$ is compact (where $\overline{B}$ denotes the closure of B). The map ϕ is said to be proper if it is proper at all $w \in W$.

Notation 1. In order to describe the routine computing the set of asymptotic critical values of $\widetilde{f}$ we introduce the following notations:

- Let $\mathbf{A} \in GL_n(\mathbb{Q})$ and $g \in \mathbb{Q}[X_1,\dots,X_n]$. We denote by $g^{\mathbf{A}}$ the polynomial $g(\mathbf{A}.\mathbf{X})$ where $\mathbf{X} = [X_1,\dots,X_n]$
- DIMENSION is a procedure taking as input a finite set of polynomials in $\mathbb{Q}[X_1,\dots,X_n]$ and return the dimension of the ideal they generate.

- Consider an ideal, encoded by a Gröbner basis G, defining a curve C in $\mathbb{C}^n$ and a projection $\pi : C \to E \subset \mathbb{C}^n$ where E is a 1-dimensional affine space.

  We denote by SETOFNONPROPERNESS(G, π) a polynomial whose set of roots is the set of non-properness of π; SETOFNONPROPERNESS denoting a procedure computing it. Such a routine is given in [44, 28].

THEOREM 3. *[42, 40] Suppose that for all $1 \leq i \leq n$, $\deg(f, X_i) \geq 1$. If the determinant of the hessian matrix associated to f is identically null, the set of asymptotic critical values of the mapping $x \to f(x)$ is empty. Else, 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 Zariski-closure of the constructible set defined by*

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

has dimension 1.

The routine given below and denoted by ASYMPTOTICCRITICALVALUES is given in [40]. It improves the one of [42]. It computes a finite set of points containing the set of generalized critical values of $\widetilde{f}$. The input is a polynomial f and the output is a univariate polynomial whose set of roots contain the set of asymptotic critical values of $\widetilde{f}$.

ASYMPTOTICCRITICALVALUES

Input: a polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ such that $\deg(f, X_i) \geq 1$ for $i = 1, \ldots, n$.
Output: a univariate polynomial non identically null whose set of roots contains the set of asymptotic critical values of $x \to f(x)$.

- If the determinant of the Hessian matrix of f is 0 return 1.
- Choose $\mathbf{A} \in GL_n(\mathbb{Q})$ and compute a Gröbner basis $G^{\mathbf{A}}$ of $I^{\mathbf{A}} = \langle f^{\mathbf{A}} - T, \frac{\partial f^{\mathbf{A}}}{\partial X_1}, \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}}, L\frac{\partial f^{\mathbf{A}}}{\partial X_n} - 1\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]$
- While DIMENSION$(I^{\mathbf{A}}) \neq 1$ do
  - Choose an other matrix $\mathbf{A} \in GL_n(\mathbb{Q})$
- Return SETOFNONPROPERNESS$(G^{\mathbf{A}}, \pi)$ where π is the projection $(x_1, \ldots, x_n, t) \to t$.

REMARK 1. *Note that if there exists $1 \leq i \leq n$, the asymptotic critical values of f can still be computed by considering f in $\mathbb{Q}[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$. Note also that the curve defined as the Zariski-closure of the complex-solution set of $f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}} = 0, \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0$ has a degree bounded by $(D-1)^{n-1}$. Thus, the set of non-properness of the projection on T restricted to this curve has a degree bounded by $(D-1)^{n-1}$.*

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. DECIDING THE EMPTINESS OF THE REAL COUNTERPART OF A SMOOTH HYPERSURFACE

We study now how to decide the emptiness of the real counterpart of a *smooth* hypersurface $\mathcal{H}$ defined by $f = 0$ (where $f \in \mathbb{Q}[X_1, \ldots, X_n]$), i.e. $\{x \in \mathcal{H} \mid \frac{\partial f}{\partial X_1}(x) = \cdots = \frac{\partial f}{\partial X_n}(x) = 0\}$ is empty. The routine we present is based on [43] since it is, in practice, the most efficient. From the complexity viewpoint, it also provides slightly better complexity bounds than the ones obtained in [3, 2, 5, 4] in a probabilistic model. Denote by π_i the canonical projection $(x_1, \ldots, x_n) \to (x_1, \ldots, x_i)$, by $\mathbf{p}_n = (p_1, \ldots, p_n)$ an arbitrarily chosen point in $\mathbb{Q}^n$ and by $\mathbf{p}_i$ the point $(p_1, \ldots, p_i) \in \mathbb{Q}^i$. The geometric scheme of resolution is based on the following results. Up to a generic linear change of variables,
- the set of critical points of the restriction of π_1 to $\mathcal{H}$ is either zero-dimensional or empty;
- $\dim\left(\mathcal{H} \cap \pi_1^{-1}(\mathbf{p}_1)\right) = \dim(\mathcal{H}) - 1$;
- each connected component C of $\mathcal{H} \cap \mathbb{R}^n$ has a closed image by π_1. Hence, either $\pi_1(C) = \mathbb{R}$ which implies that $C \cap \left(\mathcal{H} \cap \pi_1^{-1}(\mathbf{p}_1)\right) \neq \emptyset$ or C contains a critical point of the restriction of π_1 to $\mathcal{H}$. Computing at least one point in each connected component is then reduced to computing the critical points of the restriction of π_1 to $\mathcal{H}$ and performing a recursion on $\mathcal{H} \cap \pi_1^{-1}(\mathbf{p}_1)$ (whose dimension is less than the one of $\mathcal{H}$). More precisely, the following result is proved in [43]. We use in the following the notations introduced in the previous section. Additionally, given an algebraic variety $V \subset \mathbb{C}^n$ and a polynomial mapping $\varphi : \mathbb{C}^n \to \mathbb{C}^k$ (for some $k \in \{1, \ldots, n\}$), $\mathfrak{C}(\varphi, V)$ denotes the critical locus of φ restricted to V.

THEOREM 4. *[43] Let $\mathcal{H} \subset \mathbb{C}^n$ be a smooth hypersurface defined by $f = 0$ (with $f \in \mathbb{Q}[X_1, \ldots, X_n]$). There exists a proper Zariski-closed subset $\mathcal{A} \subset GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, the set of points*

$$\mathfrak{C}\left(\pi_1, \mathcal{H}^{\mathbf{A}}\right) \cup \left(\mathcal{H}^{\mathbf{A}} \cap \pi_{n-1}(\mathbf{p}_{n-1})\right) \bigcup_{i=2}^{n} \mathfrak{C}\left(\pi_i, \mathcal{H}^{\mathbf{A}} \cap \pi_{i-1}^{-1}(\mathbf{p}_i)\right)$$

has at most dimension 0 and a non-empty intersection with each connected component with $\mathcal{H}^{\mathbf{A}} \cap \mathbb{R}^n$.

REMARK 2. *In [43], the authors prove that $\mathbf{A}$ must be chosen such that the projection π_i restricted to $\mathfrak{C}\left(\pi_{i+1}, \mathcal{H}^{\mathbf{A}}\right)$ is proper. An algorithm performing this test is given in [44] (see also [28]).*

The algorithm below is called ISEMPTY. It takes as input a square-free polynomial f whose complex set of solutions is a smooth hypersurface. It returns `false` if $f = 0$ has real solutions, else it returns `true`. This algorithm requires a routine ZERODIMSOLVE taking as input a polynomial system of equations defining a zero-dimensional variety and returning its real points (encoded by numerical approximations).

ISEMPTY

Input: a polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ defining a smooth hypersurface $\mathcal{H} \subset \mathbb{C}^n$
Output: a boolean which equals `true` if and only if $\mathcal{H} \cap \mathbb{R}^n$ is empty.

- Choose randomly $\mathbf{A} \in GL_n(\mathbb{Q})$, and $\mathbf{p} \in \mathbb{Q}^n$.
- If ZERODIMSOLVE$(f^{\mathbf{A}}, \frac{\partial f^{\mathbf{A}}}{\partial X_2}, \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_n}) \neq \emptyset$ return `false`
- For $i \in \{1, \ldots, n-2\}$ if ZERODIMSOLVE$(X_1 - p_1, \ldots, X_i - p_i, f^{\mathbf{A}}, \frac{\partial f^{\mathbf{A}}}{\partial X_{i+2}}, \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_n}) \neq \emptyset$ return `false`
- If ZERODIMSOLVE$(f^{\mathbf{A}}, X_1 - p_1, \ldots, X_{n-1} - \mathbf{p}_{n-1}) \neq$ return `false` else return `true`.

4. THE ALGORITHM

The algorithm computing the supremum of a polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ is based on computations of generalized critical values and computations testing the emptiness of the real counterpart of smooth hypersurfaces.

The result below shows that if a polynomial f has a finite optimum, this optimum is either a critical value or an asymptotic critical value of f.

THEOREM 5. *Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ and $\mathcal{E} = \{e_1, \ldots, e_\ell\}$ (with $e_1 < \ldots < e_\ell$) be the set of real generalized critical values of the mapping $x \in \mathbb{R}^n \to f(x)$. Then $\sup_{x\in\mathbb{R}^n} f(x) < \infty$ if and only if there exists $1 \leq i_0 \leq \ell$ such that $\sup_{x\in\mathbb{R}^n} f(x) = e_{i_0}$.*

PROOF. Suppose that the supremum of f is finite and let $e = \sup_{x\in\mathbb{R}^n} f(x)$. This is equivalent to the following assertion: there exists $\alpha > 0$ small enough such that for all $\varepsilon \in]e, e+\alpha[$, the real counterpart of $f^{-1}(\varepsilon)$ is empty and for all $\varepsilon \in]e-\alpha, e[$ the real counterpart of $f^{-1}(\varepsilon)$ is not empty. Denote by I the interval $]e-\alpha, e+\alpha[$.

Suppose now that e is not a generalized critical value of f. Then, from Theorem 2, f realizes a locally trivial fibration over $f^{-1}(]e-\alpha, e+\alpha[)$. Hence, for all $\varepsilon \in I$, there exists a diffeomorphism φ such that the following diagram

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

commutes. Consider $\varepsilon \in]e-\alpha, e[$, $\varepsilon' \in]e, e+\alpha[$ (then $f^{-1}(\varepsilon') \cap \mathbb{R}^n = \emptyset$) and $x \in f^{-1}(\varepsilon) \cap \mathbb{R}^n$. From the above diagram, $f(\varphi(x, \varepsilon')) = \varepsilon'$ implies that $\varphi(x, \varepsilon') \in f^{-1}(\varepsilon') \cap \mathbb{R}^n$. This is a contradiction. $\square$

From Theorem 5, if the supremum of a polynomial mapping is finite, it is a generalized critical value. Determining which of these values the supremum is, can be tackled by solving the following quantifier elimination problem: $\exists e \in \mathcal{E}\, \forall \varepsilon > 0, \exists x \in \mathbb{R}^n f(x) \geq e - \varepsilon$ and $\not\exists x \in \mathbb{R}^n f(x) > e$ where $\mathcal{E}$ is the set of generalized critical values of the mapping $x \in \mathbb{R}^n \to f(x)$. The following result shows how to determine if a generalized critical value given by an isolating interval is an optimum of the polynomial f without performing a quantifier elimination.

THEOREM 6. *Let $\mathcal{E} = \{e_1, \ldots, e_\ell\}$ be the set of real generalized critical values of the mapping $x \in \mathbb{R}^n \to f(x)$ such that $e_1 < \ldots < e_\ell$. Consider $\{r_0, \ldots, r_\ell\}$ a set of rationals such that $r_0 < e_1 < r_1 < \ldots < e_\ell < r_\ell$.*
The supremum of f over $\mathbb{R}^n$ is finite if and only if there exists $i_0 \in \{1, \ldots, \ell\}$ such that $\{x \in \mathbb{R}^n \mid f(x) = r_{i_0-1}\} \neq \emptyset$ and $\forall j \geq i_0$ $\{x \in \mathbb{R}^n \mid f(x) = r_j\} = \emptyset$ if and only if $\sup_{x\in\mathbb{R}^n} f(x) = e_{i_0}$ (in this case $\sup_{x\in\mathbb{R}^n} f(x) = e_{i_0}$).

PROOF. Suppose the supremum of f over $\mathbb{R}^n$ to be finite. From Theorem 5, there exists a generalized critical value e_{i_0} of f such that $\sup_{x\in\mathbb{R}^n} = e_{i_0}$. Equivalently, we have that for all $e > e_{i_0}$, $f^{-1}(x) \cap \mathbb{R}^n$ is empty and there exists $\alpha > 0$ small enough such that for all $\varepsilon \in]e_{i_0} - \alpha, e_{i_0}[$ $f^{-1}(\varepsilon) \cap \mathbb{R}^n$ is not empty.

By convention, if $i_0 = 1$, $e_{i_0-1} = -\infty$. Denote by I the interval $]e_{i_0-1}, e_{i_0}[$. Now, it remains to prove that for all $\varepsilon \in I$, $f^{-1}(\varepsilon) \cap \mathbb{R}^n$ is not empty. From Theorem 2, given $\varepsilon \in]e_{i_0} - \alpha, e_{i_0}[$, there exists a diffeomorphism φ such that the following diagram

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

commutes. Supposing now that there exists $\varepsilon' \in I$ such that $f^{-1}(\varepsilon') \cap \mathbb{R}^n$ is empty and consider $x \in f^{-1}(\varepsilon)$. Since $f(\varphi(x, \varepsilon')) = \varepsilon'$, implies $\varphi(x, \varepsilon') \in f^{-1}(\varepsilon') \cap \mathbb{R}^n$, this yields a contradiction. $\square$

Finally, computing the supremum of a polynomial is reduced to test the emptiness of the real counterpart of smooth hypersurfaces. This problem can be tackled using the routine ISEMPTY described in Section 3.

Denoting by FINDRATIONALS a routine taking as input a univariate polynomial with coefficients in $\mathbb{Q}$ whose real roots are denoted by $e_1 < \ldots < e_\ell$ and returning a list of rational numbers $r_0 < \ldots < r_\ell$ such that $r_0 < e_1 < r_1 < e_2 < \ldots < e_\ell < r_\ell$, we obtain the following algorithm.

OPTIMIZE

Input: a polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$

Output: if $\sup_{x\in\mathbb{R}^n} f(x)$ is infinite, it returns ∞ else it returns an interval isolating $\sup_{x\in\mathbb{R}^n} f(x)$ and a polynomial whose set of roots contains $\sup_{x\in\mathbb{R}^n} f(x)$.

- $P \leftarrow$ASYMPTOTICCRITICALVALUES(f)
- $Q \leftarrow$CRITICALVALUES(f)
- $L \leftarrow$FINDRATIONALS(PQ), $N \leftarrow \sharp L$, $i \leftarrow N$
- while $i > 0$ and ISEMPTY(f-L[i]) do $i \leftarrow i - 1$
- if $i = 0$ return ∞ else return an interval isolating the i-th root of PQ and the polynomial PQ.

5. COMPLEXITY RESULTS

Complexity estimates using the geometric resolution algorithm. One can substitute Gröbner bases computations in the routines CRITICALVALUES, ASYMPTOTICCRITICALVALUES and ISEMPTY by the geometric resolution algorithm [17, 30]. This algorithm is probabilistic. It is based on evaluation and lifting techniques taking advantage of the encoding of polynomials by straight-line programs. These techniques are introduced in [16, 14, 15]. This leads to complexity estimates for solving zero-dimensional polynomial systems which are polynomial in the complexity of evaluation of the input system, the number of variables and an intrinsic geometric degree bounded by D^n (where D bounds the degree of the polynomials given as input).

In [42, 40], we describe algorithms computing critical values and asymptotic critical values using the geometric resolution algorithm given in [30] having a complexity bounded by $\mathcal{O}(n^7 D^{4n})$ arithmetic operations in $\mathbb{Q}$. The algorithm of [43] has a complexity bounded by $\mathcal{O}(n^7 D^{3n})$. Since the number of generalized critical values is bounded by $\mathcal{O}(D^n)$, there are, in the worst case, at most $\mathcal{O}(D^n)$ hypersurfaces for which one has to test the emptiness of their real counterpart (see Remark 1). This leads to the following result.

THEOREM 7. *There exists a probabilistic algorithm computing the global supremum of a polynomial $f \in \mathbb{Q}[X_1, \ldots,$*

$X_n]$ *of degree* D *with a complexity within* $\mathcal{O}(n^7 D^{4n})$ *arithmetic operations in* $\mathbb{Q}$.

The rest of this section is devoted to prove that there exists a certified algorithm computing the global supremum of f, without reduction to quantifier elimination, with a complexity within $D^{\mathcal{O}(n)}$ arithmetic operations in $\mathbb{Q}$ if some random choices done internally are generic enough. Note that proving this is equivalent to prove the same result for the computation of asymptotic critical values of f, which is the aim of the next paragraph. Indeed, the computation of real critical values of f can be done by computing the values taken by f at sampling points of the real counterpart of the algebraic variety defined by $\frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0$ with a complexity within $D^{\mathcal{O}(n)}$ arithmetic operations in $\mathbb{Q}$ using [7, Chapter 13]. The same algorithm can be used to test the emptiness of the real counterpart of smooth hypersurfaces. We give below an other way to get a complexity bounded by $D^{\mathcal{O}(n)}$ arithmetic operations in $\mathbb{Q}$ to compute the critical values of f. The method we use is of interest for itself since it generalizes [39] to the case of singular polynomial systems and can lead to efficient implementations.

Computation of asymptotic critical values. Suppose the determinant of the hessian matrix of f to be not identically null (the cost of this computation is dominated by $D^{\mathcal{O}(n)}$. From [40], there exists $\mathcal{A} \subset GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ the ideal $I^{\mathbf{A}} = J^{\mathbf{A}} \cap \mathbb{Q}[X_1, \ldots, X_n, T]$ where $J^{\mathbf{A}} = \langle f^{\mathbf{A}} - T, \frac{\partial f^{\mathbf{A}}}{\partial X_1}, \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}}, L\frac{\partial f^{\mathbf{A}}}{\partial X_n} - 1\rangle$ is radical and has dimension 1. The degree of this ideal is bounded by $(D-1)^{n-1}$ (see also [40] for more accurate bounds on the degree of this curve depending on intrinsic quantities). Moreover, there exists a proper Zariski-closed subset $\mathcal{Z} \subset \mathbb{C}$ such that for all $\theta \in \mathbb{Q} \setminus \mathcal{Z}$, the ideal $I^{\mathbf{A}} + \langle T - \theta\rangle$ has dimension at most 0. Choosing $(D-1)^{n-1} + 1$ such points x and computing a rational parametrization with respect to a separating element u of these ideals has a cost which is dominated by $D^{\mathcal{O}(n)}$. If $\mathbf{A}$ is well-chosen there exists at least one θ such that $I^{\mathbf{A}} + \langle T - \theta\rangle$ is radical which can be decided looking at the rational parametrization of its set of solutions (see [37]). If the separating element is generic enough, it is a separating element for all valid choices of θ. Once these rational parametrizations are computed, using interpolation, one obtains a rational parametrisation encoding the curve defined by $I^{\mathbf{A}}$. If the first choices of matrix $\mathbf{A}$, the rationals θ and u are correct, the cost of the whole computation is dominated by $D^{\mathcal{O}(n)}$ arithmetic operations in $\mathbb{Q}$. Following [42, Section 4], one can retrieve the set of non-properness of the projection $(x_1, \ldots, x_n, t) \to t$ restricted to $\mathfrak{C}^{\mathbf{A}}$ from such a rational parametrization, with a complexity bounded by $D^{\mathcal{O}(n)}$ arithmetic operations in $\mathbb{Q}$.

THEOREM 8. *If the first choices of* $\mathbf{A}$, θ *and* u *are correct, the procedure described above has a complexity within* $D^{\mathcal{O}(n)}$ *arithmetic operations in* $\mathbb{Q}$ *and returns the set of asymptotic critical values of the mapping* $x \to f(x)$.

Computation of critical values. If the singular locus of f is zero-dimension, [24, 25] and FGLM algorithm allow us to compute the critical values of f with a complexity within $D^{\mathcal{O}(n)}$ arithmetic operations in $\mathbb{Q}$. We show now how to modify CRITICALVALUES to obtain a complexity result without assumption on the dimension of the singular locus of f. To this end, we use deformation techniques. The method is interesting in itself. It generalizes to the case of singular polynomial systems the approach developed in [39]. This had lead to significative practical improvement for finding the real solutions of singular hypersurfaces. The complexity of the method we present here is $D^{\mathcal{O}(n)}$.

Given $(q, i_0) \in \mathbb{N}\times\mathbb{Z}$, an infinitesimal ε, and a Puiseux series field $a = \sum_{i \geq i_0} a_i \varepsilon^{i/q}$ (with $a_{i_0} \neq 0$) in $\mathbb{C}\langle\varepsilon\rangle$, $\lim_0(a)$ exists if $i_0 \geq 0$ and equals a_0. Given $x = (x_1, \ldots, x_n) \in \mathbb{C}\langle\varepsilon\rangle$, if for all i, $\lim_0(x_i)$ exists, x is said to have a bounded limit $\lim_0(x) = (\lim_0(x_1), \ldots, \lim_0(x_n))$, else x is said to have a non-bounded limit. If V is a subset of $\mathbb{C}\langle\varepsilon\rangle^n$ (or $\mathbb{R}\langle\varepsilon\rangle^n$), $\lim_0(V)$ denotes the set of bounded limits of the points in V. We consider in the sequel algebraic varieties defined in $\mathbb{C}\langle\varepsilon\rangle^n$. Given $\mathcal{I} = \{i_1, \ldots, i_\ell\} \subset \{1, \ldots, n\}$ and $\sigma \in \{-1, 1\}^n$, denote by $V^{\mathbf{a},\sigma}_{\varepsilon,\mathcal{I}}$ the algebraic variety defined by the system $S^{\mathbf{a},\sigma}_{\varepsilon,\mathcal{I}}$ $\frac{\partial f}{\partial X_{i_1}} - \sigma_{i_1} a_{i_1}\varepsilon = \cdots = \frac{\partial f}{\partial X_{i_\ell}} - \sigma_{i_\ell} a_{i_\ell}\varepsilon = 0$ (where ε is an infinitesimal). Given a point $A \in \mathbb{Q}^n$, denote by $\mathfrak{W}^{A,\mathbf{a},\sigma}_{\varepsilon,\mathcal{I}}$ the set of critical points of the square of the euclidean distance function from A restricted to $V^{\mathbf{a},\sigma}_{\varepsilon,\mathcal{I}}$. If $y \in \mathbb{R}^n$ and $E \subset \mathbb{R}^n$, $\mathrm{dist}(y, E)$ denotes the minimum distance from y to E. Finally, denote by $S \subset \mathbb{C}^n$ the algebraic variety defined by $\frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0$.

LEMMA 1. *There exists a Zariski-closed subset* $\mathcal{A} \subsetneq \mathbb{C}^n$ *such that for all* $\mathbf{a} \in \mathbb{Q}^n \setminus \mathcal{A}$, $S^{\mathbf{a},\sigma}_{\varepsilon,\mathcal{I}}$ *generates a radical ideal and* $V^{\mathbf{a},\sigma}_{\varepsilon,\mathcal{I}}$ *is smooth of dimension* $n - \sharp\mathcal{I}$ *if it is not empty. Given such a* $\mathbf{a}$, *there exists a Zariski-closed subset* $\mathcal{A}_{\mathbf{a}} \subsetneq \mathbb{C}^n$ *such that for all* $A \in \mathbb{Q}^n \setminus \mathcal{A}_{\mathbf{a}}$, $\mathfrak{W}^{A,\mathbf{a},\sigma}_{\varepsilon,\mathcal{I}}$ *is zero-dimensional or empty.*

PROOF. This is a consequence of the algebraic Sard's theorem applied to the mapping $x \in \mathbb{C}^n \to (f_{i_1}(x), \ldots, f_{i_\ell}(x))$ and of [1, Theorem 2.3] (see also [4]) applied to the system $f_{i_1} - \sigma_{i_1} a_{i_1}\varepsilon = \cdots = f_{i_\ell} - \sigma_{i_\ell} a_{i_\ell}\varepsilon = 0$. □

THEOREM 9. *Given* $A = (a_1, \ldots, a_n) \in \mathbb{Q}^n$ *and* C, *a connected component of* $S \cap \mathbb{R}^n$, *there exists* $\mathcal{I} \subset \{1, \ldots, n\}$ *such that* $\left(\lim_0(\mathfrak{W}^{A,\mathbf{a},\sigma}_{\varepsilon,\mathcal{I}}) \cap S\right) \cap C \neq \emptyset$.

PROOF. Consider a point of C which is at minimal distance to A and suppose, without loss of generality, that in any neighbourhood of x, there exists a point at which all the partial derivatives of f are positive. Consider the maximal subset $\mathcal{I} \subset \{1, \ldots, n\}$ (for the order inclusion) such that in each neighbourhood of x there exists x'_ε such that $f_i(x') - a_i\varepsilon = 0$ for all $i \in \mathcal{I}$. Remark that $\lim_0 x'_\varepsilon$ exists and equals x. We follow now *mutatis mutandis* the proof of [38, Lemma 3.7], to obtain the result.

Consider the set $\mathcal{M}$ of points of C at minimal distance from A. Let $r > 0$ be small enough so that the closed and bounded semi-algebraic set $T = \{x \in \mathbb{R}^n \mid \exists y \in \mathcal{M}\ \mathrm{dist}(y, \mathcal{M} \leq r\}$ does not intersect $S \setminus C$. According to the above $\lim_0(x_\varepsilon) \in \mathcal{M}$. Denoting $T' = \{x \in \mathbb{R}^n \mid \exists y \in \mathcal{M}\ \mathrm{dist}(y, \mathcal{M} = r\}$, remark that the points of $\lim_0(\mathfrak{W}^{A,\mathbf{a},\sigma}_{\varepsilon,\mathcal{I}}) \cap S \cap T'$ are infinitesimally close of points of $S \cap T'$ which are not at minimal distance from A. So the minimal distance from A to $\mathfrak{W}^{A,\mathbf{a},\sigma}_{\varepsilon,\mathcal{I}} \cap T$ is not obtained on T'. Thus, this minimal distance is obtained at a point which is a critical point of the square of the distance function to A on V and it is clear that the limits of these points lie in $\mathcal{M}$. □

In order to compute rational parametrizations $\mathfrak{W}^{A,\mathbf{a},\sigma}_{\varepsilon,\mathcal{I}}$, we follow a similar strategy than the one designed in the above paragraph, by specializing ε in rational values, using interpolation to obtain rational parametrizations with coefficients in $\mathbb{Q}(\varepsilon)$ and [38] to compute $\lim_0(x)$ for each point x encoded by these rational parametrizations. We obtain a complexity within $D^{\mathcal{O}(n)}$ arithmetic operations in $\mathbb{Q}$. Finally, note that the number of $\mathcal{I}$ to consider is bounded by $D^{\mathcal{O}(n)}$.

THEOREM 10. *If the first choices of* $\mathbf{a}$, $\mathbf{A}$, *specialisation values of* ε *and a separating element are generic enough, one can compute at least one point in each connected component of* $S \cap \mathbb{R}^n$ *within a complexity bounded by* $D^{\mathcal{O}(n)}$.

6. IMPLEMENTATION AND PRACTICAL EXPERIMENTS

The algorithm we implemented uses the routines described in Sections 2, 3 since, up to the experiments we did, they are more efficient than the ones described in Section 5 to obtain complexity results. The implementation is done in Maple. Our implementation uses internal functions of the RAGLIB Maple package [41]. They are based on FGB [12] (implemented in C by J.-C Faugère) for the computations of Gröbner bases. They also use RS [36] (implemented in C by F. Rouillier) for finding the real solutions of zero-dimensional systems and the isolation of real roots of univariate polynomials with rational coefficients. The computations have been done on an Intel(R) Xeon(TM) CPU 3.20GHz (2048 KB of cache) with 6 GB of RAM.

The polynomials $\sum_{i=1}^{n} \prod_{j \neq i}(X_i - X_j)$ which are called in the sequel $\mathbf{LL}_n$ are used as a benchmark for numerical methods based on LMI-relaxations (see [45]). In the sequel we consider **LL5** (which has degree 4 and contains 4 variables), **LL7** (which has degree 6 and contains 6 variables) and **LL9** (which has degree 8 and contains 8 variables) .

The following polynomial (denoted by **Vor1**) appears in [11]. The initial question was to decide if its discriminant (denoted by **Vor2**) with respect to the variable u is always positive. Answering to this question can be done by computing its infimum. The polynomial **Vor2** has 253 monomials and is of degree 18.

$$16\,a^2(\alpha^2+1+\beta^2)u^4+16\,a(-\alpha\,\beta\,a^2+ax\alpha+2\,a\alpha^2+2\,a+2\,a\beta^2+ay\beta-\alpha\,\beta)u^3+((24\,a^2+4\,a^4)\alpha^2+(-24\,\beta\,a^3-24\,a\beta-8\,ya^3+24\,xa^2-8\,ay)\alpha+24\,a^2\beta^2+4\,\beta^2-8\,\beta\,xa^3+4\,y^2a^2+24\,y\beta\,a^2-8\,ax\beta+16\,a^2+4\,x^2a^2)u^2+(-4\,\alpha\,a^3+4\,ya^2-4\,ax-8\,a\alpha+8\,\beta\,a^2+4\,\beta)(\beta-a\alpha+y-ax)u+(a^2+1)(\beta-a\alpha+y-ax)^2$$

The following polynomial appears in [10]. In this paper, one has to decide if this polynomial is always positive. We compute its infimum to answer this question.

$$1-8\,c^2d^2-196608\,e^3a^2d^2c+1536\,ead^4c^2+21504\,e^2ad^2c-4096\,e^2ac^3d^2-384\,ead^2+1024\,e^2ac+16\,c^4d^4-72\,c^2d^4+1024\,c^2e^2+36864\,e^2a^2d^4-3456\,ead^4+262144\,e^4a^2c^2-32768\,e^3ac^2+256\,c^3d^2e-576\,ced^2+81\,d^4+64\,ce-18\,d^2$$

The following polynomial appears in [29].

$$4\,a^6c^2d^2+2\,a^4b^2d^6-6\,a^4b^2d^4+a^4c^4+2\,a^4c^2d^6+6\,a^2b^2c^4-6\,a^4b^2c^4+4\,a^6b^2d^2+a^8b^4+6\,b^4c^2d^2-2\,b^6c^4d^2+a^8d^4+6\,a^2b^6d^2-8\,a^4b^4d^2-4\,a^4b^2d^6-6\,b^4c^4d^2-8\,a^4b^4c^2+6\,a^6b^2c^2-8\,a^2b^4c^2+6\,a^4b^4d^4-2\,b^4c^2d^4-4\,a^2b^4c^6-4\,a^6b^4c^2-6\,a^2b^4d^4-2\,a^4c^4d^2+10\,a^4b^2d^4-2\,a^2b^8c^2-6\,a^2b^6c^4+a^4b^8+6\,a^2b^2d^2+6\,a^6b^4d^2-4\,a^4b^6d^2+b^4d^4+b^4c^8+10\,a^2b^4c^4+6\,a^2b^2c^2+4\,a^2b^6c^2+a^4d^8+4\,b^6c^2d^2+6\,a^4b^6c^2-8\,a^4b^2d^2+4\,a^4b^2c^2-2\,a^8b^2d^2+6\,a^4c^2d^2+4\,a^2b^4d^2-6\,a^6b^2d^4+6\,a^4b^4c^4-2\,a^6c^2d^4+2\,b^4c^6d^2+2\,a^2b^2c^6-6\,a^4c^2d^4+b^8c^4+2\,a^4b^2-4\,a^4d^2+a^4-2\,b^6-2\,a^6+a^8+b^8+b^4+2\,a^2b^4+2\,b^6c^6-2\,b^8c^2-6\,b^6c^4+2\,a^6b^4-2\,a^2b^2-2\,a^6b^6+2\,a^4b^6-2\,a^2b^8-6\,a^4b^2c^4d^2+2\,a^2b^4c^4d^2+2\,a^4b^2c^2d^4-6\,a^2b^4c^2d^4-6\,a^4b^2c^2d^2-6\,a^2b^4c^2d^2+4\,a^2b^2c^4d^4+2\,a^2b^2c^2d^6+2\,a^2b^2c^4d^2+2\,a^2b^2c^2d^4-10\,a^2b^2c^2d^2+6\,a^2b^6c^2d^2-6\,a^4b^4+2\,a^2b^6-2\,a^8b^2+2\,a^6b^2+6\,a^6b^2c^2d^2-10\,a^4b^4c^2d^2-4\,b^4c^6+6\,b^4c^4+6\,b^6c^2-2\,a^6c^2+2\,a^2b^2c^6d^2+a^4c^4d^4-2\,a^4c^2-2\,b^6d^2-4\,a^4d^6+2\,a^6d^6-2\,a^8d^2-6\,a^6d^4+6\,a^6d^2+b^4c^4d^4-4\,b^4c^2+6\,a^4d^4-2\,b^4d^2(a^2-b^2)$$

In the sequel, we give the timings we obtained with an implementation of the algorithm we describe in this paper in the column **Algo**. Timings obtained by the numeric SOS Solver SOSTOOLS [34] are given in the column **SOS**. The column **CAD** contains the timings we obtained to solve the quantifier elimination problem induced by the global optimization problem by using the QEPCAD software [8]. The symbol ∞ below means that no result has been obtained after 1 week of computations.

	Algo	**SOS**	**CAD**
LL5	67 sec.	1 sec.	∞
LL7	10 hours	12 sec.	∞
LL9	∞	∞	∞
Vor1	40 sec.	53 sec.	∞
Vor2	2 hours	∞	∞
IT	10 sec.	2 sec.	5 sec.

Comparatively to **CAD**, the algorithm we describe in this paper is clearly more efficient since it can tackle problems that are not reachable by QEPCAD. We observe that *on most of these examples* numerical methods are faster. Nevertheless, *on these examples*, numerical methods have not allowed us to tackle problems that are not reachable by our method. Note also that they can't solve **Vor2**. Nevertheless, we believe that these techniques may return on answer on problems that are not tractable by our method. Finally, we observed numerical instability or wrong results for the problems **LL5**, **LL7** and **Vor1**. This shows that obtaining global optimization solvers based on computer algebra techniques is important and can be complementary to numerical methods.

7. 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 G.-M. Mbakop. Polar varieties and efficient real elimination. *Mathematische Zeitschrift*, 238(1):115–144, 2001.

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

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

[6] 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.

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

[8] C. Brown and H. et al. Hong. Qepcad - quantifier elimination by partial cylindrical algebraic decomposition. available at `http://www.cs.usna.edu/ qepcad/B/QEPCAD.html`.

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

[10] I. Emiris and E. Tsigaridas. Real algebraic numbers and polynomial systems of small degree. submitted to Journal of Symbolic Computation, 2008.

[11] H. Everett, D. Lazard, S. Lazard, and M. Safey El Din. The voronoi diagram of three lines in r^3. In

SoCG '07: Proceedings of the 23-rd annual symposium on computational geometry, pages 255–264, 6 2007.

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

[13] R.M. Freund, F Ordonez, and K.C. Toh. Behavioral measures and their correlation with ipm iteration counts on semidefinite programming problems. *Mathematial programming*, 109(2-3):445–475, 2007.

[14] M. Giusti, K. Hägele, J. Heintz, J.-E Morais, J.-L. Montaña, and L.-M. Pardo. Lower bounds for Diophantine approximation. In *Proceedings of MEGA'96*, number 117, 118 in Journal of Pure and Applied Algebra, pages 277–317, 1997.

[15] M. Giusti, J. Heintz, J.-E. Morais, J. Morgenstern, and L.-M. Pardo. Straight-line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, 124:101–146, 1998.

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

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

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

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

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

[21] D. Henrion. *Polynômes et optimisation convexe en commande robuste*. PhD thesis, LAAS, Toulouse, 2007. Habilitation à diriger des recherches.

[22] Z. Jelonek and K. Kurdyka. On asymptotic critical values of a complex polynomial. *J. Reine Angew. Math.*, 565:1–11, 2003.

[23] K. Kurdyka, P. Orro, and S. Simon. Semialgebraic sard theorem for generalized critical value. *Journal of differential geometry*, 56(1):67–92, 2000.

[24] Y. N. Lakshmann. 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'90*, volume 94 of *Progress in Mathematics*, pages 227–234. Birkhaüser, 1991.

[25] Y.N. Lakshmann and D. Lazard. On the complexity of zero-dimensional algebraic systems. In *MEGA*, volume 94 of *Progress in Mathematics*, pages 217–225. Birkhaüser, 1991.

[26] J.-B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001.

[27] J. B. Lasserre, M. Laurent, and P. Rostalski. Semidefinite characterization and computation of real radical ideals, 2006.

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

[29] Daniel Lazard. Quantifier elimination: optimal solution for two classical examples. *J. Symb. Comput.*, 5(1-2):261–266, 1988.

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

[31] Jiawang Nie, James Demmel, and Bernd Sturmfels. Minimizing polynomials via sum of squares over the gradient ideal. *Math. Program.*, 106(3):587–606, 2006.

[32] P. A. Parillo. Semi-definite relaxations for semi-algebraic problems. *Mathematical Programming*, 92(2):293–320, 2003.

[33] P. Parrilo and B. Sturmfels. Minimizing polynomial functions. *Dimacs Series in Discrete Mathematics and Theoretical Computer Science*, 60:83, 2003.

[34] S. Prajna, A. Papachristodoulou, P. Parillo, and P. Seiler. Sostools. available at `http://www.cds.caltech.edu/sostools/`.

[35] 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.

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

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

[38] 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.

[39] M. Safey El Din. Finding sampling points on real hypersurfaces in easier in singular situations. In *MEGA (Effective Methods in Algebraic Geometry) Electronic proceedings*, 2005.

[40] M. Safey El Din. Practical and theoretical issues for the computation of generalized critical values of a polynomial mapping and its applications. In *Proceedings of Asian Symposium on Computer Mathematics 2007*, 2007. to appear.

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

[42] M. Safey El Din. Testing sign conditions on a multivariate polynomial and applications. *Mathematics in Computer Science*, 1(1):177–207, December 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 ISSAC 2003*, 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*, 2004.

[45] M. Schweighofer. Global optimization of polynomials using gradient tentacles and sums of squares. *SIAM Journal on Optimization*, 17(3):920–942, 2006.