On the intrinsic complexity of point finding in real singular hypersurfaces

Bernd Bank [2], Marc Giusti [3],
Joos Heintz [4], Luis Miguel Pardo[5]

May 20, 2009

Abstract

In previous work we designed an efficient procedure that finds an algebraic sample point for each connected component of a smooth real complete intersection variety. This procedure exploits geometric properties of generic polar varieties and its complexity is intrinsic with respect to the problem. In the present paper we introduce a natural construction that allows to tackle the case of a non–smooth real hypersurface by means of a reduction to a smooth complete intersection.

*MSC:*14Q10, 14P05, 14B05, 68W30

Key words: Computational complexity; real polynomial equation solving; singular hypersurface

[1]Research partially supported by the following Argentinian, Canadian, French and Spanish agencies and grants: UBACYT X-098, UBACYT X-113, PICT–2006–02067, BLAN NT05-4-45732 (projet GECKO), MTM 2007-62799.

[2]Humboldt-Universität zu Berlin, Institut für Mathematik, D–10099 Berlin, Germany. bank@mathematik.hu-berlin.de

[3]CNRS, École Polytechnique, Laboratoire LIX, F–91228 Palaiseau Cedex, France. Marc.Giusti@Polytechnique.fr

[4]Departamento de Computación, Universidad de Buenos Aires and CONICET, Ciudad Univ., Pab.I, 1428 Ciudad Autónoma de Buenos Aires, Argentina, and Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, 39071 Santander, Spain.
joos@dc.uba.ar

[5]Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, 39071 Santander, Spain, luis.pardo@unican.es

1 Introduction and main result

This paper is devoted to the complexity of root finding in real algebraic sets in the particular case of a real *singular* hypersurface given by an equation $F \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree d in the variables $X_1, \ldots, X_n$. For the standard dense or sparse representation of F by its coefficients it is possible to find algebraic sample points for the connected components of $V_{\mathbb{R}} := \{x \in \mathbb{R}^n \mid F(x) = 0\}$ using $(nd^n)^{O(1)} = d^{O(n)}$ arithmetic and $((nh)d^n)^{O(1)} = (hd)^{O(n)}$ bit operations, where h measures the bit length of the coefficients of F.

Here we suppose that all connected components of $V_{\mathbb{R}}$ have dimension $n-1$ (this means that $V_{\mathbb{R}}$ is a real hypersurface) and we work in an uniform deterministic complexity model, codifying the coordinates of the output points by suitable sign conditions on univariate polynomial equations over $\mathbb{Z}$ (Thom's codification of real algebraic points).

It is not too difficult to generalize this complexity result to arbitrary semi–algebraic sets given by polynomial equations and inequalities (see e.g. the original papers [9, 11, 7, 13]).

The complexity bounds above are almost optimal for the given encoding of the input equation and the output points, but, unfortunately, they are out of reach for practical implementations. Moreover, the underlying algorithms are not incremental and do not take into account special, e.g. geometric, features of the equation F.

Therefore we replaced in [1] the classic dense or sparse representation of F by the arithmetic circuit encoding and introduced a geometric invariant, namely the maximal geometric degree δ of the entries of an arbitrary generic flag of classic polar varieties of the *complex* variety $V := \{x \in \mathbb{C}^n \mid F(x) = 0\}$. The outcome was an efficient algorithm which solves the root finding problem under consideration in time $L(nd\delta)^{O(1)} = (nd)^{O(n)}$, where L is the size of the given circuit representation of F. Here we suppose that the polynomial F is squarefree, the real variety $V_{\mathbb{R}}$ is *smooth* and *compact* and we work in a probabilistic uniform or deterministic non–uniform algebraic complexity model over $\mathbb{Q}$. The algorithm is incremental and capable to distinguish geometrically between well and ill–conditioned real root

finding problems. Moreover its complexity depends mainly on the geometric (i.e., semantic) invariant δ which is, by Bézout's Theorem, in worst case of order $d^{O(n)}$. In this sense, the complexity of the algorithm is intrinsic.

In [2, 3, 4] we generalized this result to an arbitrary *smooth* real variety given by reduced complete intersections of circuit represented polynomials. However, in the non–compact case, the maximal degree of the entries of a generic flag of *classic* polar varieties has to be replaced by its *dual* counterpart (see [5] for the geometric underpinning).

By means of appropriate deformations of the complex hypersurface V we obtain certain smooth algebraic complete intersection varieties together with a canonical atlas of them. The charts of such an atlas are closed smooth subvarieties of suitable affine spaces. The generic dual polar varieties of these subvarieties are called *bipolar* varieties of V and their maximal degree δ is the invariant we are looking for. In these terms we are able to state the following complexity result.

Theorem 1

Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a squarefree polynomial of degree $d \geq 2$ defining as before complex and real hypersurfaces V and $V_{\mathbb{R}}$. Suppose that F is given by a division–free arithmetic circuit of non–scalar size L. Then there exists a procedure (in fact, we shall show later in this paper, many of them) that finds a finite set of real algebraic sample points for the connected components of $V_{\mathbb{R}}$. The procedure may be modeled alternatively as being uniform probabilistic or non–uniform deterministic. The number of arithmetic operations in $\mathbb{Q}$ required by the procedure is linear in L and polynomial in d, n and δ.

Following [8, 10] this asymptotic complexity bound is almost optimal and cannot be improved by procedures based on standard program development techniques, even if alternative data types and structures are used.

For an alternative approach relying on the so–called "critical point method" for real root finding in singular real hypersurfaces we refer to [15].

The concept of classic polar varieties goes back to F. Severi and J. A. Todd in the 1930's and beyond that to the work of J.-V. Poncelet in the period of 1813–1829. The

modern theory started in 1975 with essential contributions due to R. Piene (global theory), B. Teissier and D. T. Lê , J. P. Henry and M. Merle (local theory), J. P. Brasselet and others (see [16], [12] and [6] for a historical account and references). The aim was a deeper understanding of singular (complex) varieties. On the other hand, classic (and the at that time novel) dual polar varieties became about ten years ago a fundamental tool for the design of efficient computer procedures with *intrinsic* complexity for real root finding problems.

It is not clear how the Theorem 1 may be generalized to more general cases (as e.g. arbitrary real complete intersection varieties). Nevertheless, the higher flexibility gained by admitting hypersurfaces with singularities for our algorithmic treatment transforms Theorem 1 in an usable and relevant tool for the resolution of more ambitious real elimination problems. Finally, we mention that there exists a strong relation between root finding in (singular) real varieties and the problem of sample point finding for strict polynomial inequalities.

The rest of this paper is devoted to the geometric foundation of Theorem 1 and a refinement of it, namely Theorem 3.

2 Geometry and complexity

Since $V_{\mathbb{R}}$ is a real hypersurface and F is reduced, the gradient of F does not vanish identically on any connected component of $V_{\mathbb{R}}$.

For any $1 \leq i \leq n-1$ let $a := a_i = [a_{k,l}]_{\substack{1 \leq k \leq n-i \\ 1 \leq l \leq n}}$ be a complex $((n-i) \times n)$–matrix of maximal rank $\operatorname{rk} a = n-i$. The (classic) i–th polar variety of V associated with a is denoted by $P_i(a)$ and consists of the closure of the set of all points of V, where the tangent space does not intersect transversally the kernel of a. When a is generically chosen from $\mathbb{C}^{(n-i)\times n}$, then $P_i(a)$ becomes a classic polar variety in the usual sense. In this case we shall say that $P_i(a)$ is *(fully) generic*.

Suppose that the polar variety $P_i(a)$ is generic and non–empty. Then $P_i(a)$ is of pure codimension i in V and normal and Cohen–Macaulay at any point which is smooth in V. Moreover, there exist canonical equations of degree at most nd with a circuit representation of size $O(L+n^3)$ that describe $P_i(a)$ locally as transversal

(and hence as reduced, complete) intersection outside of a subvariety at least of codimension one.

If $V_{\mathbb{R}}$ is smooth and compact and a is real matrix, then the real trace $P_i(a) \cap \mathbb{R}^n$ of $P_i(a)$ contains an algebraic sample point for every connected component of $V_{\mathbb{R}}$. This may happen to be wrong in case that $V_{\mathbb{R}}$ is not smooth anymore, even when $V_{\mathbb{R}}$ is compact.

Let $J(F) := (\frac{\partial F}{\partial X_1}, \ldots, \frac{\partial F}{\partial X_n})$ be the gradient of the polynomial F and $J(F)^T$ its transposition.

In the spirit of the canonic Room–Kempf desingularization of determinantal varieties we consider the incidence variety $\mathcal{H}_i$ consisting of the solutions $(x, a, \lambda, \mu) \in \mathbb{C}^n \times \mathbb{C}^{(n-i)\times n} \times \mathbb{C}^1 \times \mathbb{C}^{n-i}$ of the equation system

$$(*) \qquad F(x) = 0, \quad J(F)^T(x)\,\lambda + a^T \cdot \mu = 0$$

which satisfy the open conditions $\operatorname{rk} a = n - i$ and $\mu \neq 0$.

In the special case $i := n - 1$, the matrix $a = a_{n-1}$ is a n–tuple, and if a belongs to $\mathbb{R}^n$, then the real trace of $\mathcal{H}_i$ describes the extremal points and the Lagrange multipliers of the real valued function induced by a on $V_{\mathbb{R}}$.

Moreover, the image of $\mathcal{H}_i$ under its canonical projection into $\mathbb{C}^n$ is exactly the set of non–singular points of V. It is not difficult to show that $\mathcal{H}_i$ is a locally closed and smooth algebraic subvariety of the affine ambient space $\mathbb{C}^n \times \mathbb{C}^{(n-i)\times n} \times \mathbb{C}^1 \times \mathbb{C}^{n-i}$. Furthermore $\mathcal{H}_i$ is of pure dimension $(n-i)(n+1)$ and the equations $(*)$ intersect transversally at any point of $\mathcal{H}_i$.

We consider now the configuration space

$$E_i := \{(x, a, \lambda, \mu) \in \mathbb{C}^n \times \mathbb{C}^{(n-i)\times n} \times \mathbb{C}^1 \times \mathbb{C}^{n-i} \mid \operatorname{rk} a = n - i,\ \mu \neq 0\}.$$

E_i is an open subset of $\mathbb{C}^n \times \mathbb{C}^{(n-i)\times n} \times \mathbb{C}^1 \times \mathbb{C}^{n-i}$ and hence a smooth algebraic variety.

The algebraic group $G_i := GL(n-i) \times GL(1)$ acts in the following way from the right

on E_i : For $g := (b,t) \in G_i$ and $e := (x,a,\lambda,\mu) \in E_i$ let $e \cdot g := (x, b^T a,\, tb,\, tb^{-1} \cdot \mu)$. We denote by E_i^* the (topological) orbit space of E_i with respect to G_i. Since the algebraic group G_i is linearly reductive, E_i^* owns a natural structure of an algebraic variety. It turns out that E_i^* is smooth and equidimensional of dimension $r_i := n + i(n-i)$. Observe that $\mathcal{H}_i$ is a subvariety of E_i and that the action of G_i on E_i leaves $\mathcal{H}_i$ invariant. The manifold E_i^* owns a canonical atlas of $N_i := \binom{n}{n-i}(n-i)$ open charts U_k, $1 \leq k \leq N_i$ which are all isomorphic to $\mathbb{A}^{r_i}$. Let $\varphi_i : E_i \to E_i^*$ be the morphism of algebraic varieties which maps each point of E_i onto its G_i–orbit. Then φ_i is a smooth morphism of analytic manifolds. Let $S_i := \varphi_i(\mathcal{H}_i)$ and $S_{i,k} := S_i \cap U_k$ for $1 \leq k \leq N_i$. The geometric main issue is the following result.

Lemma 2

Let $1 \leq k \leq N_i$. Then, identifying U_k with $\mathbb{A}^{r_i}$, the constructible set $S_{i,k}$ becomes a smooth closed subvariety of the affine space $\mathbb{A}^{r_i}$. Moreover, $S_{i,k}$ is equidimensional of dimension $D_i := i(n-i) - 1$ and given as a transversal intersection of $n+1$ equations of degree d which have a circuit representation of size $O(L+n+i(n-i))$. In particular, S_i is a smooth subvariety of E_i^* and the varieties $S_{i,k}$, $1 \leq k \leq N_i$ form an open atlas of S_i.

We may now apply the algorithmic procedure designed in [3] and [4] or [15] in order to find for each connected component of the real trace of $S_{i,k}$ a sample point. The complexity of this procedure is dominated by the geometric degree of the dual polar varieties $B_{i,j,k}$, $1 \leq j \leq D_i$ of $S_{i,k}$ which we call *bipolar varieties* of V. The maximal geometric degree of the bipolar varieties of V is an invariant of V. For fixed i and k the bipolar varieties of V are organized by decreasing codimension j in strictly ascending chains as follows:

$$B_{i,D_i,k} \subset \cdots \subset B_{i,j,k} \subset \cdots \subset B_{i,1,k} \subset B_{i,0,k} = S_{i,k}$$

Finally with i running from $n-1$ to 1, we obtain a three–dimensional lattice of bipolar varieties. A *walk* in this lattice is a path, which starts with some n–tuple of zero–dimensional bipolar varieties $(B_{i_1,D_{i_1},k})_{1 \leq k \leq n}$ and ends with some orbit

variety S_{i_2}. At each step, the index i or the codimension j decreases and the bipolar varieties visited along the walk, modulo suitable sections and identifications, form an ascending chain of algebraic varieties of dimension increasing exactly by one. Their real trace is dense. Running through a given walk in the reverse mode, we obtain an algorithmic strategy, which as soon that it finds smooth real points on the bipolar varieties, projects them onto smooth real points of V.

This argumentation explains fairly well the geometric ideas behind our approach to point finding in singular real hypersurfaces.

For given $1 \leq i \leq n-1$, an algorithmic walk which follows textually our explanations would involve computations with polynomials in $O(n + (n-i)^2)$ variables. This woul lead to a worst case complexity estimation of $d^{O(n+(n-i)^2)}$ whereas the expected worst case complexity is $d^{O(n)}$. There are two ways out of this dilemma. One way is to choose the index i, $1 \leq i \leq n-1$ close to $n-1$ and the other consists in remodeling the deformation of $J(F)$ used in the equation system $(*)$ in the spirit of the concept of *sufficiently generic* varieties introduced in [5]. If we choose $i := n-1$ we obtain an intrinsic variant of the so called "critical point" method, which is often used in a geometrically unstructured way with extrinsic complexity bounds. Summarizing we have the following complexity result which implies Theorem 1.

Theorem 3

Let $F(X_1, \ldots, X_n)$ be a polynomial of degree $d \geq 2$ defining as before complex and real hypersurfaces V and $V_{\mathbb{R}}$. Suppose that F is given by a straight–line program of size L. Then each walk $\mathcal{W}$ yields a procedure $\mathcal{R}_{\mathcal{W}}$ that finds at least one algebraic sample point for each connected component of $V_{\mathbb{R}}$. The sequential time complexity of the procedure $\mathcal{R}_{\mathcal{W}}$ is linear in L and polynomial in d, n and a suitable geometric quantity $\delta_{\mathcal{W}}$. The quantity $\delta_{\mathcal{W}}$ is the maximal degree of the bipolar varieties of V visited during the walk and is therefore an intrinsic invariant of V and $\mathcal{W}$. It bounds also the number and the algebraic degree of the sample points produced by $\mathcal{R}_{\mathcal{W}}$.

References

[1] B. Bank, M. Giusti, J. Heintz, G.M. Mbakop, Polar varieties, real equation solving and data structures: The hypersurface case, J. Complexity 13 (1997) 5-27, Best Paper Award J. Complexity 1997.

[2] B. Bank, M. Giusti, J. Heintz, G.M. Mbakop, Polar varieties and efficient real elimination, Math. Z. 238 (2001) 115-144.

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

[4] B. Bank, M. Giusti, J. Heintz, L.M. Pardo, Generalized polar varieties: Geometry and algorithms. J. Complexity 21 (2005) 377-412.

[5] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, E. Schost, On the geometry of polar varieties. Submitted to AAECC (2009)

[6] J.P. Brasselet, Milnor classes via polar varieties, in: AMS, Contemp. Math. 266, 181-187 (2000)

[7] J. F. Canny: Some Algebraic and Geometric Computations in PSPACE, Proc. 20th ACM Symp. on Theory of Computing (1988) 460-467

[8] D. Castro, M. Giusti, J. Heintz, G. Matera, L. M. Pardo, The hardness of polynomial equation solving, Found. Comput. Math. 3 (2003) 347–420.

[9] D. Grigor'ev, N. Vorobjov, Solving systems of polynomial inequalities in subexponential time, J. Symb. Comput. 5 (1988) 37-64.

[10] J. Heintz, B. Kuijpers, Constraint databases, data structures and efficient query evaluation. in Kuijpers, Bart et al. (eds.), Constraint databases. First international symposium, CDB 2004, Paris, France, June 12–13, 2004. Proceedings. Berlin: Springer. Lecture Notes in Computer Science 3074, 1-24 (2004)

[11] J. Heintz, M.F. Roy, P. Solernó, On the complexity of semialgebraic sets, in: G.X. Ritter (Ed.), IFIP Information Processing 89, Elsevier, 1989, 293-298.

[12] R. Piene, Polar classes of singular varieties, Ann. Scient. Éc. Norm. Sup. 4. Sér. 11 (1978) 247-276.

[13] J. Renegar: A faster PSPACE algorithm for deciding the existential theory of the reals. 29th Annual Symposium on Foundations of Computer Science, 291-295, (1988).

[14] M. Safey El Din, E. Schost, Properness defects of projections and computation of at least one point in each connected component of a real algebraic set, J. Discrete and Comput. Geom. 32 (2004) 417-430.

[15] M. Safey El Din, Finding sampling points on real hypersurfaces is easier in singular situations, prépublication (2005).

[16] B. Teissier, Quelques points de l'histoire des variétés polaires, de Poncelet à nos jours, Sémin. Anal., Univ. Blaise Pascal 1987-1988, 4 (1988).