Bit complexity for critical point computation in smooth and compact real hypersurfaces

Jesse Elliott* and Éric Schost†

David R. Cheriton School of Computer Science
University of Waterloo, Canada

Abstract

Consider the polynomial mapping defined by the projection to the first coordinate on a real, smooth and compact hypersurface. The critical points of this mapping in generic coordinates have several applications in real algebraic geometry. We provide bit complexity estimates for computing them.

Generic coordinates are obtained by applying a randomly chosen linear change of variables to the polynomial defining the hypersurface. The coordinates are sufficiently generic when the Jacobian matrix of the system under study has full rank at the critical points and when the number of critical points is finite. We have proven a new quantitative extension of Thom's weak transversality theorem [1]. By applying this extension, we are able to choose sufficiently generic changes of variables with arbitrarily high probability.

1 Introduction

1.1 Notation and problem statement

Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be squarefree with total degree d and $V(f)$ smooth. Let $\vartheta \in \mathbb{Q}^{n^2}$ be a linear change of variables that we apply to f obtaining $f^\vartheta(x) = f(\vartheta x)$. We provide bit size estimates for computing the critical points $x \in V(f^\vartheta) \cap \mathbb{R}^n$ of the projection $(x_1, \ldots, x_n) \mapsto x_1$ denoted by $\Pi_1 : \mathbb{C}^n \to \mathbb{C}$.

The point x is a *critical point* if $\dim \Pi_1(T_x V(f^\vartheta)) = 0$ with $T_x V(f^\vartheta)$ denoting the *Zariski-tangent space* defined by the equations $\frac{\partial g}{\partial X_1}(x)v_1 + \ldots + \frac{\partial g}{\partial X_n}(x)v_n = 0$, for all polynomials $g \in I(V(f^\vartheta))$. Hence, a point is a critical point when the dimension of the tangent space at the point drops from 1 to 0. We show that the set of all critical points is defined by the vanishing of the polynomials $f^\vartheta, \frac{\partial f^\vartheta}{\partial X_2}, \ldots, \frac{\partial f^\vartheta}{\partial X_n}$. A *critical value* is the image of a critical point. Points that are not critical points are called *regular points* and a *regular value* is the image of a regular point.

For $a = \frac{u}{v}$ in $\mathbb{Q} - \{0\}$ the *height* of a is the maximum of $\log(|u|)$ and $\log(|v|)$, where $u \in \mathbb{Z}$ and $v \in \mathbb{N}$ are coprime. If v is the minimal common denominator of all non zero coefficients of f, then the *height* of f is defined as the maximum of the logarithms of v and of the absolute values of the coefficients of vf.

1.2 Main results

Notice that we are computing the critical points in generic coordinates by applying the linear change of variables ϑ to the input polynomial f. These critical points have applications in real algebraic geometry which we discuss in Section 2.1.

Our main result is the following theorem.

*jakellio@uwaterloo.ca
†eschost@uwaterloo.ca

Theorem 1 *Suppose that f satisfies $\deg f \leq d$, height $f \leq s$, with f given by a straight-line program Γ of size L with integer constants of height at most b. There exists a randomized algorithm that takes L, d, and s as input and produces a zero-dimensional parameterization of the critical points*

$$V(f^\vartheta, \frac{\partial f^\vartheta}{\partial X_2}, \ldots, \frac{\partial f^\vartheta}{\partial X_n}),$$

with probability at least $18/32$, where $\vartheta \in \mathbb{Q}^{n^2}$ is a linear change of variables chosen randomly by the algorithm. Otherwise the algorithm either produces a subset of the critical points or FAIL. In any case, the algorithm uses

$$O^\sim(Lb + d^{2n}(s+d)(L+d))$$

boolean operations.

Hence, the algorithm is Monte Carlo and can error on one side by producing a proper subset of the critical points. Running the algorithm k times gives a list of outputs among which the highest cardinality set includes all critical points with probability at least $1 - (14/32)^k$.

The algorithm requires some genericity properties which essentially imply that the Jacobian of the system of polynomials $f^\vartheta, \frac{\partial f^\vartheta}{\partial X_2}, \ldots, \frac{\partial f^\vartheta}{\partial X_n}$ has full rank at the critical points and that the number of critical points is finite. If ϑ is sufficiently generic, these properties will hold. In Section 3.2, we show how to choose ϑ so that the properties hold with arbitrarily high probability.

2 Motivation

2.1 Applications

2.1.1 Computing roadmaps of semi-algebraic sets

Computing the real critical points of Π_1 in generic coordinates is an important step in computing a *roadmap* of a semi-algebraic set, as for instance in [1]. A *roadmap* R of a semi-algebraic set S is a curve with non-empty and connected intersection with each connected component of S. Hence, roadmaps can be used for deciding connectivity properties in semi-algebraic sets while reducing these problems to computations in dimension 1. Roadmaps were introduced by Canny for solving motion planning problems in robotics [6].

2.1.2 More applications in real algebraic geometry

The set of real critical points of Π_1 in generic coordinates is finite and gives one point on each connected component of $V(f) \cap \mathbb{R}^n$, assuming $V(f) \cap \mathbb{R}^n$ is smooth and compact. Hence, computing the critical points determines an upper bound on the number of connected components and determines whether real solutions exist [2, 3].

2.2 Bit complexity

Bit complexity provides a more realistic model of computation compared to algebraic complexity, which only counts each operation at unit cost. Bit estimates provide more information for both time and space resources that are needed in practice.

3 Methods

3.1 Genericity properties

We assume our input polynomial f is squarefree with $V(f) \cap \mathbb{R}^n$ smooth and compact. Given these assumptions, the critical points are defined by the vanishing of $f, \frac{\partial f}{\partial X_2}, \ldots, \frac{\partial f}{\partial X_n}$. When ϑ is sufficiently generic, the Jacobian of the system of polynomials $f^\vartheta, \frac{\partial f^\vartheta}{\partial X_2}, \ldots, \frac{\partial f^\vartheta}{\partial X_n}$ will have full rank at all $x \in V(f^\vartheta) \cap \mathbb{R}^n$. It then follows by the Jacobian criterion [4, Theorem 16.19] that

1. the set of critical points in generic coordinates $V(f^\vartheta, \frac{\partial f^\vartheta}{\partial X_2}, \ldots, \frac{\partial f^\vartheta}{\partial X_n})$ is finite, and

2. the ideal $\langle f^\vartheta, \frac{\partial f^\vartheta}{\partial X_2}, \ldots, \frac{\partial f^\vartheta}{\partial X_n} \rangle$ is radical.

The algorithm requires that properties 1 and 2 hold.

Definition. We say that $\vartheta \in \mathbb{Q}^{n^2}$ is *lucky* if the Jacobian of the system of polynomials $f^\vartheta, \frac{\partial f^\vartheta}{\partial X_2}, \ldots, \frac{\partial f^\vartheta}{\partial X_n}$ has full rank at all $x \in V(f^\vartheta) \cap \mathbb{R}^n$. Otherwise we say that ϑ is *unlucky*.

3.2 Transverslaity results

We prove the following theorem.

Theorem 2 *The unlucky changes of variables are contained in a hypersurface of degree at most* $(d+1)^n$.

Using Theorem 2 and the Schwartz-Zippel lemma, we then go on and prove the following corollary.

Corollary 1 *Fix* $S \subset \mathbb{Q}$ *with* $|S| \geq \epsilon^{-1}(d+1)^n$ *and* $\epsilon > 0$. *Then for* ϑ *randomly chosen from* S^{n^2},

$$Pr[\vartheta \text{ is lucky }] \geq 1 - \epsilon.$$

3.3 Explanation and summary of proof techniques for Theorem 2

3.3.1 Finding a hypersurface Δ that contains the unlucky changes of variables

Let $\Phi : \mathbb{C}^n \times \mathbb{C}^{\widetilde{d}} \to \mathbb{C}^m$ be a polynomial mapping where $n, \widetilde{d}$, and m are positive integers. Assume the total degree of Φ is bounded by an integer d. For $\vartheta \in \mathbb{C}^{\widetilde{d}}$, let $\Phi_\vartheta : \mathbb{C}^n \to \mathbb{C}^m$ be the induced mapping $x \mapsto \Phi(x, \vartheta)$. It follows from Thom's weak transversality [1] that, when Φ is *transverse* to 0, which means that 0 is a regular value of Φ, an open dense set $\mathscr{U} \subset \mathbb{C}^{\widetilde{d}}$ exists with the property that for $\vartheta \in \mathscr{U}$, Φ_ϑ is transverse to 0. Hence, if ϑ is such that 0 is not a regular value of Φ_ϑ then ϑ is contained in the hypersurface $\Delta = \mathbb{C}^{\widetilde{d}} - \mathscr{U}$.

Put $X = \Phi^{-1}(0)$ and denote by $\pi : \mathbb{C}^n \times \mathbb{C}^{\widetilde{d}} \to \mathbb{C}^{\widetilde{d}}$ the projection $(x, \vartheta) \mapsto \vartheta$. The classical proof of Thom's weak transversality goes by showing that if $\vartheta \in \mathbb{C}^{\widetilde{d}}$ is such that 0 is not a regular value of Φ_ϑ then ϑ is a critical value of $\pi|_X$. It then follows from Sard's lemma [1] that the critical values of $\pi|_X$ are contained in a hypersurface.

We take $\widetilde{d}$ to be n^2 and m to be $n - i + 1$, and we take Φ to be the polynomial mapping $(x, \vartheta) \mapsto (f^\vartheta(x), \frac{\partial f^\vartheta}{\partial X_2}(x), \ldots, \frac{\partial f^\vartheta}{\partial X_n}(x))$ so that $\Phi^{-1}(0)$ defines the critical points in generic coordinates. We show that 0 is a regular value of Φ and thus by Thom's weak transversality there exists a hypersurface $\Delta \subset \mathbb{C}^{n^2}$ with the property that, if $\vartheta \in \mathbb{C}^{n^2}$ is such that 0 is not a regular value of Φ_ϑ, so that there exists an $x \in V(f^\vartheta)$ where $\mathrm{jac}_x \Phi_\vartheta$ does not have full rank and therefore ϑ is unlucky, then ϑ is contained in the hypersurface Δ.

3.3.2 Bounding the degree of the hypersurface Δ

We first bound the degree of an algebraic set Δ' containing the critical points (x, ϑ) of $\pi|_X$. We show that

$$\deg \Delta \leq \deg \Delta' \leq (d+1)^n.$$

We bound the degree of Δ' as follows. Denote by M the matrix of polynomials

$$M = \begin{bmatrix} \mathrm{jac}(\pi|_X) \\ \mathrm{jac}(\Phi) \end{bmatrix}.$$

We prove that $M(x,\vartheta)$ has full rank $\widetilde{d}+m$ if and only if (x,ϑ) is a regular point of $\pi|_X$. Hence, $\Delta^{'}$ is defined by the minors of $M(x,\vartheta)$ of order $\widetilde{d}+m$. Next, we observe that

$$M(x,\vartheta) = \begin{bmatrix} \mathrm{jac}_{(x,\vartheta)}(\pi|_X) \\ \mathrm{jac}_{(x,\vartheta)}(\Phi) \end{bmatrix} = \begin{bmatrix} \mathbf{0}_{n\times\widetilde{d}} & \mathbf{I}_{\widetilde{d}} \\ \mathrm{jac}_{(x,\vartheta)}(\Phi) \end{bmatrix} = \begin{bmatrix} \mathbf{0}_{n\times\widetilde{d}} & \mathbf{I}_{\widetilde{d}} \\ \mathrm{jac}_{(x,\vartheta)}(\Phi)[;1,n] & \mathrm{jac}_{(x,\vartheta)}(\Phi)[;n+1,\widetilde{d}] \end{bmatrix},$$

and we show that $\Delta^{'}$ is also defined by the minors of the sub-matrix $J = \mathrm{jac}_{(x,\vartheta)}(\Phi)[;1,n]$ of order $\min\{n,m\}$. We then introduce Lagrange multipliers $L=(L_1,\ldots,L_m)$ and let $G_1,\ldots,G_n$ be the equations defined by the Lagrange system

$$[L_1,\ldots,L_m]\ J(x,\vartheta)\ = [G_1(x,\vartheta,L),\ldots,G_n(x,\vartheta,L)] = [0,\ldots,0].$$

We let $\mathfrak{Z}$ denote the algebraic set defined by the vanishing of $G_1,\ldots,G_n$, and show that

$$\deg\Delta^{'} \leq \deg\mathfrak{Z} \leq (d+1)^n.$$

4 Conclusion

4.1 Summary of main results

We have provided bit size estimates for computing the critical points $x \in V(f^{\vartheta}) \cap \mathbb{R}^n$ of the projection $\Pi_1 : \mathbb{C}^n \to \mathbb{C}$. These critical points arise in several applications in real algebraic geometry. Furthermore, we have proven a new quantitative extension of Thom's weak transversality theorem. By applying this extension, we are able to choose sufficiently generic changes of variables with arbitrarily high probability.

4.2 Next steps and further work

Our ultimate goal is to determine the bit complexity of the algorithm in [1] which computes a roadmap of a semi-algebraic set. This algorithm requires some additional genericity properties. We need to prove that these additional properties hold for generic cases and we need to develop quantitative versions of these statements. Furthermore, we need to remove the compactness assumption using the methods from [5].

References

[1] É. Schost and M. Safey El Din. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. Journal of the ACM, Vol. 63(6), 2017.

[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] D. Eisenbud. Commutative algebra with a view toward algebraic geometry, volume 150 of Graduate Texts in Mathematics. Springer-Verlag, 1995.

[5] É. Schost and M. Safey El Din. Polar varieties and computation of one point in each connected component of a smooth real algebraic set, In ISSAC$^{'}$03 pages 224-231. ACM, 2003.

[6] J. Canny. The complexity of robot motion planning. PhD thesis, MIT, 1987.