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

Problem statement

Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be squarefree with total degree d and $V(f) \cap \mathbb{R}^n$ smooth and compact. Let $A \in \mathbb{Q}^{n^2}$ be a linear change of variables that we apply to f obtaining $f^A(x) = f(Ax)$. We provide bit size estimates for computing the critical points in generic coordinates $x \in V(f^A) \cap \mathbb{R}^n$ of the projection $\Pi_1 : (x_1, \ldots, x_n) \in \mathbb{C}^n \mapsto x_1 \in \mathbb{C}$. The critical points are defined by the vanishing of $f^A, \frac{\partial f^A}{\partial X_2}, \ldots, \frac{\partial f^A}{\partial X_n}$.

An example of the critical points

Let $f = X_1^2 + X_2^2 + X_3^2 - 1$ and consider

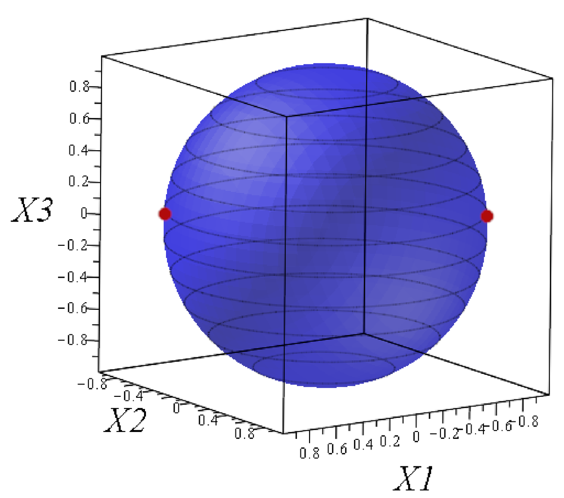
$$V(X_1^2 + X_2^2 + X_3^2 - 1) \subset \mathbb{C}^3.$$

The real critical points of Π_1 are defined by

$$X_1^2 + X_2^2 + X_3^2 - 1 = X_2 = X_3 = 0$$

and thus define the algebraic set

$$V(f, X_2, X_3) = V(f, \frac{\partial f}{\partial X_2}, \frac{\partial f}{\partial X_3}).$$



Applications

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]. Roadmaps are used for deciding connectivity properties in semi-algebraic sets.

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].

Generic coordinates

When A is sufficiently generic, the Jacobian of the system of polynomials $f^A, \frac{\partial f^A}{\partial X_2}, \ldots, \frac{\partial f^A}{\partial X_n}$ will have full rank at all $x \in V(f^A) \cap \mathbb{R}^n$. It then follows by the Jacobian criterion [4, Theorem 16.19] that the set of critical points $V(f^A, \frac{\partial f^A}{\partial X_2}, \ldots, \frac{\partial f^A}{\partial X_n})$ is finite, and the ideal $\langle f^A, \frac{\partial f^A}{\partial X_2}, \ldots, \frac{\partial f^A}{\partial X_n} \rangle$ is radical. In this case we say A is good. Otherwise we say that A is bad.

Theorem 1. The bad changes of variables are contained in a hypersurface $\Delta \subset \mathbb{C}^{n^2}$ of degree at most $(d+1)^n$.

Corollary 2. Fix $S \subset \mathbb{Q}$ with $|S| \geq \epsilon^{-1}(d+1)^n$ and $\epsilon > 0$. Then for A in S^{n^2} chosen randomly, $Pr[A \text{ is good }] \geq 1 - \epsilon$.

Bit complexity

Theorem 3. 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 Γ, d, and s as input and produces a zero-dimensional parameterization of the critical points

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

with probability at least 9/16, where $A \in \mathbb{Q}^{n^2}$ 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.

Running the algorithm k times gives a list of outputs among which the highest cardinality set includes all critical points with probability at least $1 - (7/16)^k$.

Transversality

We prove Theorem 1 by developing a quantitative extension of Thom's weak transversality [1, Proposition B.3], specialized to the particular case of transversality to a point which can be rephrased entirely in terms of critical and regular values: f is transverse to a point $\{a\}$ if and only if $\{a\}$ is a regular value of f, where regular /critical values are images of respectively regular /critical points.

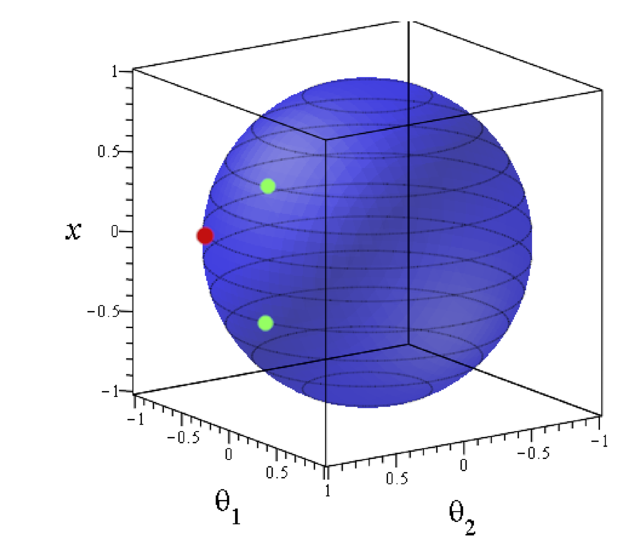
Let $\Phi : \mathbb{C}^n \times \mathbb{C}^{\tilde{d}} \to \mathbb{C}^m$ be a polynomial mapping where $n, \tilde{d}$, and m are positive integers. Assume the total degree of Φ is bounded by an integer d. For $A \in \mathbb{C}^{\tilde{d}}$, let $\Phi_A : \mathbb{C}^n \to \mathbb{C}^m$ be the induced mapping $x \mapsto \Phi(x, A)$.

Theorem 4. Suppose that 0 is a regular value of Φ. Then there exists a hypersurface $\Delta \subset \mathbb{C}^{\tilde{d}}$ of degree bounded by $(d+1)^n$ for which, if $A \in \mathbb{C}^{\tilde{d}} - \Delta$ then 0 is a regular value of Φ_A.

We use Theorem 4 to show that Δ contains that bad changes of variables.

An example of Thom's weak transversality

Let $\Phi(x, \vartheta_1, \vartheta_2) = x^2 + \vartheta_1^2 + \vartheta_2^2 - 1$ so that $\Phi^{-1}(0)$ is a smooth variety which implies that Φ is transverse to 0. Now, Thom's theorem tells us that, for a generic choice of $A = [A_1, A_2]$, the polynomial $\Phi(x, A_1, A_2) = \Phi_A(x)$ is transverse to 0. $\Phi_A(x)$ is univariate and transverse to zero when $x \in \Phi_A^{-1}(0) \Rightarrow \mathrm{grad}_x \Phi_A \neq 0$. Hence, when squarefree. The green points correspond to a generic choice of A_1 and A_2 whereas the red point corresponds to a double root which is an unlucky choice.



The bad ϑ are contained in Δ

We let Φ be the 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 Theorem 4, a hypersurface $\Delta \subset \mathbb{C}^{n^2}$ exists with the property that, if $A \in \mathbb{C}^{n^2} - \Delta$, then 0 is a regular value of Φ_A, which means that $\mathrm{jac}_x \Phi_A$ has full rank for all $x \in V(f^A)$ and therefore A is good. Hence, Δ contains the bad changes of variables.

Proving Theorem 4

Put $X = \Phi^{-1}(0)$ and let $\pi : (x, \vartheta) \in \mathbb{C}^n \times \mathbb{C}^{\tilde{d}} \mapsto \vartheta \in \mathbb{C}^{\tilde{d}}$.

The classical proof of Thom's weak transversality goes by showing that if $\vartheta \in \mathbb{C}^{\tilde{d}}$ 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 $\Delta \subset \mathbb{C}^{\tilde{d}}$.

We first bound the degree of an algebraic set Δ' containing the critical points (x, ϑ) of $\pi|_X$. We show that $\deg \Delta \leq \deg \Delta' \leq (d+1)^n$.

Let $M = \begin{bmatrix} \mathrm{jac}(\pi|_X) \\ \mathrm{jac}(\Phi) \end{bmatrix}$. We prove that $M(x, \vartheta)$ has full rank $\tilde{d} + m$ if and only if (x, ϑ) is a regular point of $\pi|_X$. Hence, Δ' is defined by the minors of $M(x, \vartheta)$ of order $\tilde{d} + m$.

Next, we observe that

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

and we show that Δ' is also defined by the minors of the sub-matrix $J = \mathrm{jac}_{(x,\vartheta)}(\Phi)[; 1, n]$ of order 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

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

We let $\mathfrak{Z}$ denote the algebraic set defined by the vanishing of $G_1, \ldots, G_n$, and show that $\deg \Delta \leq \deg \Delta' \leq \deg \mathfrak{Z} \leq (d+1)^n$.

References

[1] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. Journal of the ACM 63(6):1-48, 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.