On the bit complexity of some randomized algorithms in real algebraic geometry

Jesse Elliott, Mark Giesbrecht, Éric Schost

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

Outline

1. Computing one point in each connected component of a smooth real algebraic set
   - Problem statement
   - Polar varieties
   - The algorithm
   - Weak transversality
   - Quantitative genericity statements
   - Proving the main result
2. Deciding connectivity queries in smooth and bounded real hypersurfaces
   - Problem statement
   - Other work on roadmap computation
   - Estimating the height of the output

Outline

1. Computing one point in each connected component of a smooth real algebraic set
   - Problem statement
   - Polar varieties
   - The algorithm
   - Weak transversality
   - Quantitative genericity statements
   - Proving the main result

2. Deciding connectivity queries in smooth and bounded real hypersurfaces
   - Problem statement
   - Other work on roadmap computation
   - Estimating the height of the output

Problem statement

Problem 1

- Suppose that $F = (f_1, \ldots, f_p) \in \mathbb{Z}[X_1, \ldots, X_n]^p$ is a sequence of polynomials.
- Suppose that the ideal $\langle f_1, \ldots, f_p \rangle$ is radical and that $V = V(F) \subset \mathbb{C}^n$ is smooth and equidimensional with dimension $n - p$.
- Compute at least one point in each connected component of $V(F) \cap \mathbb{R}^n$.

Applications

- Used in higher level algorithms.
- Decide if $V(F) \cap \mathbb{R}^n$ has solutions.
- Determine an upper bound on the number of connected components of $V(F) \cap \mathbb{R}^n$.

Starting point

- An algorithm by [Safey El Din, Schost, 2003]
  - Uses random changes of variables that are proven to generically ensure certain desirable geometric properties.
  - Cost given in an algebraic complexity model.

Contributions

- We determine the bit complexity and error probability.
- We provide a quantitative analysis of the genericity properties:
  - Weak transversality.
  - Noether normalization for polar varieties.

Future work

- Reuse the techniques in the analysis of other algorithms.
  - Randomized algorithms for deciding connectivity queries on smooth and bounded real hypersurfaces.

Main result

- Let $F = (f_1, \ldots, f_p) \in \mathbb{Z}[X_1, \ldots, X_n]^p$ with $\deg(f_i) \le d$ and $\mathrm{ht}(f_i) \le b$. Suppose $\langle f_1, \ldots, f_p \rangle$ is radical and $V = V(F) \subset \mathbb{C}^n$ is smooth and equidimensional with dimension $n - p$.
  - The height of a polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ is the maximum of the logarithms of the absolute values of the coefficients of f.

Theorem

- For $0 < \epsilon < 1$, there exists a randomized algorithm that takes F and ϵ as input and returns a finite set including at least one point on each connected component of $V(F) \cap \mathbb{R}^n$.
- The algorithm succeeds with probability at least $1 - \epsilon$, and otherwise returns a proper subset of the points or FAIL.
- The algorithm uses

$$O^{\sim}(d^{3n+2p+1}(\log 1/\epsilon)(b + \log 1/\epsilon))$$

bit operations. The polynomials in the output have degree at most d^{n+p}, and height

$$O^{\sim}(d^{n+p+1}(b + \log 1/\epsilon)).$$

Main result

- The algorithm uses
$$O^{\sim}(d^{3n+2p+1}(\log 1/\epsilon)(b+\log 1/\epsilon))$$
bit operations. The polynomials in the output have degree at most d^{n+p}, and height
$$O^{\sim}(d^{n+p+1}(b+\log 1/\epsilon)).$$
- Roughly optimal: equal to the output bit-size times the algebraic complexity.
- Close to matching what is implemented in practice, in Maple, available through RAGlib.
- A different algorithm with bit complexity $d^{O(n)}$ [Basu, Pollack, Roy, 2003].
  - This algorithm is general and makes no assumptions on the input polynomials.
  - Given the generality of the algorithm, the constant in the exponent is large (not used in practice).

Outline

- Let $T_{\boldsymbol{x}}V$ denote the Zariski-tangent space to V at $\boldsymbol{x} \in V$. And for $i \in \{1, \ldots, n-p+1\}$, denote by π_i the projection

$$\begin{aligned} \mathbb{C}^n &\to \mathbb{C}^i \\ (x_1, \ldots, x_n) &\mapsto (x_1, \ldots, x_i). \end{aligned}$$

- The i-th polar variety

$$W(i, V) := \{\boldsymbol{x} \in V \mid \dim \pi_i(T_{\boldsymbol{x}}V) < i\}$$

is the set of critical points of π_i on V.

Determinantal modeling of polar varieties

- Let $\mathrm{jac}(F, i)$ denote the truncated Jacobian matrix

$$\begin{bmatrix} \frac{\partial f_1}{\partial X_{i+1}} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial f_p}{\partial X_{i+1}} & \cdots & \frac{\partial f_p}{\partial X_n} \end{bmatrix}.$$

  - $W(i, V(F)) = \{\boldsymbol{x} \in \mathbb{C}^n \mid F(\boldsymbol{x}) = 0 \text{ and } \mathrm{rank}(\mathrm{jac}_{\boldsymbol{x}}(F, i)) < p\}$.

- Let $M_{i,1}, \ldots, M_{i,S_i}$ be the p-minors of $\mathrm{jac}(F, i)$.
  - $W(i, V(F)) = V\left(F, M_{i,1}, \ldots, M_{i,S_i}\right)$.

- When $V = V(F) = V(f)$ is a hypersurface, then

$$W(i, V(f)) = V\left(f, \frac{\partial f}{\partial X_{i+1}}, \ldots, \frac{\partial f}{\partial X_n}\right).$$

Example

- Let $f = X_1^2 + X_2^2 + X_3^2 - 1$ and consider
$$V = V(X_1^2 + X_2^2 + X_3^2 - 1) \subset \mathbb{C}^3.$$
- The critical points of the projection
$$\pi_2 : (x_1, x_2, x_3) \mapsto (x_1, x_2)$$
on $V(f)$ are defined by $V\left(f, \frac{\partial f}{\partial X_3}\right)$. Hence, the polar variety is defined by those points where
$$X_1^2 + X_2^2 + X_3^2 - 1 = X_3 = 0.$$

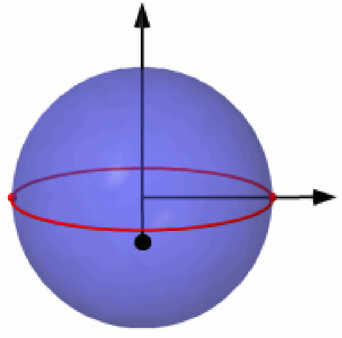


Image from
[Safey El Din, Schost, 2017]

Lagrangian modeling of polar varieties

- Due to the relations between minors of a matrix, the equations

$$\left(F, M_{i,1}, \ldots, M_{i,S_i}\right)$$

  are in general not a complete intersection.
- For both the polynomial system algorithm we use, and an effective Nullstellensatz application, we want equations that define a complete intersection.
- By introducing new indeterminates $(L_1, \ldots, L_p)$, we can model polar varieties as projections of Lagrange systems:

$$V\left(F, [L_1 \cdots L_p] \cdot \mathrm{jac}(F, i), \sum_{i=1}^{p} u_i L_i - 1\right).$$

- The existence of a solution characterizes the set where $\mathrm{jac}(F, i)$ is rank deficient.

Example

- Consider $f = X_1^2 + X_2^2 + X_3^2 - 1$ and $V(X_1^2 + X_2^2 + X_3^2 - 1) \subset \mathbb{C}^3$, then

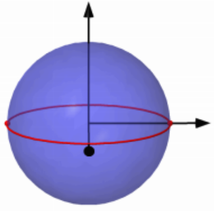
$$\mathrm{jac}(X_1^2 + X_2^2 + X_3^2 - 1, 2) = 2X_3.$$

- The Lagrangian modeling gives

$$V(X_1^2 + X_2^2 + X_3^2 - 1, LX_3, L - 1) = V(X_1^2 + X_2^2 - 1, X_3, L - 1).$$

  The equations on the right hand side are a lexicographically ordered Gröebner basis of the ideal $\langle X_1^2 + X_2^2 + X_3^2 - 1, LX_3, L - 1\rangle$.

- $\pi_{\mathbf{X}}\left(V(X_1^2 + X_2^2 - 1, X_3, L - 1)\right)$ describes $W(2, V(f))$:



Outline

1. Computing one point in each connected component of a smooth real algebraic set
   - Problem statement
   - Polar varieties
   - The algorithm
   - Weak transversality
   - Quantitative genericity statements
   - Proving the main result

2. Deciding connectivity queries in smooth and bounded real hypersurfaces
   - Problem statement
   - Other work on roadmap computation
   - Estimating the height of the output

The algorithm

- If we apply a generic change of coordinates $\boldsymbol{A} \in \mathbb{Z}^{n\times n}$ to $F = (f_1, \ldots, f_p)$:

$$F^{\boldsymbol{A}} = \big(f_1(\boldsymbol{AX}), \ldots, f_p(\boldsymbol{AX})\big),$$

  then $W(i, V(F^{\boldsymbol{A}})$ is known to be equidimensional of dimension $(i-1)$ or empty [Bank, Giusti, Heintz, Mbakop, 1997]
  and to be in *Noether position.*

- It then suffices to choose a generic $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{n-p})$ in $\mathbb{Z}^{n-p}$ and solve the systems defined by

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, \left(F^{\boldsymbol{A}}, M_{i,1}^{\boldsymbol{A}}, \ldots, M_{i,S_i}^{\boldsymbol{A}}\right)$$

  for $i = 1, \ldots, n-p+1$.

  - Computes the intersection of $W(i, F^{\boldsymbol{A}})$ with the fiber $\pi_i^{-1}(\sigma_1, \ldots, \sigma_{i-1})$.

- They all admit finitely many solutions.
- The union of their solution sets contains one point on each connected component of $V(F) \cap \mathbb{R}^n$.
  [Safey El Din, Schost, 2003]

The algorithm

- Since the equations

$$\left(F, M_{i,1}, \ldots, M_{i,S_i}\right)$$

are in general not a complete intersection, we instead use the Lagrangian modeling of polar varieties and solve the equations

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, \left(F, [L_1 \cdots L_p] \cdot \mathrm{jac}(F, i), \sum_{i=1}^{p} u_i L_i - 1\right),$$

for $i = 1, \ldots, n-p+1$, and then compute the projections of each solution set on the $\boldsymbol{X}$-space.

Main contributions

- We analyze precisely what conditions on our change of coordinates $\boldsymbol{A} \in \mathbb{Z}^{n\times n}$ guarantee success.
- We revisit key ingredients in the proofs given in
  [Bank, Giusti, Heintz, Mbakop, 1997],
  [Safey El Din, Schost, 2003]
  and we give quantitative versions of these results, bounding the degrees of the hypersurfaces we have to avoid.
- To solve the equations

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, \left(F, [L_1 \cdots L_p] \cdot \mathrm{jac}(F, i), \sum_{i=1}^{p} u_i L_i - 1\right)$$

  we use the algorithm in [Safey El Din, Schost, 2018] for which a complete bit complexity analysis is available.

Outline

1. Computing one point in each connected component of a smooth real algebraic set
   - Problem statement
   - Polar varieties
   - The algorithm
   - Weak transversality
   - Quantitative genericity statements
   - Proving the main result
2. Deciding connectivity queries in smooth and bounded real hypersurfaces
   - Problem statement
   - Other work on roadmap computation
   - Estimating the height of the output

Weak transversality

Thom's weak transversality theorem

- Generalizes Sard's lemma: *the set of critical values of a smooth function $\mathbb{R}^n \to \mathbb{R}^m$ have measure zero.*
  - Algebraic versions exist for which the sets of critical values are contained in algebraic sets in the codomain.
- We develop a quantitative version which allows us to bound the degrees of the hypersurfaces we have to avoid.
- The bad parameters show up as the critical values of a smooth function.

Weak transversality

- Let n, s, and m be positive integers, with $m \leq n$, and let

$$\mathbf{\Phi} : \mathbb{C}^n \times \mathbb{C}^s \ \to \mathbb{C}^m$$

be a mapping defined by polynomials in $\mathbb{C}[\boldsymbol{X}, \boldsymbol{\Theta}]$.

- For $\boldsymbol{\vartheta}$ in $\mathbb{C}^s$, let

$$\begin{aligned} \mathbf{\Phi}_{\boldsymbol{\vartheta}} : \mathbb{C}^n &\to \mathbb{C}^m \\ \boldsymbol{x} &\mapsto \mathbf{\Phi}(\boldsymbol{x}, \boldsymbol{\vartheta}). \end{aligned}$$

- A point $\boldsymbol{z}$ is a regular value of $\mathbf{\Phi}$ iff for all $(\boldsymbol{y}, \boldsymbol{\vartheta})$ with $\mathbf{\Phi}(\boldsymbol{y}, \boldsymbol{\vartheta}) = \boldsymbol{z}$, the Jacobian of $\mathbf{\Phi}$ has full rank at $(\boldsymbol{y}, \boldsymbol{\vartheta})$.

Proposition (weak transversality)

- Suppose that $\mathbf{0}$ is a regular value of $\mathbf{\Phi}$. Then there exists a non-zero polynomial $\Gamma \in \mathbb{C}[\boldsymbol{\Theta}]$ of degree at most d^{m+n} such that for $\boldsymbol{\vartheta}$ in $\mathbb{C}^s$, if $\Gamma(\boldsymbol{\vartheta}) \neq 0$, then $\mathbf{0}$ is a regular value of $\mathbf{\Phi}_{\boldsymbol{\vartheta}}$.

Our contribution is the degree estimate.

Example

- Consider $f \in \mathbb{C}[X_1, X_2]$, squarefree, $\deg(f) \leq d$ and $V(f) \subset \mathbb{C}^2$ smooth.
- Let the mapping $\mathbf{\Phi} : \mathbb{C}^2 \times \mathbb{C} \to \mathbb{C}^2$ be defined by

$$\mathbf{\Phi}(X_1, X_2, \Theta) = (X_1 - \Theta, f(X_1, X_2)).$$

- The Jacobian of $\mathbf{\Phi}$ has rank two at any point in $\mathbf{\Phi}^{-1}(\mathbf{0})$:

$$\mathrm{jac}(\mathbf{\Phi}) = \begin{bmatrix} 1 & 0 & -1 \\ \partial f/\partial X_1 & \partial f/\partial X_2 & 0 \end{bmatrix}.$$

  - The assumptions of the proposition apply.

Example (continued)

- Thus $\Gamma \in \mathbb{C}[\Theta]$ exists, with $\deg(\Gamma) \le d^4$, such that when $\Gamma(\vartheta) \neq \boldsymbol{0}$ then $\boldsymbol{0}$ is a regular value of
$$\mathbf{\Phi}_\vartheta(X_1, X_2) = (X_1 - \vartheta, f(X_1, X_2)).$$
- The Jacobian of $\mathbf{\Phi}_{\boldsymbol{\vartheta}}$ has rank two at any point in $\mathbf{\Phi}_{\boldsymbol{\vartheta}}^{-1}(0)$:
$$\mathrm{jac}(\mathbf{\Phi}_{\boldsymbol{\vartheta}}) = \begin{bmatrix} 1 & 0 \\ \partial f/\partial X_1 & \partial f/\partial X_2 \end{bmatrix}.$$
- By the Jacobian Criterion, the ideal $(X_1 - \vartheta, f(X_1, X_2))$ is radical; equivalently, $f(\vartheta, X_2)$ is squarefree.
  - For all ϑ in $\mathbb{C}$ except at most d^4 values.
- Note that using the discriminant of f with respect to X_2 produces the same result.
- This examples illustrates how we apply the result when solving the equations in the main algorithm.

Example (continued)

Compare with the equations solved in the main algorithm

- In the example, $\mathbf{\Phi} : \mathbb{C}^2 \times \mathbb{C} \to \mathbb{C}^2$ is defined by the polynomials

$$X_1 - \Theta, f(X_1, X_2).$$

- Compare with the equations we solve in the main algorithm: (for $i = 1 \ldots, n - p + 1$)

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, \left(F, [L_1 \cdots L_p] \cdot \mathrm{jac}(F, i), \sum_{i=1}^{p} u_i L_i - 1 \right).$$

- Following the same steps as in the example, we bound the degree of a polynomial such that if $\boldsymbol{\sigma}$ is not a zero then these equations have finitely many solutions.

Outline

1. Computing one point in each connected component of a smooth real algebraic set
   - Problem statement
   - Polar varieties
   - The algorithm
   - Weak transversality
   - Quantitative genericity statements
   - Proving the main result
2. Deciding connectivity queries in smooth and bounded real hypersurfaces
   - Problem statement
   - Other work on roadmap computation
   - Estimating the height of the output

Genericity properties

- Let $F = (f_1, \dots, f_p) \in \mathbb{C}[X_1, \dots, X_n]^p$.
- For $i = 1, \dots, n - p + 1$,

F satisfies $\boldsymbol{H}_i$ if

1. $W(i, V(F))$ is either empty or $(i-1)$-equidimensional.
2. The Jacobian matrix of the polynomials

$$\big(F, [L_1 \cdots L_p] \cdot \mathrm{jac}(F, i)\big)$$

   has full rank at any $(\boldsymbol{x}, \boldsymbol{l})$ that cancels equations.
3. $W(i, V(F))$ is either empty or in Noether position for π_{i-1}.

Noether position

- An equidimensional algebraic set $X \subset \mathbb{C}^n$ of dimension d is in Noether position for the projection
$$\pi_d : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_d)$$
when the extension
$$\mathbb{C}[X_1, \ldots, X_d] \to \mathbb{C}[X_1, \ldots, X_n]/I(X)$$
is integral.
- Consequently, for any $\boldsymbol{x} \in \mathbb{C}^d$, the fiber $X \cap \pi_d^{-1}(\boldsymbol{x})$ has dimension zero (so it is finite and not empty).

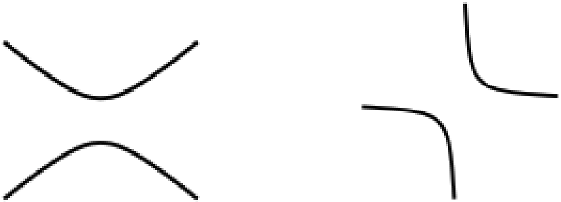


Figure 1: X is in Noether position for π_1 on the left, but not on the right.

- Let $F = (f_1, \ldots, f_p) \in \mathbb{C}[X_1, \ldots, X_n]^p$.
- For $i = 1, \ldots, n - p + 1$,

F satisfies $\boldsymbol{H}_i$ if

1. $W(i, V(F))$ is either empty or $(i-1)$-equidimensional.
2. The Jacobian matrix of the polynomials

$$\big(F, [L_1 \ldots L_p] \cdot \mathrm{jac}(F, i)\big)$$

   has full rank at any $(\boldsymbol{x}, \boldsymbol{l})$ that cancels equations.
3. $W(i, V(F))$ is either empty or in Noether position for π_{i-1}.

Note that $W(i, V(F^{\boldsymbol{A}}))$ may not equal $W(i, V(F))^{\boldsymbol{A}}$, as, for instance, their dimensions may vary.

- For $i = 1, \ldots, n-p+1$, if F satisfies $\boldsymbol{H}_i$, then given $\boldsymbol{\sigma}$ in $\mathbb{Z}^{i-1}$, we further say

F and $\boldsymbol{\sigma}$ satisfy $\boldsymbol{H}_i^{'}$ if

1. 0 is a regular value of the polynomials

$$\big(X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, F, [L_1 \cdots L_p] \cdot \mathrm{jac}(F, i)\big),$$

in the open set defined by $(L_1 \cdots L_p) \neq (0 \cdots 0)$.

- For $i = 1, \dots, n-p+1$, if F satisfies $\boldsymbol{H}_i$, and F and $\boldsymbol{\sigma}$ satisfy $\boldsymbol{H}'_i$, then given $\boldsymbol{u} \in \mathbb{C}^p$ we further say

$\boldsymbol{u}$ satisfies $\boldsymbol{H}''_i$ if

1. $\boldsymbol{u}$ is such that the projections on the $\boldsymbol{X}$-space of the solutions of

$$X_1 - \sigma_1, \dots, X_{i-1} - \sigma_{i-1}, \left(F, [L_1 \cdots L_p] \cdot \mathrm{jac}(F, i), \sum_{i=1}^{p} u_i L_i - 1\right) \tag{1}$$

are the solutions of

$$X_1 - \sigma_1, \dots, X_{i-1} - \sigma_{i-1}, \left(F, M_{i,1}, \dots, M_{i,S_i}\right). \tag{2}$$

Genericity statements

Proposition

- There exists a polynomial

$$\Delta_1 \in \mathbb{C}[(\mathfrak{A}_{j,k})_{1 \leq j,k \leq n}]$$

of degree at most $5n^3(2d)^{5n}$ such that if $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ does not cancel Δ_1, then $\boldsymbol{A}$ is invertible and $F^{\boldsymbol{A}} = F(\boldsymbol{AX})$ satisfies $\boldsymbol{H}_i$:

1. $W(i, V(F))$ is either empty or $(i-1)$-equidimensional.
2. The Jacobian matrix of
$$\big(F, [L_1 \cdots L_p] \cdot \mathrm{jac}(F, i)\big)$$
has full rank at any $(\boldsymbol{x}, \boldsymbol{l})$ that cancels equations.
3. $W(i, V(F))$ is either empty or in Noether position for π_{i-1}.

For all $i \in \{1, \ldots, n-p+1\}$.

Genericity statements

Proposition

- Suppose that $F = (f_1, \dots, f_p)$ satisfies $\boldsymbol{H}_i$ for all $i = 1, \dots, n - p + 1$.
- There exists a polynomial
$$\Delta_2 \in \mathbb{C}[S_1, \dots, S_{i-1}]$$
of degree at most nd^{4n} such that if $\boldsymbol{\sigma} \in \mathbb{C}^{i-1}$ does not cancel Δ_2, then F and $\boldsymbol{\sigma}$ satisfy $\boldsymbol{H}'_i$:
  1. 0 is a regular value of the polynomials
  $$\big(X_1 - \sigma_1, \dots, X_{i-1} - \sigma_{i-1}, F, [L_1 \cdots L_p] \cdot \mathrm{jac}(F, i)\big),$$
  in the open set defined by $[L_1 \cdots L_s] \neq [0 \cdots 0]$.

For all $i \in \{1, \dots, n - p + 1\}$.

Proposition

- Suppose that F satisfies $\boldsymbol{H}_i$ and F and $\boldsymbol{\sigma}$ satisfy $\boldsymbol{H}_i^{'}$, for all $i \in \{1, \ldots, n-p+1\}$.
- There exists a polynomial

$$\Delta_3 \in \mathbb{C}[T_1, \ldots, T_p]$$

of degree at most $n(n(d-1))^n$ such that if $\boldsymbol{u} \in \mathbb{C}^p$ does not cancel Δ_3, then $\boldsymbol{u}$ satisfies $\boldsymbol{H}_i''$:

1. $\boldsymbol{u}$ is such that the projections on the $\boldsymbol{X}$-space of the solutions of

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, \left(F, [L_1 \cdots L_p] \cdot \mathrm{jac}(F, i), \sum_{i=1}^{p} u_i L_i - 1\right) \qquad (1)$$

are the solutions of

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, \left(F, M_{i,1}, \ldots, M_{i,S_i}\right). \qquad (2)$$

For all $i \in \{1, \ldots, n-p+1\}$.

Outline

Proving the main result

1. The algorithm first randomly chooses $\boldsymbol{A} \in \mathbb{Z}^{n\times n}$. Using the degree bound for Δ_1, the entries of $\boldsymbol{A}$ are chosen from a sufficiently large set so that by the Schwartz–Zippel lemma
$$\mathbb{P}[\Delta_1(\boldsymbol{A}) = 0] \leq 1 - \epsilon.$$
2. Next, the algorithm chooses $\boldsymbol{\sigma} \in \mathbb{Z}^{n-p}$ at random and we again quantify using the Schwartz–Zippel lemma: we bound
$$\mathbb{P}[\Delta_2(\boldsymbol{\sigma}) = 0 \mid \Delta_1(\boldsymbol{A}) \neq 0] \leq 1 - \epsilon.$$
3. Finally, the algorithm randomly chooses $\boldsymbol{u} \in \mathbb{Z}^p$ and we quantify once more using the Schwartz–Zippel lemma: we bound
$$\mathbb{P}[\Delta_3(\boldsymbol{u}) = 0 \mid \Delta_1(\boldsymbol{A})\Delta_2(\boldsymbol{\sigma}) \neq 0] \leq 1 - \epsilon.$$

Outline

Problem statement

Roadmaps

- A roadmap $\mathscr{R}$ for an algebraic set X is a curve with non-empty and connected intersection with all connected components of X.

Applications

- Deciding connectivity queries.
- Robot motion planning.

Problem 2

- Let f be a squarefree polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ such that $V(f)$ has a finite number of singular points and $V(f) \cap \mathbb{R}^n$ is bounded.
- Compute a roadmap $\mathscr{R}$ of $V(f) \cap \mathbb{R}^n$.

Starting point

- Another algorithm by [Safey El Din, Schost, 2011].
  - Also uses random changes of variables proven to generically ensure weak transversality and Noether position.
  - Recursive algorithm based on calculating polar curves of polar varieties.
  - Cost given in an algebraic complexity model:

$$(nd)^{O(n^{1.5})} \text{ operations in } \mathbb{Q}.$$

Contributions (ongoing)

- Determining the bit complexity and error probability.
- Giving a quantitative analysis of the genericity properties.
  - Weak transversality (reusing techniques from previous analysis).
  - Noether normalization for polar varieties (reusing techniques from previous analysis).
  - Additional genericity properties.

Another genericity property

- Let $F = (f_1, \ldots, f_p) \in \mathbb{Z}[X_1, \ldots, X_n]^p$ with degree $f_i \leq d$. Suppose the F defines a radical ideal and $V(F)$ is equidimensional of dimension $n - p$ with a finite number of singular points and $V(F) \cap \mathbb{R}^n$ bounded.
- For $i = 2, \ldots, (n - p + 3)/2$,

F satisfies $\boldsymbol{G}_i$ if

- $W(1, W(i, V(F)))$ is finite.

  - Proven to hold generically in [Safey El Din, Schost, 2011].

Proposition

- There exists a hypersurface $\Delta \subset \mathbb{C}[(\mathfrak{A}_{j,k})_{1 \leq j,k \leq n}]$ with degree at most

$$n(p+n)^n (2d)^{p+n}$$

with the property that if $\Delta(\boldsymbol{A}) \neq 0$ then $F^{\boldsymbol{A}} = F(\boldsymbol{A}\boldsymbol{X})$ satisfies $\boldsymbol{G}_i$, for all $i \in \{2, \ldots, (n - p + 3)/2\}$.

Outline

Other work on roadmap computation

- $d^{O(n^4)}$, deterministic, semi-algebraic sets, no assumptions [Canny, 1987]
- $d^{O(n^2)}$, randomized, semi-algebraic sets, no assumptions [Canny, 1987]

Other work on roadmap computation

- $d^{O(n^4)}$, deterministic, semi-algebraic sets, no assumptions [Canny, 1987]
- $d^{O(n^2)}$, randomized, semi-algebraic sets, no assumptions [Canny, 1987]
- $d^{O(n^2)}$, deterministic, semi-algebraic sets, no assumptions [Basu, Pollack, Roy, 1999]

Other work on roadmap computation

- $d^{O(n^4)}$, deterministic, semi-algebraic sets, no assumptions [Canny, 1987]
- $d^{O(n^2)}$, randomized, semi-algebraic sets, no assumptions [Canny, 1987]
- $d^{O(n^2)}$, deterministic, semi-algebraic sets, no assumptions [Basu, Pollack, Roy, 1999]

- $(nd)^{O(n^{1.5})}$, randomized, real hypersurfaces, smooth and bounded [Safey El Din, Schost, 2011]
- $d^{O(n^{1.5})}$, deterministic, real algebraic sets, no assumptions [Basu, Roy, Safey El Din, Schost, 2014]

Other work on roadmap computation

- $d^{O(n^4)}$, deterministic, semi-algebraic sets, no assumptions
  [Canny, 1987]
- $d^{O(n^2)}$, randomized, semi-algebraic sets, no assumptions
  [Canny, 1987]
- $d^{O(n^2)}$, deterministic, semi-algebraic sets, no assumptions
  [Basu, Pollack, Roy, 1999]

- $(nd)^{O(n^{1.5})}$, randomized, real hypersurfaces, smooth and bounded
  [Safey El Din, Schost, 2011]
- $d^{O(n^{1.5})}$, deterministic, real algebraic sets, no assumptions
  [Basu, Roy, Safey El Din, Schost, 2014]

- $(nd)^{O^{\sim}(n)}$, deterministic, real hypersurfaces, no assumptions
  [Basu, Roy, 2014]

Other work on roadmap computation

- $d^{O(n^4)}$, deterministic, semi-algebraic sets, no assumptions
  [Canny, 1987]
- $d^{O(n^2)}$, randomized, semi-algebraic sets, no assumptions
  [Canny, 1987]
- $d^{O(n^2)}$, deterministic, semi-algebraic sets, no assumptions
  [Basu, Pollack, Roy, 1999]

- $(nd)^{O(n^{1.5})}$, randomized, real hypersurfaces, smooth and bounded
  [Safey El Din, Schost, 2011]
- $d^{O(n^{1.5})}$, deterministic, real algebraic sets, no assumptions
  [Basu, Roy, Safey El Din, Schost, 2014]

- $(nd)^{O^{\sim}(n)}$, deterministic, real hypersurfaces, no assumptions
  [Basu, Roy, 2014]
- $(nd)^{O(n \log d)}$, real algebraic sets, smooth and bounded
  [Safey El Din, Schost, 2017]

Other work on roadmap computation

- $d^{O(n^4)}$, deterministic, semi-algebraic sets, no assumptions [Canny, 1987]
- $d^{O(n^2)}$, randomized, semi-algebraic sets, no assumptions [Canny, 1987]
- $d^{O(n^2)}$, deterministic, semi-algebraic sets, no assumptions [Basu, Pollack, Roy, 1999]

- $(nd)^{O(n^{1.5})}$, randomized, real hypersurfaces, smooth and bounded [Safey El Din, Schost, 2011]
- $d^{O(n^{1.5})}$, deterministic, real algebraic sets, no assumptions [Basu, Roy, Safey El Din, Schost, 2014]

- $(nd)^{O^{\sim}(n)}$, deterministic, real hypersurfaces, no assumptions [Basu, Roy, 2014]
- $(nd)^{O(n \log d)}$, real algebraic sets, smooth and bounded [Safey El Din, Schost, 2017]
- $(nd)^{O(n \log d)}$, real algebraic sets, smooth (unbounded) [Prebet, Safey El Din, Schost, 2022]

Outline

1. Computing one point in each connected component of a smooth real algebraic set
   - Problem statement
   - Polar varieties
   - The algorithm
   - Weak transversality
   - Quantitative genericity statements
   - Proving the main result
2. Deciding connectivity queries in smooth and bounded real hypersurfaces
   - Problem statement
   - Other work on roadmap computation
   - Estimating the height of the output

Height of the output

- Algebraic complexity and degree of the output: $(nd)^{O(n^{1.5})}$.
- Expect height to be $(nd)^{O(n^{1.5})}$.

Difficulties

- Need to solve polynomial equations with a special shape.
- Two blocks of variables subject to different constraints:
  - $X_1, \ldots, X_i$, high degree and bit-size.
  - $X_{i+1}, \ldots, X_n$, low degree and bit-size.
- Classical arithmetic Bézout gives height $(nd)^{O(n^2)}$.

Solutions

- Multi-projective height techniques that involve the arithmetic Chow ring [Krick, Sombra, D'Andrea, 2012] precisely allow you to handle the two blocks separately.
- We get height $(nd)^{O(n^{1.5})}$.

Thank you.