Lower Bounds for Zero-Dimensional Projections

W. Dale Brownawell[1] Chee K. Yap[2,3]

[1]Department of Mathematics
Penn State University
University Park, PA 16802, USA
and
[2]Courant Institute of Mathematical Sciences
New York University
New York, NY 10012, USA
and
[3]School of Computational Science
Korea Institute of Advanced Study (KIAS)
Seoul, Korea

34th ISSAC, July 28–31, 2009

Lower Bounds for Zero-Dimensional Projections

Abstract

Let I be an ideal generated by polynomials $P_1, \ldots, P_m \in \mathbb{Z}[X_1, \ldots, X_n]$, and $\mathfrak{P}$ be an isolated prime component of I. If the projection of $\textsc{Zero}(\mathfrak{P}) \subseteq \mathbb{C}^n$ onto the first coordinate is a finite set, and $\overline{\zeta} = (\zeta_1, \ldots, \zeta_n) \in \textsc{Zero}(\mathfrak{P})$ where $\zeta_1 \neq 0$, then we prove a lower bound on $|\zeta_1|$ in terms of n, m and the maximum degree D and maximum height H of the polynomials.

Overview of Talk

- Introduction
- Main Result
- Applications
- Conclusion

Coming Up Next

What is the Main Result?

A Projection Zero Bound

Suppose $V \subseteq \mathbb{C}^n$ is an algebraic set whose projection $\Pi_1(V)$ is zero-dimensional. Let $(\zeta_1, \ldots, \zeta_n) \in V$ where $\zeta_1 \neq 0$.
Then we prove a lower bound on $|\zeta_1|$ in terms of n, and in the size m, maximum degree D and maximum height H of any set of polynomials defining V.

Previous Bounds

- Canny (1990) provided such a bound when $m = n$ and the projective variety $\widehat{V} \subseteq \mathbb{P}^n(\mathbb{C})$ is zero-dimensional.
- Yap (2000) relaxed Canny's zero-dimensional requirement, only requiring the affine part V to be zero-dimensional.
- Now, we allow any number m of polynomials, and relax the zero-dimensional requirement to only the component of interest.

What is the Main Result?

A Projection Zero Bound

Suppose $V \subseteq \mathbb{C}^n$ is an algebraic set whose projection $\Pi_1(V)$ is zero-dimensional. Let $(\zeta_1, \ldots, \zeta_n) \in V$ where $\zeta_1 \neq 0$.
Then we prove a lower bound on $|\zeta_1|$ in terms of n, and in the size m, maximum degree D and maximum height H of any set of polynomials defining V.

Previous Bounds

- Canny (1990) provided such a bound when $m = n$ and the projective variety $\widehat{V} \subseteq \mathbb{P}^n(\mathbb{C})$ is zero-dimensional.
- Yap (2000) relaxed Canny's zero-dimensional requirement, only requiring the affine part V to be zero-dimensional.
- Now, we allow any number m of polynomials, and relax the zero-dimensional requirement to only the component of interest.

What is the Main Result?

A Projection Zero Bound

Suppose $V \subseteq \mathbb{C}^n$ is an algebraic set whose projection $\Pi_1(V)$ is zero-dimensional. Let $(\zeta_1, \ldots, \zeta_n) \in V$ where $\zeta_1 \neq 0$.
Then we prove a lower bound on $|\zeta_1|$ in terms of n, and in the size m, maximum degree D and maximum height H of any set of polynomials defining V.

Previous Bounds

- Canny (1990) provided such a bound when $m = n$ and the projective variety $\widehat{V} \subseteq \mathbb{P}^n(\mathbb{C})$ is zero-dimensional.
- Yap (2000) relaxed Canny's zero-dimensional requirement, only requiring the affine part V to be zero-dimensional.
- Now, we allow any number m of polynomials, and relax the zero-dimensional requirement to only the component of interest.

What is the Main Result?

A Projection Zero Bound

Suppose $V \subseteq \mathbb{C}^n$ is an algebraic set whose projection $\Pi_1(V)$ is zero-dimensional. Let $(\zeta_1, \ldots, \zeta_n) \in V$ where $\zeta_1 \neq 0$.
Then we prove a lower bound on $|\zeta_1|$ in terms of n, and in the size m, maximum degree D and maximum height H of any set of polynomials defining V.

Previous Bounds

- Canny (1990) provided such a bound when $m = n$ and the projective variety $\widehat{V} \subseteq \mathbb{P}^n(\mathbb{C})$ is zero-dimensional.
- Yap (2000) relaxed Canny's zero-dimensional requirement, only requiring the affine part V to be zero-dimensional.
- Now, we allow any number m of polynomials, and relax the zero-dimensional requirement to only the component of interest.

What is the Main Result?

A Projection Zero Bound

Suppose $V \subseteq \mathbb{C}^n$ is an algebraic set whose projection $\Pi_1(V)$ is zero-dimensional. Let $(\zeta_1, \ldots, \zeta_n) \in V$ where $\zeta_1 \neq 0$.
Then we prove a lower bound on $|\zeta_1|$ in terms of n, and in the size m, maximum degree D and maximum height H of any set of polynomials defining V.

Previous Bounds

- Canny (1990) provided such a bound when $m = n$ and the projective variety $\widehat{V} \subseteq \mathbb{P}^n(\mathbb{C})$ is zero-dimensional.
- Yap (2000) relaxed Canny's zero-dimensional requirement, only requiring the affine part V to be zero-dimensional.
- Now, we allow any number m of polynomials, and relax the zero-dimensional requirement to only the component of interest.

What is the Main Result?

A Projection Zero Bound

Suppose $V \subseteq \mathbb{C}^n$ is an algebraic set whose projection $\Pi_1(V)$ is zero-dimensional. Let $(\zeta_1, \ldots, \zeta_n) \in V$ where $\zeta_1 \neq 0$.
Then we prove a lower bound on $|\zeta_1|$ in terms of n, and in the size m, maximum degree D and maximum height H of any set of polynomials defining V.

Previous Bounds

- Canny (1990) provided such a bound when $m = n$ and the projective variety $\widehat{V} \subseteq \mathbb{P}^n(\mathbb{C})$ is zero-dimensional.
- Yap (2000) relaxed Canny's zero-dimensional requirement, only requiring the affine part V to be zero-dimensional.
- Now, we allow any number m of polynomials, and relax the zero-dimensional requirement to only the component of interest.

Why We Need Bounds in Algebraic Computation

In Computational Science and Engineering (CS&E), geometric problems are posed in the continuum (say $\mathbb{R}^n$)

- What does this mean?
- E.g., we are interested in $\text{ZERO}(f_1, \ldots, f_m) \subseteq \mathbb{R}^n$, NOT the ideal $(f_1, \ldots, f_m) \subseteq \mathbb{Z}[X_1, \ldots, X_n]$
- Further, we prefer $\text{ZERO}(X^2 - 3) \approx \{\pm 1.732\}$ to $\text{ZERO}(X^2 - 3) = \{\pm\sqrt{3}\}$
- I.e., we are interested in embedding of $\text{ZERO}(f_1, \ldots, f_m)$ in $\mathbb{R}^n$

  Conclusion 1: we need numerical computation

Why We Need Bounds in Algebraic Computation

In Computational Science and Engineering (CS&E), geometric problems are posed in the continuum (say $\mathbb{R}^n$)

- What does this mean?
- E.g., we are interested in $\text{ZERO}(f_1, \ldots, f_m) \subseteq \mathbb{R}^n$, NOT the ideal $(f_1, \ldots, f_m) \subseteq \mathbb{Z}[X_1, \ldots, X_n]$
- Further, we prefer $\text{ZERO}(X^2 - 3) \approx \{\pm 1.732\}$ to $\text{ZERO}(X^2 - 3) = \{\pm\sqrt{3}\}$
- I.e., we are interested in embedding of $\text{ZERO}(f_1, \ldots, f_m)$ in $\mathbb{R}^n$

Conclusion 1: we need numerical computation

Why We Need Bounds in Algebraic Computation

In Computational Science and Engineering (CS&E), geometric problems are posed in the continuum (say $\mathbb{R}^n$)

- What does this mean?
- E.g., we are interested in $\text{Zero}(f_1, \ldots, f_m) \subseteq \mathbb{R}^n$, NOT the ideal $(f_1, \ldots, f_m) \subseteq \mathbb{Z}[X_1, \ldots, X_n]$
- Further, we prefer $\text{Zero}(X^2 - 3) \approx \{\pm 1.732\}$ to $\text{Zero}(X^2 - 3) = \{\pm\sqrt{3}\}$
- I.e., we are interested in embedding of $\text{Zero}(f_1, \ldots, f_m)$ in $\mathbb{R}^n$

Conclusion 1: we need numerical computation

Why We Need Bounds in Algebraic Computation

In Computational Science and Engineering (CS&E), geometric problems are posed in the continuum (say $\mathbb{R}^n$)

- What does this mean?
- E.g., we are interested in $\text{Zero}(f_1, \ldots, f_m) \subseteq \mathbb{R}^n$, NOT the ideal $(f_1, \ldots, f_m) \subseteq \mathbb{Z}[X_1, \ldots, X_n]$
- Further, we prefer $\text{Zero}(X^2 - 3) \approx \{\pm 1.732\}$ to $\text{Zero}(X^2 - 3) = \{\pm\sqrt{3}\}$
- I.e., we are interested in embedding of $\text{Zero}(f_1, \ldots, f_m)$ in $\mathbb{R}^n$

Conclusion 1: we need numerical computation

Why We Need Bounds in Algebraic Computation

In Computational Science and Engineering (CS&E), geometric problems are posed in the continuum (say $\mathbb{R}^n$)

- What does this mean?
- E.g., we are interested in $\text{ZERO}(f_1, \ldots, f_m) \subseteq \mathbb{R}^n$, NOT the ideal $(f_1, \ldots, f_m) \subseteq \mathbb{Z}[X_1, \ldots, X_n]$
- Further, we prefer $\text{ZERO}(X^2 - 3) \approx \{\pm 1.732\}$ to $\text{ZERO}(X^2 - 3) = \{\pm\sqrt{3}\}$
- I.e., we are interested in embedding of $\text{ZERO}(f_1, \ldots, f_m)$ in $\mathbb{R}^n$

Conclusion 1: we need numerical computation

Why We Need Bounds in Algebraic Computation

In Computational Science and Engineering (CS&E), geometric problems are posed in the continuum (say $\mathbb{R}^n$)

- What does this mean?
- E.g., we are interested in $\text{ZERO}(f_1, \ldots, f_m) \subseteq \mathbb{R}^n$, NOT the ideal $(f_1, \ldots, f_m) \subseteq \mathbb{Z}[X_1, \ldots, X_n]$
- Further, we prefer $\text{ZERO}(X^2 - 3) \approx \{\pm 1.732\}$ to $\text{ZERO}(X^2 - 3) = \{\pm\sqrt{3}\}$
- I.e., we are interested in embedding of $\text{ZERO}(f_1, \ldots, f_m)$ in $\mathbb{R}^n$

Conclusion 1: we need numerical computation

What Else?

But we are also interested in exact geometry

- E.g., the approximation of $\text{ZERO}(f_1, \ldots, f_m)$ must preserve geometric/topological properties
- Such properties are determined by zeros
- Conclusion 2: Our approximations must suffice to decide zero
- This depends on zero bounds
- Better bounds $\Rightarrow$ Faster Algorithms

Stripped-down Algebraic Properties

- E.g., Zero bounds (in lieu of resultant computation)
- E.g., Parity (odd/even) of zeros (in lieu of of multiplicities) [Cheng-Gao-Y. ISSAC'07]

What Else?

But we are also interested in exact geometry

- E.g., the approximation of $\text{ZERO}(f_1, \ldots, f_m)$ must preserve geometric/topological properties
- Such properties are determined by zeros
- Conclusion 2: Our approximations must suffice to decide zero
- This depends on zero bounds
- Better bounds $\Rightarrow$ Faster Algorithms

Stripped-down Algebraic Properties

- E.g., Zero bounds (in lieu of resultant computation)
- E.g., Parity (odd/even) of zeros (in lieu of of multiplicities) [Cheng-Gao-Y. ISSAC'07]

What Else?

But we are also interested in exact geometry

- E.g., the approximation of $\text{ZERO}(f_1, \ldots, f_m)$ must preserve geometric/topological properties
- Such properties are determined by zeros
- Conclusion 2: Our approximations must suffice to decide zero
- This depends on zero bounds
- Better bounds $\Rightarrow$ Faster Algorithms

Stripped-down Algebraic Properties

- E.g., Zero bounds (in lieu of resultant computation)
- E.g., Parity (odd/even) of zeros (in lieu of of multiplicities) [Cheng-Gao-Y. ISSAC'07]

What Else?

But we are also interested in exact geometry

- E.g., the approximation of $\text{ZERO}(f_1, \ldots, f_m)$ must preserve geometric/topological properties
- Such properties are determined by zeros
- Conclusion 2: Our approximations must suffice to decide zero
- This depends on zero bounds
- Better bounds $\Rightarrow$ Faster Algorithms

Stripped-down Algebraic Properties

- E.g., Zero bounds (in lieu of resultant computation)
- E.g., Parity (odd/even) of zeros (in lieu of of multiplicities) [Cheng-Gao-Y. ISSAC'07]

What Else?

But we are also interested in exact geometry

- E.g., the approximation of $\text{ZERO}(f_1, \ldots, f_m)$ must preserve geometric/topological properties
- Such properties are determined by zeros
- Conclusion 2: Our approximations must suffice to decide zero
- This depends on zero bounds
- Better bounds $\Rightarrow$ Faster Algorithms

Stripped-down Algebraic Properties

- E.g., Zero bounds (in lieu of resultant computation)
- E.g., Parity (odd/even) of zeros (in lieu of of multiplicities) [Cheng-Gao-Y. ISSAC'07]

What Else?

But we are also interested in exact geometry

- E.g., the approximation of $\text{ZERO}(f_1, \ldots, f_m)$ must preserve geometric/topological properties
- Such properties are determined by zeros
- Conclusion 2: Our approximations must suffice to decide zero
- This depends on zero bounds
- Better bounds $\Rightarrow$ Faster Algorithms

Stripped-down Algebraic Properties

- E.g., Zero bounds (in lieu of resultant computation)
- E.g., Parity (odd/even) of zeros (in lieu of of multiplicities) [Cheng-Gao-Y. ISSAC'07]

What Else?

But we are also interested in exact geometry

- E.g., the approximation of $\mathrm{ZERO}(f_1, \ldots, f_m)$ must preserve geometric/topological properties
- Such properties are determined by zeros
- Conclusion 2: Our approximations must suffice to decide zero
- This depends on zero bounds
- Better bounds $\Rightarrow$ Faster Algorithms

Stripped-down Algebraic Properties

- E.g., Zero bounds (in lieu of resultant computation)
- E.g., Parity (odd/even) of zeros (in lieu of of multiplicities) [Cheng-Gao-Y. ISSAC'07]

What Else?

But we are also interested in exact geometry

- E.g., the approximation of $\text{ZERO}(f_1, \ldots, f_m)$ must preserve geometric/topological properties
- Such properties are determined by zeros
- Conclusion 2: Our approximations must suffice to decide zero
- This depends on zero bounds
- Better bounds $\Rightarrow$ Faster Algorithms

Stripped-down Algebraic Properties

- E.g., Zero bounds (in lieu of resultant computation)
- E.g., Parity (odd/even) of zeros (in lieu of of multiplicities) [Cheng-Gao-Y. ISSAC'07]

What Else?

But we are also interested in exact geometry

- E.g., the approximation of $\text{ZERO}(f_1, \ldots, f_m)$ must preserve geometric/topological properties
- Such properties are determined by zeros
- Conclusion 2: Our approximations must suffice to decide zero
- This depends on zero bounds
- Better bounds $\Rightarrow$ Faster Algorithms

Stripped-down Algebraic Properties

- E.g., Zero bounds (in lieu of resultant computation)
- E.g., Parity (odd/even) of zeros (in lieu of of multiplicities) [Cheng-Gao-Y. ISSAC'07]

Coming Up Next

Statement of Main Result

Theorem (Main Result)

Let $I := (P_1, \ldots, P_m) \subseteq \mathbb{Z}[X_1, \ldots, X_n]$.
Let $\mathfrak{P}$ *be an isolated prime component of* I *with* $\Pi_1(\textsc{Zero}(\mathfrak{P}))$ *a finite set.*
If $(\zeta_1, \ldots, \zeta_n) \in \textsc{Zero}(\mathfrak{P})$ *with* $\zeta_1 \neq 0$, *then*

$$|\zeta_1| \geq ((n+1)^2 e^{n+2})^{-n(n+1)D^{n-d}} (d^{n-d-1} m H)^{-(n-d)D^{n-d-1}}$$

where $\dim \mathfrak{P} = d$, $H \geq \mathit{Height}(P_i)$ *and* $D \geq \deg(P_i)$.

Tools in Proof (Sketch)

- From transcendental number theory
- Let $\mathfrak{P} \subseteq \mathbb{Z}[X_0, \ldots, X_n] =: A$ be homogeneous prime ideal of dimension d.
- (Nesterenko) Chow forms of $\mathfrak{P}$ is polynomial $F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}}$ is irreducible in $\mathbb{Z}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}} = 0$ iff $d+1$ generic hyperplanes intersect at a zero of $\mathfrak{P}$
- Degree of $\mathfrak{P}$ is g, the degree of $F_{\mathfrak{P}}$ in $\overline{u}_0$.
- Chow form factors in suitable extension field into a product of g linear forms, $F_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} \overline{\alpha}^{(i)} \cdot \overline{u}_d$.
- (Nesterenko) The resultant of $F_{\mathfrak{P}}$ and $Q \in \mathbb{Z}[X_0, \ldots, X_n]$ is $\mathtt{res}(F_{\mathfrak{P}}, Q) := a(\overline{u}_0, \ldots, \overline{u}_{d-1})^{\deg Q} \prod_{i=1}^{g} Q(\overline{\alpha}^{(i)})$.

Tools in Proof (Sketch)

- From transcendental number theory
- Let $\mathfrak{P} \subseteq \mathbb{Z}[X_0, \ldots, X_n] =: A$ be homogeneous prime ideal of dimension d.
- (Nesterenko) Chow forms of $\mathfrak{P}$ is polynomial $F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}}$ is irreducible in $\mathbb{Z}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}} = 0$ iff $d+1$ generic hyperplanes intersect at a zero of $\mathfrak{P}$
- Degree of $\mathfrak{P}$ is g, the degree of $F_{\mathfrak{P}}$ in $\overline{u}_0$.
- Chow form factors in suitable extension field into a product of g linear forms, $F_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} \overline{\alpha}^{(i)} \cdot \overline{u}_d$.
- (Nesterenko) The resultant of $F_{\mathfrak{P}}$ and $Q \in \mathbb{Z}[X_0, \ldots, X_n]$ is $\mathtt{res}(F_{\mathfrak{P}}, Q) := a(\overline{u}_0, \ldots, \overline{u}_{d-1})^{\deg Q} \prod_{i=1}^{g} Q(\overline{\alpha}^{(i)})$.

Tools in Proof (Sketch)

- From transcendental number theory
- Let $\mathfrak{P} \subseteq \mathbb{Z}[X_0, \ldots, X_n] =: A$ be homogeneous prime ideal of dimension d.
- (Nesterenko) Chow forms of $\mathfrak{P}$ is polynomial $F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}}$ is irreducible in $\mathbb{Z}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}} = 0$ iff $d+1$ generic hyperplanes intersect at a zero of $\mathfrak{P}$
- Degree of $\mathfrak{P}$ is g, the degree of $F_{\mathfrak{P}}$ in $\overline{u}_0$.
- Chow form factors in suitable extension field into a product of g linear forms, $F_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} \overline{\alpha}^{(i)} \cdot \overline{u}_d$.
- (Nesterenko) The resultant of $F_{\mathfrak{P}}$ and $Q \in \mathbb{Z}[X_0, \ldots, X_n]$ is $\mathtt{res}(F_{\mathfrak{P}}, Q) := a(\overline{u}_0, \ldots, \overline{u}_{d-1})^{\deg Q} \prod_{i=1}^{g} Q(\overline{\alpha}^{(i)})$.

Tools in Proof (Sketch)

- From transcendental number theory
- Let $\mathfrak{P} \subseteq \mathbb{Z}[X_0, \ldots, X_n] =: A$ be homogeneous prime ideal of dimension d.
- (Nesterenko) Chow forms of $\mathfrak{P}$ is polynomial $F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}}$ is irreducible in $\mathbb{Z}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}} = 0$ iff $d + 1$ generic hyperplanes intersect at a zero of $\mathfrak{P}$
- Degree of $\mathfrak{P}$ is g, the degree of $F_{\mathfrak{P}}$ in $\overline{u}_0$.
- Chow form factors in suitable extension field into a product of g linear forms, $F_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} \overline{\alpha}^{(i)} \cdot \overline{u}_d$.
- (Nesterenko) The resultant of $F_{\mathfrak{P}}$ and $Q \in \mathbb{Z}[X_0, \ldots, X_n]$ is $\mathtt{res}(F_{\mathfrak{P}}, Q) := a(\overline{u}_0, \ldots, \overline{u}_{d-1})^{\deg Q} \prod_{i=1}^{g} Q(\overline{\alpha}^{(i)})$.

Tools in Proof (Sketch)

- From transcendental number theory
- Let $\mathfrak{P} \subseteq \mathbb{Z}[X_0, \ldots, X_n] =: A$ be homogeneous prime ideal of dimension d.
- (Nesterenko) Chow forms of $\mathfrak{P}$ is polynomial $F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}}$ is irreducible in $\mathbb{Z}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}} = 0$ iff $d + 1$ generic hyperplanes intersect at a zero of $\mathfrak{P}$
- Degree of $\mathfrak{P}$ is g, the degree of $F_{\mathfrak{P}}$ in $\overline{u}_0$.
- Chow form factors in suitable extension field into a product of g linear forms, $F_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} \overline{\alpha}^{(i)} \cdot \overline{u}_d$.
- (Nesterenko) The resultant of $F_{\mathfrak{P}}$ and $Q \in \mathbb{Z}[X_0, \ldots, X_n]$ is $\mathtt{res}(F_{\mathfrak{P}}, Q) := a(\overline{u}_0, \ldots, \overline{u}_{d-1})^{\deg Q} \prod_{i=1}^{g} Q(\overline{\alpha}^{(i)})$.

Tools in Proof (Sketch)

- From transcendental number theory
- Let $\mathfrak{P} \subseteq \mathbb{Z}[X_0, \ldots, X_n] =: A$ be homogeneous prime ideal of dimension d.
- (Nesterenko) Chow forms of $\mathfrak{P}$ is polynomial $F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}}$ is irreducible in $\mathbb{Z}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}} = 0$ iff $d + 1$ generic hyperplanes intersect at a zero of $\mathfrak{P}$
- Degree of $\mathfrak{P}$ is g, the degree of $F_{\mathfrak{P}}$ in $\overline{u}_0$.
- Chow form factors in suitable extension field into a product of g linear forms, $F_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} \overline{\alpha}^{(i)} \cdot \overline{u}_d$.
- (Nesterenko) The resultant of $F_{\mathfrak{P}}$ and $Q \in \mathbb{Z}[X_0, \ldots, X_n]$ is $\mathtt{res}(F_{\mathfrak{P}}, Q) := a(\overline{u}_0, \ldots, \overline{u}_{d-1})^{\deg Q} \prod_{i=1}^{g} Q(\overline{\alpha}^{(i)})$.

Tools in Proof (Sketch)

- From transcendental number theory
- Let $\mathfrak{P} \subseteq \mathbb{Z}[X_0, \ldots, X_n] =: A$ be homogeneous prime ideal of dimension d.
- (Nesterenko) Chow forms of $\mathfrak{P}$ is polynomial $F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}}$ is irreducible in $\mathbb{Z}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}} = 0$ iff $d+1$ generic hyperplanes intersect at a zero of $\mathfrak{P}$
- Degree of $\mathfrak{P}$ is g, the degree of $F_{\mathfrak{P}}$ in $\overline{u}_0$.
- Chow form factors in suitable extension field into a product of g linear forms, $F_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} \overline{\alpha}^{(i)} \cdot \overline{u}_d$.
- (Nesterenko) The resultant of $F_{\mathfrak{P}}$ and $Q \in \mathbb{Z}[X_0, \ldots, X_n]$ is $\mathtt{res}(F_{\mathfrak{P}}, Q) := a(\overline{u}_0, \ldots, \overline{u}_{d-1})^{\deg Q} \prod_{i=1}^{g} Q(\overline{\alpha}^{(i)})$.

Tools in Proof (Sketch)

- From transcendental number theory
- Let $\mathfrak{P} \subseteq \mathbb{Z}[X_0, \ldots, X_n] =: A$ be homogeneous prime ideal of dimension d.
- (Nesterenko) Chow forms of $\mathfrak{P}$ is polynomial $F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}}$ is irreducible in $\mathbb{Z}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}} = 0$ iff $d+1$ generic hyperplanes intersect at a zero of $\mathfrak{P}$
- Degree of $\mathfrak{P}$ is g, the degree of $F_{\mathfrak{P}}$ in $\overline{u}_0$.
- Chow form factors in suitable extension field into a product of g linear forms, $F_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} \overline{\alpha}^{(i)} \cdot \overline{u}_d$.
- (Nesterenko) The resultant of $F_{\mathfrak{P}}$ and $Q \in \mathbb{Z}[X_0, \ldots, X_n]$ is $\mathtt{res}(F_{\mathfrak{P}}, Q) := a(\overline{u}_0, \ldots, \overline{u}_{d-1})^{\deg Q} \prod_{i=1}^{g} Q(\overline{\alpha}^{(i)})$.

Tools in Proof (Sketch)

- From transcendental number theory
- Let $\mathfrak{P} \subseteq \mathbb{Z}[X_0, \ldots, X_n] =: A$ be homogeneous prime ideal of dimension d.
- (Nesterenko) Chow forms of $\mathfrak{P}$ is polynomial $F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}}$ is irreducible in $\mathbb{Z}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}} = 0$ iff $d+1$ generic hyperplanes intersect at a zero of $\mathfrak{P}$
- Degree of $\mathfrak{P}$ is g, the degree of $F_{\mathfrak{P}}$ in $\overline{u}_0$.
- Chow form factors in suitable extension field into a product of g linear forms, $F_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} \overline{\alpha}^{(i)} \cdot \overline{u}_d$.
- (Nesterenko) The resultant of $F_{\mathfrak{P}}$ and $Q \in \mathbb{Z}[X_0, \ldots, X_n]$ is $\mathtt{res}(F_{\mathfrak{P}}, Q) := a(\overline{u}_0, \ldots, \overline{u}_{d-1})^{\deg Q} \prod_{i=1}^{g} Q(\overline{\alpha}^{(i)})$.

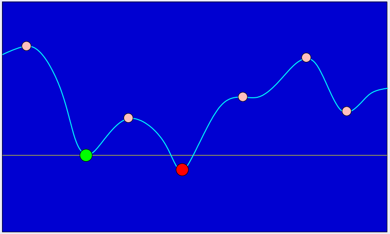
Tools in Proof (Sketch)

- From transcendental number theory
- Let $\mathfrak{P} \subseteq \mathbb{Z}[X_0, \ldots, X_n] =: A$ be homogeneous prime ideal of dimension d.
- (Nesterenko) Chow forms of $\mathfrak{P}$ is polynomial $F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}}$ is irreducible in $\mathbb{Z}(\overline{u}_0, \ldots, \overline{u}_d)$
  - $F_{\mathfrak{P}} = 0$ iff $d + 1$ generic hyperplanes intersect at a zero of $\mathfrak{P}$
- Degree of $\mathfrak{P}$ is g, the degree of $F_{\mathfrak{P}}$ in $\overline{u}_0$.
- Chow form factors in suitable extension field into a product of g linear forms, $F_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} \overline{\alpha}^{(i)} \cdot \overline{u}_d$.
- (Nesterenko) The resultant of $F_{\mathfrak{P}}$ and $Q \in \mathbb{Z}[X_0, \ldots, X_n]$ is $\mathtt{res}(F_{\mathfrak{P}}, Q) := a(\overline{u}_0, \ldots, \overline{u}_{d-1})^{\deg Q} \prod_{i=1}^{g} Q(\overline{\alpha}^{(i)})$.

Coming Up Next

Evaluation Bounds

$EV(f)$



For $f \in \mathbb{Z}[X_1, \ldots, X_n]$,
$EV(f) :=$
$\inf\{|f(\alpha)| : \alpha \in \mathbb{C}^n, f(\alpha) \neq 0, \nabla f(\alpha) = \mathbf{0}\}$

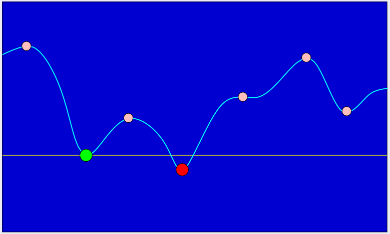
Bound for $f(X, Y)$, [Burr/Choi/Galehouse/Y. ISSAC'08]

$$-\lg EV(f) \leq 4D^2(2D \lg D + L)$$

This leads to a method (based on Mountain Pass Theorem) to isolate the isolated singularities of an algebraic curve.

Evaluation Bounds

$EV(f)$



For $f \in \mathbb{Z}[X_1, \ldots, X_n]$,

$EV(f) :=$

$\inf\{|f(\alpha)| : \alpha \in \mathbb{C}^n, f(\alpha) \neq 0, \nabla f(\alpha) = \mathbf{0}\}$

Bound for $f(X, Y)$, [Burr/Choi/Galehouse/Y. ISSAC'08]

$$-\lg EV(f) \leq 4D^2(2D\lg D + L)$$

This leads to a method (based on Mountain Pass Theorem) to isolate the isolated singularities of an algebraic curve.

Generalization of this Bound

Lemma

For $f \in \mathbb{C}[X_1, \ldots, X_n]$, let $I_f := (f - Z, \partial_1 f, \ldots, \partial_n f) \subseteq \mathbb{Z}[Z, X_1, \ldots, X_n]$ *where Z is a new variable. Then $\text{ZERO}(I_f) \subseteq \mathbb{C}^{n+1}$ with $\Pi_Z(\text{ZERO}(I_f))$ is a finite set.*

Proof.

Idea: Use Algebraic Sard's Lemma. View f as a regular map on varieties, $f : X \to Y$ where $X = \mathbb{C}^n$ and $Y = \mathbb{C}$. From Harris [Prop.14.4], ($\exists$ a Zariski open set $U \subseteq \mathbb{C}$) such that $(\forall p \in f^{-1}(U))$, the differential $d_f(p) = \nabla f(p)$ is surjective. Surjectivity means $\nabla f(p) \neq (0, \ldots, 0) = \mathbf{0}$. Contrapositively, $\nabla f(p) = \mathbf{0}$ implies $f(p) \in \mathbb{C} \setminus U$. Thus $\Pi_Z(\text{ZERO}(I_f)) \subseteq \mathbb{C} \setminus U$. But $\mathbb{C} \setminus U$ is a finite set (being Zariski closed). □

Generalization of this Bound

Lemma

For $f \in \mathbb{C}[X_1, \ldots, X_n]$, let $I_f := (f - Z, \partial_1 f, \ldots, \partial_n f) \subseteq \mathbb{Z}[Z, X_1, \ldots, X_n]$ *where Z is a new variable. Then $\text{ZERO}(I_f) \subseteq \mathbb{C}^{n+1}$ with $\Pi_Z(\text{ZERO}(I_f))$ is a finite set.*

Proof.

Idea: Use Algebraic Sard's Lemma. View f as a regular map on varieties, $f : X \to Y$ where $X = \mathbb{C}^n$ and $Y = \mathbb{C}$. From Harris [Prop.14.4], ($\exists$ a Zariski open set $U \subseteq \mathbb{C}$) such that $(\forall p \in f^{-1}(U))$, the differential $d_f(p) = \nabla f(p)$ is surjective. Surjectivity means $\nabla f(p) \neq (0, \ldots, 0) = \mathbf{0}$. Contrapositively, $\nabla f(p) = \mathbf{0}$ implies $f(p) \in \mathbb{C} \setminus U$. Thus $\Pi_Z(\text{ZERO}(I_f)) \subseteq \mathbb{C} \setminus U$. But $\mathbb{C} \setminus U$ is a finite set (being Zariski closed). □

Generalization of this Bound

Lemma

For $f \in \mathbb{C}[X_1, \ldots, X_n]$, let $I_f := (f - Z, \partial_1 f, \ldots, \partial_n f) \subseteq \mathbb{Z}[Z, X_1, \ldots, X_n]$ where Z is a new variable. Then $\text{ZERO}(I_f) \subseteq \mathbb{C}^{n+1}$ with $\Pi_Z(\text{ZERO}(I_f))$ is a finite set.

Proof.

Idea: Use Algebraic Sard's Lemma. View f as a regular map on varieties, $f : X \to Y$ where $X = \mathbb{C}^n$ and $Y = \mathbb{C}$. From Harris [Prop.14.4], ($\exists$ a Zariski open set $U \subseteq \mathbb{C}$) such that $(\forall p \in f^{-1}(U))$, the differential $d_f(p) = \nabla f(p)$ is surjective. Surjectivity means $\nabla f(p) \neq (0, \ldots, 0) = \mathbf{0}$. Contrapositively, $\nabla f(p) = \mathbf{0}$ implies $f(p) \in \mathbb{C} \setminus U$. Thus $\Pi_Z(\text{ZERO}(I_f)) \subseteq \mathbb{C} \setminus U$. But $\mathbb{C} \setminus U$ is a finite set (being Zariski closed). □

Generalization

Corollary

If $f \in \mathbb{Z}[X_1, \ldots, X_n]$ *has degree* D *and height* $< 2^L$ *then*

$$EV(f) \geq ((n+2)^2 e^{n+3})^{-(n+1)(n+2)D^{n+1}} (n^n (n+1) D 2^L)^{-(n+1)D^n}.$$

For $n = 2$*, this yields*

$$-\lg EV(f) \leq 3D^2(44.9D + L + \lg 12D).$$

This bound for $n = 2$ is slightly better than the bound in [Choi et al, ISSAC'08]

Generalization

Corollary

If $f \in \mathbb{Z}[X_1, \ldots, X_n]$ has degree D and height $< 2^L$ then

$$EV(f) \geq ((n+2)^2 e^{n+3})^{-(n+1)(n+2)D^{n+1}} (n^n (n+1) D 2^L)^{-(n+1)D^n}.$$

For $n = 2$, this yields

$$-\lg EV(f) \leq 3D^2(44.9D + L + \lg 12D).$$

This bound for $n = 2$ is slightly better than the bound in [Choi et al, ISSAC'08]

Coming Up Next

How Good Are These Bounds? (1)

Example: $f = (xy+1)^2 - 1$,

$$f_x = 2(xy+1)y, \quad f_y = 2(xy+1)x.$$

- Let $I_f := (f - z, f_x, f_y) \subseteq \mathbb{Z}[x,y,z]$.
- By corollary, if $(\zeta_1, \zeta_2, \zeta_3) \in \text{ZERO}(I_f)$ and $\zeta_3 \neq 0$ then

$$|\zeta_3| \geq (16e^5)^{-12\cdot 4^3}(9\cdot 4\cdot 2)^{-3\cdot 4^2} = (16e^5)^{-768}(72)^{-48}$$

- Need about 8000 bits of accuracy
- Exact value? $|\zeta_3| = 1$
  - $\text{ZERO}(f_x, f_y) = \text{ZERO}(xy+1) \cup \text{ZERO}(x,y)$
  - f is 1 on $V(xy+1)$ and f is 0 on $V(x,y)$.

How Good Are These Bounds? (1)

Example: $f = (xy+1)^2 - 1$,

$$f_x = 2(xy+1)y, \quad f_y = 2(xy+1)x.$$

- Let $I_f := (f - z, f_x, f_y) \subseteq \mathbb{Z}[x,y,z]$.
- By corollary, if $(\zeta_1, \zeta_2, \zeta_3) \in \text{ZERO}(I_f)$ and $\zeta_3 \neq 0$ then

$$|\zeta_3| \geq (16e^5)^{-12\cdot 4^3}(9\cdot 4\cdot 2)^{-3\cdot 4^2} = (16e^5)^{-768}(72)^{-48}$$

- Need about 8000 bits of accuracy
- Exact value? $|\zeta_3| = 1$
  - $\text{ZERO}(f_x, f_y) = \text{ZERO}(xy+1) \cup \text{ZERO}(x,y)$
  - f is 1 on $V(xy+1)$ and f is 0 on $V(x,y)$.

How Good Are These Bounds? (1)

Example: $f = (xy+1)^2 - 1$,
$$f_x = 2(xy+1)y, \quad f_y = 2(xy+1)x.$$

- Let $I_f := (f - z, f_x, f_y) \subseteq \mathbb{Z}[x,y,z]$.
- By corollary, if $(\zeta_1, \zeta_2, \zeta_3) \in \textsc{Zero}(I_f)$ and $\zeta_3 \neq 0$ then

$$|\zeta_3| \geq (16e^5)^{-12\cdot 4^3}(9\cdot 4\cdot 2)^{-3\cdot 4^2} = (16e^5)^{-768}(72)^{-48}$$

- Need about 8000 bits of accuracy
- Exact value? $|\zeta_3| = 1$
  - $\textsc{Zero}(f_x, f_y) = \textsc{Zero}(xy+1) \cup \textsc{Zero}(x,y)$
  - f is 1 on $V(xy+1)$ and f is 0 on $V(x,y)$.

How Good Are These Bounds? (1)

Example: $f = (xy+1)^2 - 1$,

$$f_x = 2(xy+1)y, \quad f_y = 2(xy+1)x.$$

- Let $I_f := (f - z, f_x, f_y) \subseteq \mathbb{Z}[x,y,z]$.
- By corollary, if $(\zeta_1, \zeta_2, \zeta_3) \in \text{ZERO}(I_f)$ and $\zeta_3 \neq 0$ then

$$|\zeta_3| \geq (16e^5)^{-12\cdot 4^3}(9\cdot 4\cdot 2)^{-3\cdot 4^2} = (16e^5)^{-768}(72)^{-48}$$

- Need about 8000 bits of accuracy
- Exact value? $|\zeta_3| = 1$
  - $\text{ZERO}(f_x, f_y) = \text{ZERO}(xy+1) \cup \text{ZERO}(x,y)$
  - f is 1 on $V(xy+1)$ and f is 0 on $V(x,y)$.

How Good Are These Bounds? (1)

Example: $f = (xy+1)^2 - 1,$

$$f_x = 2(xy+1)y, \quad f_y = 2(xy+1)x.$$

- Let $I_f := (f - z, f_x, f_y) \subseteq \mathbb{Z}[x,y,z]$.
- By corollary, if $(\zeta_1, \zeta_2, \zeta_3) \in \text{Zero}(I_f)$ and $\zeta_3 \neq 0$ then

$$|\zeta_3| \geq (16e^5)^{-12\cdot 4^3}(9\cdot 4\cdot 2)^{-3\cdot 4^2} = (16e^5)^{-768}(72)^{-48}$$

- Need about 8000 bits of accuracy
- Exact value? $|\zeta_3| = 1$
  - $\text{Zero}(f_x, f_y) = \text{Zero}(xy+1) \cup \text{Zero}(x,y)$
  - f is 1 on $V(xy+1)$ and f is 0 on $V(x,y)$.

How Good Are These Bounds? (1)

Example: $f = (xy+1)^2 - 1$,

$$f_x = 2(xy+1)y, \quad f_y = 2(xy+1)x.$$

- Let $I_f := (f - z, f_x, f_y) \subseteq \mathbb{Z}[x,y,z]$.
- By corollary, if $(\zeta_1, \zeta_2, \zeta_3) \in \text{ZERO}(I_f)$ and $\zeta_3 \neq 0$ then

$$|\zeta_3| \geq (16e^5)^{-12\cdot 4^3}(9\cdot 4\cdot 2)^{-3\cdot 4^2} = (16e^5)^{-768}(72)^{-48}$$

- Need about 8000 bits of accuracy
- Exact value? $|\zeta_3| = 1$
  - $\text{ZERO}(f_x, f_y) = \text{ZERO}(xy+1) \cup \text{ZERO}(x,y)$
  - f is 1 on $V(xy+1)$ and f is 0 on $V(x,y)$.

How Good Are These Bounds? (1)

Example: $f = (xy+1)^2 - 1,$

$$f_x = 2(xy+1)y, \quad f_y = 2(xy+1)x.$$

- Let $I_f := (f - z, f_x, f_y) \subseteq \mathbb{Z}[x,y,z]$.
- By corollary, if $(\zeta_1, \zeta_2, \zeta_3) \in \textsc{Zero}(I_f)$ and $\zeta_3 \neq 0$ then

$$|\zeta_3| \geq (16e^5)^{-12\cdot 4^3}(9\cdot 4\cdot 2)^{-3\cdot 4^2} = (16e^5)^{-768}(72)^{-48}$$

- Need about 8000 bits of accuracy
- Exact value? $|\zeta_3| = 1$
  - $\textsc{Zero}(f_x, f_y) = \textsc{Zero}(xy+1) \cup \textsc{Zero}(x,y)$
  - f is 1 on $V(xy+1)$ and f is 0 on $V(x,y)$.

How Good Are These Bounds? (1)

Example: $f = (xy+1)^2 - 1$,
$$f_x = 2(xy+1)y, \quad f_y = 2(xy+1)x\,.$$

- Let $I_f := (f - z, f_x, f_y) \subseteq \mathbb{Z}[x,y,z]$.
- By corollary, if $(\zeta_1, \zeta_2, \zeta_3) \in \textsc{Zero}(I_f)$ and $\zeta_3 \neq 0$ then

$$|\zeta_3| \geq (16e^5)^{-12\cdot 4^3}(9\cdot 4\cdot 2)^{-3\cdot 4^2} = (16e^5)^{-768}(72)^{-48}$$

- Need about 8000 bits of accuracy
- Exact value? $|\zeta_3| = 1$
  - $\textsc{Zero}(f_x, f_y) = \textsc{Zero}(xy+1) \cup \textsc{Zero}(x,y)$
  - f is 1 on $V(xy+1)$ and f is 0 on $V(x,y)$.

How Good Are These Bounds? (2)

Comparison

Canny	$(3DH)^{-nD^n}$	
Yap	$(2^{3/2}NK)^{-nD^{n-1}}2^{-(n+1)D^n}$	$N = \binom{1+nD}{n}, K = H\sqrt{\binom{n+D-1}{D}}$
New ($\approx$)	$(n^2e^n)^{-n^2D^n}(d^{n-1}mH)^{-(n)D^{n-1}}$	set $m = n$ for comparison

The "shape" is about right.

Conclusion

- MANY advantages in numerical approaches to algebraic and geometric problems
- To obtain exact results, we need zero bounds
- OPEN: obtain sharper bounds (for special cases)
- OPEN: algorithms for (a posteriori) computational bounds

Conclusion

- MANY advantages in numerical approaches to algebraic and geometric problems
- To obtain exact results, we need zero bounds
- OPEN: obtain sharper bounds (for special cases)
- OPEN: algorithms for (a posteriori) computational bounds

Conclusion

- MANY advantages in numerical approaches to algebraic and geometric problems
- To obtain exact results, we need zero bounds
- OPEN: obtain sharper bounds (for special cases)
- OPEN: algorithms for (a posteriori) computational bounds

Conclusion

- MANY advantages in numerical approaches to algebraic and geometric problems
- To obtain exact results, we need zero bounds
- OPEN: obtain sharper bounds (for special cases)
- OPEN: algorithms for (a posteriori) computational bounds

Conclusion

- MANY advantages in numerical approaches to algebraic and geometric problems
- To obtain exact results, we need zero bounds
- OPEN: obtain sharper bounds (for special cases)
- OPEN: algorithms for (a posteriori) computational bounds

Conclusion

- MANY advantages in numerical approaches to algebraic and geometric problems
- To obtain exact results, we need zero bounds
- OPEN: obtain sharper bounds (for special cases)
- OPEN: algorithms for (a posteriori) computational bounds

Thank you!