Polynomial Root Distribution and its Impact on Solutions to Thue Equations

Greg Knapp

Department of Mathematics
University of Oregon

23 May 2023

Thesis and Outline

Thesis

Important information about roots of polynomials can be gleaned from knowledge of the coefficients.

Thesis and Outline

Thesis

Important information about roots of polynomials can be gleaned from knowledge of the coefficients.

Outline

- Rational approximations to algebraic numbers (Diophantine approximation).

Thesis and Outline

Thesis

Important information about roots of polynomials can be gleaned from knowledge of the coefficients.

Outline

- Rational approximations to algebraic numbers (Diophantine approximation).
- The impact of Diophantine approximation on bounding the number of solutions to Thue equations.

Thesis and Outline

Thesis

Important information about roots of polynomials can be gleaned from knowledge of the coefficients.

Outline

- Rational approximations to algebraic numbers (Diophantine approximation).
- The impact of Diophantine approximation on bounding the number of solutions to Thue equations.
- A more general study of polynomial root distribution in the complex plane.

The Density of $\mathbb{Q}$ in $\mathbb{R}$

Theorem (Classical)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

The Density of $\mathbb{Q}$ in $\mathbb{R}$

Theorem (Classical)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Pros and Cons

- Pro: this relates easy-to-understand numbers (rational numbers) hard-to-understand numbers (real numbers).

The Density of $\mathbb{Q}$ in $\mathbb{R}$

Theorem (Classical)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Pros and Cons

- Pro: this relates easy-to-understand numbers (rational numbers) hard-to-understand numbers (real numbers).
- Con: this theorem is *ineffective*. It gives no indication of how large p or q must be to attain the desired accuracy.

A More Useful Approximation Result

Theorem (Classical)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

A More Useful Approximation Result

Theorem (Classical)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$|q\alpha - p| < \varepsilon,$$

A More Useful Approximation Result

Theorem (Classical)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$|q\alpha - p| < \varepsilon,$$

i.e.

$$\left|\alpha - \frac{p}{q}\right| < \frac{\varepsilon}{q}$$

A More Useful Approximation Result

Theorem (Classical)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$|q\alpha - p| < \varepsilon,$$

i.e.

$$\left|\alpha - \frac{p}{q}\right| < \frac{\varepsilon}{q} \leqslant \varepsilon.$$

A More Useful Approximation Result

Theorem (Classical)

Let $\alpha \in \mathbb{R}$ *and let* $\varepsilon > 0$*. Then there exist integers* p *and* q *with* $q > 0$ *so that*

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ *and let* $\varepsilon > 0$*. Then there exist integers* p *and* q *with*

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{\varepsilon}{q} \leqslant \varepsilon.$$

A More Useful Approximation Result

Theorem (Classical)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{\varepsilon}{q} \leqslant \varepsilon.$$

Benefit: to obtain ε-accuracy, we only need to find q as large as $\frac{1}{\varepsilon}$.

A More Useful Approximation Result

Theorem

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{\varepsilon}{q}$$

A More Useful Approximation Result

Theorem

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{\varepsilon}{q} \leqslant \frac{1}{q^2}.$$

A More Useful Approximation Result

Theorem

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{\varepsilon}{q} \leqslant \frac{1}{q^2}.$$

Benefit: $|\alpha - p/q| < 1/q^2$ is independent of ε.

Distinguishing Between Rationals and Irrationals

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Distinguishing Between Rationals and Irrationals

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

The number of distinct rationals which satisfy $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$ will turn out to be a key feature which indicates whether or not α is rational or irrational.

Correspondence

Definition

A pair $(p, q) \in \mathbb{Z}^2$ is said to be *primitive* if $\gcd(p, q) = 1$.

Correspondence

Definition

A pair $(p, q) \in \mathbb{Z}^2$ is said to be *primitive* if $\gcd(p, q) = 1$.

Connection to Rationals

We will regularly use the one-to-one correspondence

$$\{\text{primitive pairs } (p, q) \in \mathbb{Z} \times \mathbb{Z}_{>0}\} \to \mathbb{Q}$$
$$(p, q) \mapsto \frac{p}{q}$$

Distinguishing Between Rationals and Irrationals

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Distinguishing Between Rationals and Irrationals

Theorem (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$ and let $\varepsilon > 0$. Then there exist integers p and q with

$$0 < q \leqslant \frac{1}{\varepsilon}$$

so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Corollary (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$. Then α is irrational if and only if there are infinitely many primitive pairs $(p, q) \in \mathbb{Z}^2$ with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Distinguishing Between Rationals and Irrationals

Corollary (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$. Then α is irrational if and only if there are infinitely many primitive pairs $(p, q) \in \mathbb{Z}^2$ with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Key to understanding: the exponent on q in the error term.

Distinguishing Between Rationals and Irrationals

Corollary (Dirichlet, 1842)

Let $\alpha \in \mathbb{R}$. Then α is irrational if and only if there are infinitely many primitive pairs $(p, q) \in \mathbb{Z}^2$ with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Key to understanding: the exponent on q in the error term.

Up Next

Let's look at how that exponent changes according to properties of the number α.

Rational Approximation of Rationals

Fact

Let $\alpha \in \mathbb{Q} \setminus \mathbb{Z}$. Then there are infinitely many primitive pairs $(p, q) \in \mathbb{Z}^2$ with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q}.$$

Rational Approximation of Rationals

Fact

Let $\alpha \in \mathbb{Q} \setminus \mathbb{Z}$. Then there are infinitely many primitive pairs $(p, q) \in \mathbb{Z}^2$ with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q}.$$

If $\varepsilon > 0$, then there are only finitely many primitive pairs $(p, q) \in \mathbb{Z}^2$ with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{1+\varepsilon}}.$$

Distinguishing Between Algebraic and Transcendental Numbers

Recall that irrational numbers fit into one of two categories.

Distinguishing Between Algebraic and Transcendental Numbers

Recall that irrational numbers fit into one of two categories.

Definition

A complex number α is said to be *algebraic* if there exists a polynomial $f(x) \in \mathbb{Z}[x]$ with $f(\alpha) = 0$. Otherwise, α is said to be *transcendental*.

Distinguishing Between Algebraic and Transcendental Numbers

Recall that irrational numbers fit into one of two categories.

Definition

A complex number α is said to be *algebraic* if there exists a polynomial $f(x) \in \mathbb{Z}[x]$ with $f(\alpha) = 0$. Otherwise, α is said to be *transcendental*.

Question

Since we have approximation results which distinguish between rational numbers and irrational numbers, can we find an approximation result which distinguishes between algebraic and transcendental numbers?

Distinguishing Between Algebraic and Transcendental Numbers

Question

Is there an approximation result that distinguishes between algebraic and transcendental numbers?

Distinguishing Between Algebraic and Transcendental Numbers

Question

Is there an approximation result that distinguishes between algebraic and transcendental numbers?

Theorem (Roth, 1955)

Suppose that $\alpha \in \mathbb{R}$ is algebraic and $\varepsilon > 0$. Then there are only finitely many primitive pairs $(p, q) \in \mathbb{Z}^2$ with $q > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}.$$

Approximation Summary

Facts

- Real numbers α are classified by the "largest" exponent μ which allows infinitely many rational solutions to

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\mu}}.$$

Approximation Summary

Facts

- Real numbers α are classified by the "largest" exponent μ which allows infinitely many rational solutions to

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\mu}}.$$

- Rational numbers have $\mu = 1$.

Approximation Summary

Facts

- Real numbers α are classified by the "largest" exponent μ which allows infinitely many rational solutions to

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\mu}}.$$

- Rational numbers have $\mu = 1$.
- Irrational numbers have $\mu \geqslant 2$.

Approximation Summary

Facts

- Real numbers α are classified by the "largest" exponent μ which allows infinitely many rational solutions to

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\mu}}.$$

- Rational numbers have $\mu = 1$.
- Irrational numbers have $\mu \geqslant 2$.
- Irrational algebraic numbers have $\mu = 2$.

Approximation Summary

Facts

- Real numbers α are classified by the "largest" exponent μ which allows infinitely many rational solutions to

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\mu}.$$

- Rational numbers have $\mu = 1$.
- Irrational numbers have $\mu \geqslant 2$.
- Irrational algebraic numbers have $\mu = 2$.

Problem

For $\delta > \mu$, how do we find the finitely many rational solutions to

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\delta}?$$

Intro to Thue Equations

Thue equations provide a classical context in which rational approximation results play an important role.

Intro to Thue Equations

Thue equations provide a classical context in which rational approximation results play an important role.

Definition

A polynomial $F(x, y) \in \mathbb{Z}[x, y]$ which is homogeneous is said to be an *integral binary form*.

Intro to Thue Equations

Thue equations provide a classical context in which rational approximation results play an important role.

Definition

A polynomial $F(x, y) \in \mathbb{Z}[x, y]$ which is homogeneous is said to be an *integral binary form*.

Definition

Let $F(x, y)$ be an integral binary form which is irreducible over $\mathbb{Q}$ and has degree at least 3. Let h be an integer. Then the equation

$$F(x, y) = h$$

is known as a *Thue equation* and the inequality

$$|F(x, y)| \leqslant h$$

is known as a *Thue inequality*.

Solutions to Thue equations

Definition

Let $F(x, y)$ be an integral binary form which is irreducible over $\mathbb{Q}$ and has degree at least 3. Let h be an integer. Then the equation

$$F(x, y) = h$$

is known as a *Thue equation* and the inequality

$$|F(x, y)| \leqslant h$$

is known as a *Thue inequality*.

Solutions to Thue equations

Definition

Let $F(x, y)$ be an integral binary form which is irreducible over $\mathbb{Q}$ and has degree at least 3. Let h be an integer. Then the equation

$$F(x, y) = h$$

is known as a *Thue equation* and the inequality

$$|F(x, y)| \leqslant h$$

is known as a *Thue inequality*.

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation.

Solutions to Thue equations

Definition

Let $F(x, y)$ be an integral binary form which is irreducible over $\mathbb{Q}$ and has degree at least 3. Let h be an integer. Then the equation

$$F(x, y) = h$$

is known as a *Thue equation* and the inequality

$$|F(x, y)| \leqslant h$$

is known as a *Thue inequality*.

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation.

Corollary (Thue, 1909)

There are finitely many integer solutions to any Thue inequality.

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Proof Idea

If $p, q \in \mathbb{Z}$ with $q \neq 0$ and $n = \deg(F)$,

$$F(p, q) = h$$

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Proof Idea

If $p, q \in \mathbb{Z}$ with $q \neq 0$ and $n = \deg(F)$,

$$F(p, q) = h \Rightarrow F\left(\frac{p}{q}, 1\right) = \frac{h}{q^n}.$$

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Proof Idea

If $p, q \in \mathbb{Z}$ with $q \neq 0$ and $n = \deg(F)$,

$$F(p, q) = h \Rightarrow F\left(\frac{p}{q}, 1\right) = \frac{h}{q^n}.$$

Let $f(X) := F(X, 1)$ and factor $f(X)$ over $\mathbb{C}[X]$ as $f(X) = a\prod_{i=1}^{n}(X - \alpha_i)$.

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Proof Idea

Suppose $n = \deg(F)$ and $F(p, q) = h$. Let $f(X) := F(X, 1)$ and factor $f(X)$ over $\mathbb{C}[X]$ as $f(X) = a\prod_{i=1}^{n}(X - \alpha_i)$. Then

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Proof Idea

Suppose $n = \deg(F)$ and $F(p, q) = h$. Let $f(X) := F(X, 1)$ and factor $f(X)$ over $\mathbb{C}[X]$ as $f(X) = a \prod_{i=1}^{n}(X - \alpha_i)$. Then

$$F(p, q) = h \Rightarrow F\left(\frac{p}{q}, 1\right) = \frac{h}{q^n}$$

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Proof Idea

Suppose $n = \deg(F)$ and $F(p, q) = h$. Let $f(X) := F(X, 1)$ and factor $f(X)$ over $\mathbb{C}[X]$ as $f(X) = a\prod_{i=1}^{n}(X - \alpha_i)$. Then

$$F(p,q) = h \Rightarrow F\left(\frac{p}{q}, 1\right) = \frac{h}{q^n}$$
$$\Rightarrow f\left(\frac{p}{q}\right) = \frac{h}{q^n}$$

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Proof Idea

Suppose $n = \deg(F)$ and $F(p, q) = h$. Let $f(X) := F(X, 1)$ and factor $f(X)$ over $\mathbb{C}[X]$ as $f(X) = a\prod_{i=1}^{n}(X - \alpha_i)$. Then

$$\begin{aligned} F(p,q) = h &\Rightarrow F\left(\frac{p}{q}, 1\right) = \frac{h}{q^n} \\ &\Rightarrow f\left(\frac{p}{q}\right) = \frac{h}{q^n} \\ &\Rightarrow |a|\prod_{i=1}^{n}\left|\frac{p}{q} - \alpha_i\right| = \frac{|h|}{|q|^n} \end{aligned}$$

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Proof Idea

Suppose $n = \deg(F)$ and $F(p, q) = h$. Let $f(X) := F(X, 1)$ and factor $f(X)$ over $\mathbb{C}[X]$ as $f(X) = a\prod_{i=1}^{n}(X - \alpha_i)$. Then

$$\begin{aligned} F(p,q) = h &\Rightarrow F\left(\frac{p}{q}, 1\right) = \frac{h}{q^n} \\ &\Rightarrow f\left(\frac{p}{q}\right) = \frac{h}{q^n} \\ &\Rightarrow |a|\prod_{i=1}^{n}\left|\frac{p}{q} - \alpha_i\right| = \frac{|h|}{|q|^n} = \text{small}. \end{aligned}$$

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Proof Idea

Suppose $n = \deg(F)$ and $F(p, q) = h$. Let $f(X) := F(X, 1)$ and factor $f(X)$ over $\mathbb{C}[X]$ as $f(X) = a \prod_{i=1}^{n}(X - \alpha_i)$. Then

$$|a| \prod_{i=1}^{n} \left| \frac{p}{q} - \alpha_i \right| = \text{small}$$

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Proof Idea

Suppose $n = \deg(F)$ and $F(p, q) = h$. Let $f(X) := F(X, 1)$ and factor $f(X)$ over $\mathbb{C}[X]$ as $f(X) = a\prod_{i=1}^{n}(X - \alpha_i)$. Then

$$|a| \prod_{i=1}^{n} \left| \frac{p}{q} - \alpha_i \right| = \text{small}$$

Therefore, for some i, $\left|\frac{p}{q} - \alpha_i\right|$ is small.

Thue's Theorem

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Proof Idea

Suppose $n = \deg(F)$ and $F(p, q) = h$. Let $f(X) := F(X, 1)$ and factor $f(X)$ over $\mathbb{C}[X]$ as $f(X) = a\prod_{i=1}^{n}(X - \alpha_i)$. Then

$$|a| \prod_{i=1}^{n} \left| \frac{p}{q} - \alpha_i \right| = \text{small}$$

Therefore, for some i, $\left|\frac{p}{q} - \alpha_i\right|$ is small. Now we can use Diophantine approximation results to show that the number of solutions is finite.

Follow-up Questions

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Follow-up Questions

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Questions

- What are the solutions to $F(x, y) = h$?

Follow-up Questions

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Questions

- What are the solutions to $F(x, y) = h$?
- How many (integer) solutions are there to $F(x, y) = h$?

Follow-up Questions

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue equation, $F(x, y) = h$.

Questions

- What are the solutions to $F(x, y) = h$?
- How many (integer) solutions are there to $F(x, y) = h$?
- On which features of $F(x, y)$ and h do the number of solutions depend?

Manageable Follow-up Questions

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue inequality, $|F(x,y)| \leqslant h$.

Questions

- What are the solutions to $|F(x,y)| \leqslant h$?
- How many (integer) solutions are there to $|F(x,y)| \leqslant h$?
- On which features of $F(x,y)$ and h do the number of solutions depend?

Manageable Follow-up Questions

Theorem (Thue, 1909)

There are finitely many integer solutions to any Thue inequality, $|F(x, y)| \leqslant h$.

Questions

- What are the solutions to $|F(x, y)| \leqslant h$?
- How many (integer) solutions are there to $|F(x, y)| \leqslant h$?
- On which features of $F(x, y)$ and h do the number of solutions depend?

We'll answer the last question first.

Relevant Parameters

Notation

- Let $F(x, y)$ be an irreducible integral binary form of degree $\geqslant 3$.

Relevant Parameters

Notation

- Let $F(x, y)$ be an irreducible integral binary form of degree $\geqslant 3$.
  - Set $n = \deg(F)$.

Relevant Parameters

Notation

- Let $F(x,y)$ be an irreducible integral binary form of degree $\geqslant 3$.
  - Set $n = \deg(F)$.
  - Suppose that F has $s+1$ nonzero summands: i.e.

$$F(x,y) = \sum_{i=0}^{s} a_i x^{n_i} y^{n-n_i}.$$

Relevant Parameters

Notation

- Let $F(x, y)$ be an irreducible integral binary form of degree $\geqslant 3$.
  - Set $n = \deg(F)$.
  - Suppose that F has $s + 1$ nonzero summands: i.e.

$$F(x, y) = \sum_{i=0}^{s} a_i x^{n_i} y^{n-n_i}.$$

  - Set $H = \max_i |a_i|$ to be the height of F.

Relevant Parameters

Notation

- Let $F(x, y)$ be an irreducible integral binary form of degree $\geqslant 3$.
  - Set $n = \deg(F)$.
  - Suppose that F has $s + 1$ nonzero summands: i.e.

$$F(x, y) = \sum_{i=0}^{s} a_i x^{n_i} y^{n-n_i}.$$

  - Set $H = \max_i |a_i|$ to be the height of F.
- Example: $F(x, y) = x^6 - 2x^4y^2 + 10x^2y^4 + 10y^6$

Relevant Parameters

Notation

- Let $F(x,y)$ be an irreducible integral binary form of degree $\geqslant 3$.
  - Set $n = \deg(F)$.
  - Suppose that F has $s+1$ nonzero summands: i.e.

$$F(x,y) = \sum_{i=0}^{s} a_i x^{n_i} y^{n-n_i}.$$

  - Set $H = \max_i |a_i|$ to be the height of F.
- Example: $F(x,y) = x^6 - 2x^4y^2 + 10x^2y^4 + 10y^6$
  - $n = 6$

Relevant Parameters

Notation

- Let $F(x,y)$ be an irreducible integral binary form of degree $\geqslant 3$.
  - Set $n = \deg(F)$.
  - Suppose that F has $s+1$ nonzero summands: i.e.

$$F(x,y) = \sum_{i=0}^{s} a_i x^{n_i} y^{n-n_i}.$$

  - Set $H = \max_i |a_i|$ to be the height of F.
- Example: $F(x,y) = x^6 - 2x^4y^2 + 10x^2y^4 + 10y^6$
  - $n = 6$
  - $s = 3$

Relevant Parameters

Notation

- Let $F(x, y)$ be an irreducible integral binary form of degree $\geqslant 3$.
  - Set $n = \deg(F)$.
  - Suppose that F has $s + 1$ nonzero summands: i.e.

$$F(x, y) = \sum_{i=0}^{s} a_i x^{n_i} y^{n-n_i}.$$

  - Set $H = \max_i |a_i|$ to be the height of F.
- Example: $F(x, y) = x^6 - 2x^4y^2 + 10x^2y^4 + 10y^6$
  - $n = 6$
  - $s = 3$
  - $H = 10$

Relevant Parameters

Notation

- Let $F(x, y)$ be an irreducible integral binary form of degree $\geqslant 3$.
  - Set $n = \deg(F)$.
  - Suppose that F has $s + 1$ nonzero summands: i.e.

$$F(x, y) = \sum_{i=0}^{s} a_i x^{n_i} y^{n-n_i}.$$

  - Set $H = \max_i |a_i|$ to be the height of F.
- Example: $F(x, y) = x^6 - 2x^4y^2 + 10x^2y^4 + 10y^6$
  - $n = 6$
  - $s = 3$
  - $H = 10$
- Let $h \in \mathbb{Z}_{>0}$

Why s?

Height and degree are commonly used to describe complexity.

Why s?

Height and degree are commonly used to describe complexity.

Question

Why is the number of nonzero summands of $F(x, y)$ relevant?

Why s?

Height and degree are commonly used to describe complexity.

Question

Why is the number of nonzero summands of $F(x, y)$ relevant?

Answer

- Recall that if $F(p, q) = h$, then $\frac{p}{q}$ is close to a root of $f(X) := F(X, 1)$.

Why s?

Height and degree are commonly used to describe complexity.

Question

Why is the number of nonzero summands of $F(x, y)$ relevant?

Answer

- Recall that if $F(p, q) = h$, then $\frac{p}{q}$ is close to a root of $f(X) := F(X, 1)$.
- Intuitively, $\frac{p}{q}$ is unlikely to be close to a nonreal root of $f(X)$.

Why s?

Height and degree are commonly used to describe complexity.

Question

Why is the number of nonzero summands of $F(x, y)$ relevant?

Answer

- Recall that if $F(p, q) = h$, then $\frac{p}{q}$ is close to a root of $f(X) := F(X, 1)$.
- Intuitively, $\frac{p}{q}$ is unlikely to be close to a nonreal root of $f(X)$.
- Solutions to $F(x, y) = h$ "should" correspond to rational approximations to real roots of $f(X)$.

Why s?

Height and degree are commonly used to describe complexity.

Question

Why is the number of nonzero summands of $F(x, y)$ relevant?

Answer

- Recall that if $F(p, q) = h$, then $\frac{p}{q}$ is close to a root of $f(X) := F(X, 1)$.
- Intuitively, $\frac{p}{q}$ is unlikely to be close to a nonreal root of $f(X)$.
- Solutions to $F(x, y) = h$ "should" correspond to rational approximations to real roots of $f(X)$.

Note

This is where polynomial root *distribution* impacts solutions to Thue equations.

Why s?

Height and degree are commonly used to describe complexity.

Question

Why is the number of nonzero summands of $F(x, y)$ relevant?

Answer

- Recall that if $F(p, q) = h$, then $\frac{p}{q}$ is close to a root of $f(X) := F(X, 1)$.
- Intuitively, $\frac{p}{q}$ is unlikely to be close to a nonreal root of $f(X)$.
- Solutions to $F(x, y) = h$ "should" correspond to rational approximations to real roots of $f(X)$.

Lemma (Descartes, 1637)

If $g(x) \in \mathbb{R}[x]$ has $s + 1$ nonzero summands, then $g(x)$ has no more than $2s + 1$ real roots.

Parameter Summary

Goal

Bound the number of (integer) solutions to $|F(x, y)| \leqslant h$ in terms of n (the degree of F), s (the number of nonzero summands of F), and h.

Parameter Summary

Goal

Bound the number of (integer) solutions to $|F(x,y)| \leqslant h$ in terms of n (the degree of F), s (the number of nonzero summands of F), and h.

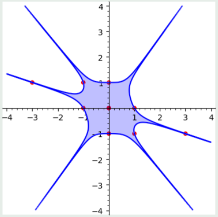
Notation

Let $N(F,h)$ denote the number of integer solutions to the Thue inequality $|F(x,y)| \leqslant h$.

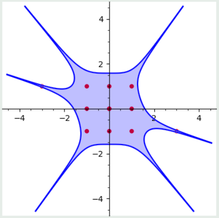
Geometric View of $|F(x,y)| \leqslant h$

A Picture

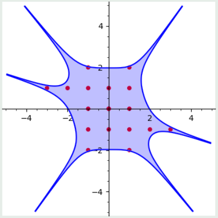
$|F(x,y)| \leqslant h$ corresponds to a region of the xy-plane:



$|x^5 + 3x^4y - y^5| \leqslant 1$



$|x^5 + 3x^4y - y^5| \leqslant 10$

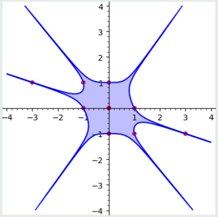


$|x^5 + 3x^4y - y^5| \leqslant 30$

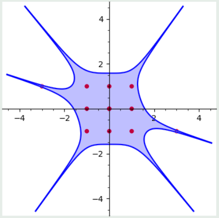
Geometric View of $|F(x,y)| \leqslant h$

A Picture

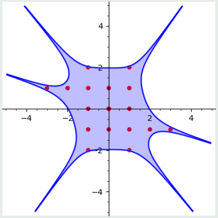
$|F(x,y)| \leqslant h$ corresponds to a region of the xy-plane:



$|x^5 + 3x^4y - y^5| \leqslant 1$



$|x^5 + 3x^4y - y^5| \leqslant 10$



$|x^5 + 3x^4y - y^5| \leqslant 30$

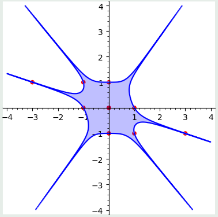
Computing $N(F,h)$

Some values of $N(F,h)$ for $F(x,y) = x^5 + 3x^4y - y^5$:

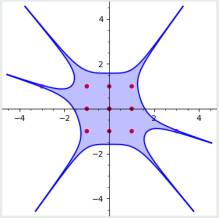
Geometric View of $|F(x,y)| \leqslant h$

A Picture

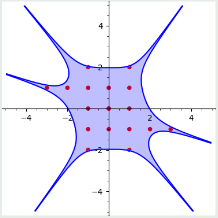
$|F(x,y)| \leqslant h$ corresponds to a region of the xy-plane:



$|x^5 + 3x^4y - y^5| \leqslant 1$



$|x^5 + 3x^4y - y^5| \leqslant 10$



$|x^5 + 3x^4y - y^5| \leqslant 30$

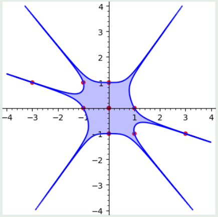
Computing $N(F,h)$

Some values of $N(F,h)$ for $F(x,y) = x^5 + 3x^4y - y^5$:

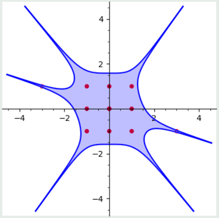
h	1	10	30
$N(F,h)$	9	11	17

Exploring Dependence on h

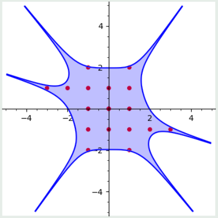
A Picture



$$|x^5 + 3x^4y - y^5| \leqslant 1$$



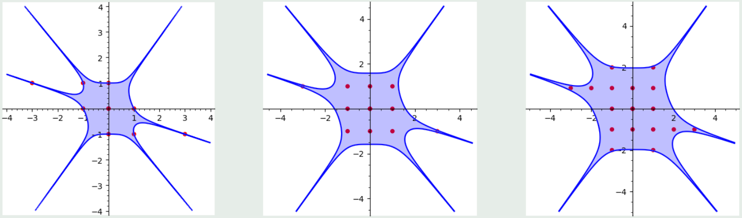
$$|x^5 + 3x^4y - y^5| \leqslant 10$$



$$|x^5 + 3x^4y - y^5| \leqslant 30$$

Exploring Dependence on h

A Picture



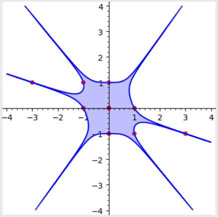
$|x^5 + 3x^4y - y^5| \leqslant 1$ $\quad$ $|x^5 + 3x^4y - y^5| \leqslant 10$ $\quad$ $|x^5 + 3x^4y - y^5| \leqslant 30$

$N(F, h)$ and volume

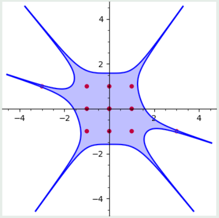
$$N(F,h) = \text{number of lattice points ``inside'' } |F(x,y)| \leqslant h$$

Exploring Dependence on h

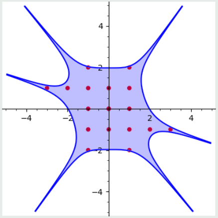
A Picture



$|x^5 + 3x^4y - y^5| \leqslant 1$



$|x^5 + 3x^4y - y^5| \leqslant 10$



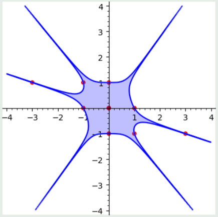
$|x^5 + 3x^4y - y^5| \leqslant 30$

$N(F,h)$ and volume

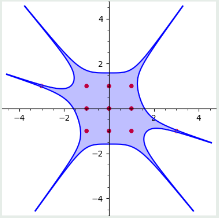
$$N(F,h) = \text{number of lattice points "inside" } |F(x,y)| \leqslant h$$
$$\approx \operatorname{vol}\{(x,y) \in \mathbb{R}^2 : |F(x,y)| \leqslant h\}$$

Exploring Dependence on h

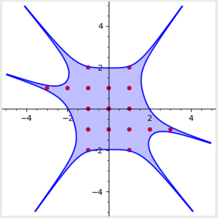
A Picture



$|x^5 + 3x^4y - y^5| \leqslant 1$



$|x^5 + 3x^4y - y^5| \leqslant 10$



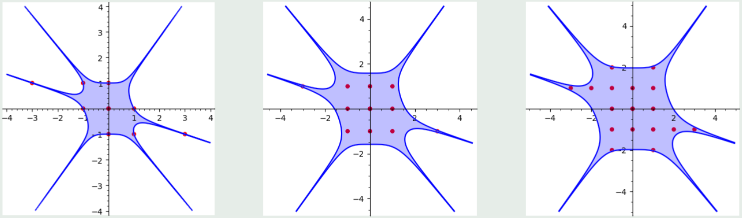
$|x^5 + 3x^4y - y^5| \leqslant 30$

$N(F,h)$ and volume

$$\begin{aligned} N(F,h) &= \text{number of lattice points "inside" } |F(x,y)| \leqslant h \\ &\approx \operatorname{vol}\{(x,y) \in \mathbb{R}^2 : |F(x,y)| \leqslant h\} \\ &= h^{2/n} \operatorname{vol}\{(u,v) \in \mathbb{R}^2 : |F(u,v)| \leqslant 1\} \end{aligned}$$

Exploring Dependence on h

A Picture



$|x^5 + 3x^4y - y^5| \leqslant 1$ $\quad$ $|x^5 + 3x^4y - y^5| \leqslant 10$ $\quad$ $|x^5 + 3x^4y - y^5| \leqslant 30$

$N(F, h)$ and volume

$$\begin{aligned} N(F,h) &= \text{number of lattice points “inside” } |F(x,y)| \leqslant h \\ &\approx \operatorname{vol}\{(x,y) \in \mathbb{R}^2 : |F(x,y)| \leqslant h\} \\ &= h^{2/n} \operatorname{vol}\{(u,v) \in \mathbb{R}^2 : |F(u,v)| \leqslant 1\} \\ &\approx h^{2/n} N(F,1) \end{aligned}$$

Exploring dependence on h

Theorem (Mahler, 1934)

Let

$$V(F,1) := \mathrm{vol}\{(x,y) \in \mathbb{R}^2 : |F(x,y)| \leqslant 1\}.$$

Then

$$N(F,h) \asymp h^{2/n} V(F,1)$$

Exploring dependence on h

Theorem (Mahler, 1934)

Let

$$V(F,1) := \mathrm{vol}\{(x,y) \in \mathbb{R}^2 : |F(x,y)| \leqslant 1\}.$$

Then

$$N(F,h) \asymp h^{2/n} V(F,1)$$

i.e. there are constants C_1 *and* C_2 *so that*

$$C_1 h^{2/n} V(F,1) \leqslant N(F,h) \leqslant C_2 h^{2/n} V(F,1).$$

Exploring dependence on h

Theorem (Mahler, 1934)

Let

$$V(F,1) := \mathrm{vol}\{(x,y) \in \mathbb{R}^2 : |F(x,y)| \leqslant 1\}.$$

Then

$$N(F,h) \asymp h^{2/n} V(F,1)$$

i.e. there are constants C_1 and C_2 so that

$$C_1 h^{2/n} V(F,1) \leqslant N(F,h) \leqslant C_2 h^{2/n} V(F,1).$$

Moral

The factor of $h^{2/n}$ is necessary and sufficient and we expect

$$N(F,h) \approx h^{2/n} \cdot N(F,1).$$

Exploring $N(F, 1)$

Previous Facts

- Solutions (p, q) to $|F(x, y)| \leqslant 1$ correspond to rational approximations of some root of $f(X) := F(X, 1)$.

Exploring $N(F, 1)$

Previous Facts

- Solutions (p, q) to $|F(x, y)| \leqslant 1$ correspond to rational approximations of some root of $f(X) := F(X, 1)$.
- We expect solutions to produce rational approximations of *real* roots of $f(X)$.

Exploring $N(F, 1)$

Previous Facts

- Solutions (p, q) to $|F(x, y)| \leqslant 1$ correspond to rational approximations of some root of $f(X) := F(X, 1)$.
- We expect solutions to produce rational approximations of *real* roots of $f(X)$.
- There are $s + 1$ nonzero summands of $F(x, y)$.

Exploring $N(F,1)$

Previous Facts

- Solutions (p,q) to $|F(x,y)| \leqslant 1$ correspond to rational approximations of some root of $f(X) := F(X,1)$.
- We expect solutions to produce rational approximations of *real* roots of $f(X)$.
- There are $s+1$ nonzero summands of $F(x,y)$.
- There are at most $2s+1$ real roots of $f(X)$.

Exploring $N(F, 1)$

Previous Facts

- Solutions (p, q) to $|F(x, y)| \leqslant 1$ correspond to rational approximations of some root of $f(X) := F(X, 1)$.
- We expect solutions to produce rational approximations of *real* roots of $f(X)$.
- There are $s + 1$ nonzero summands of $F(x, y)$.
- There are at most $2s + 1$ real roots of $f(X)$.

Number of Approximations per Root

Based on some approximation theorems, we expect the number of rational approximations per root to be absolutely bounded.

Exploring $N(F, 1)$

Previous Facts

- Solutions (p, q) to $|F(x, y)| \leqslant 1$ correspond to rational approximations of some root of $f(X) := F(X, 1)$.
- We expect solutions to produce rational approximations of *real* roots of $f(X)$.
- There are $s + 1$ nonzero summands of $F(x, y)$.
- There are at most $2s + 1$ real roots of $f(X)$.

Number of Approximations per Root

Based on some approximation theorems, we expect the number of rational approximations per root to be absolutely bounded.

Conclusion

We expect there to be no more than a constant times s solutions to $|F(x, y)| \leqslant 1$.

Useful Notation

Notation

- $f(x) \ll g(x)$ means that there exists an absolute constant C so that $f(x) \leqslant C \cdot g(x)$.

Useful Notation

Notation

- $f(x) \ll g(x)$ means that there exists an absolute constant C so that $f(x) \leqslant C \cdot g(x)$.
- $f(x) \ll_n g(x)$ means that there exists a constant C depending on n so that $f(x) \leqslant C \cdot g(x)$.

Useful Notation

Notation

- $f(x) \ll g(x)$ means that there exists an absolute constant C so that $f(x) \leqslant C \cdot g(x)$.
- $f(x) \ll_n g(x)$ means that there exists a constant C depending on n so that $f(x) \leqslant C \cdot g(x)$.

Meaning

The symbol $\ll$ means "(is) no more than a constant times."

Useful Notation

Notation

- $f(x) \ll g(x)$ means that there exists an absolute constant C so that $f(x) \leqslant C \cdot g(x)$.
- $f(x) \ll_n g(x)$ means that there exists a constant C depending on n so that $f(x) \leqslant C \cdot g(x)$.

Meaning

The symbol $\ll$ means "(is) no more than a constant times."

Conclusion (rephrased)

We expect there to be $\ll s$ solutions to $|F(x, y)| \leqslant 1$.

A Conjecture and Theorem of Mueller and Schmidt

The Pieces

Recall that we expect:

$$N(F,h) \approx h^{2/n} \cdot N(F,1)$$
$$N(F,1) \ll s$$

A Conjecture and Theorem of Mueller and Schmidt

The Pieces

Recall that we expect:

$$N(F, h) \approx h^{2/n} \cdot N(F, 1)$$
$$N(F, 1) \ll s$$

Conjecture (Mueller and Schmidt, 1987)

$$N(F, h) \ll sh^{2/n}$$

A Conjecture and Theorem of Mueller and Schmidt

The Pieces

Recall that we expect:

$$N(F,h) \approx h^{2/n} \cdot N(F,1)$$
$$N(F,1) \ll s$$

Conjecture (Mueller and Schmidt, 1987)

$$N(F,h) \ll sh^{2/n}$$

Theorem (Mueller and Schmidt, 1987)

$$N(F,h) \ll s^2 h^{2/n}(1 + \log h^{1/n})$$

Picking Values for s and h

Theorem (Bennett, 2001)

$ax^n - by^n = 1$ *has at most one solution in positive integers* x *and* y*.*

Picking Values for s and h

Theorem (Bennett, 2001)

$ax^n - by^n = 1$ has at most one solution in positive integers x and y.

Theorem (Thomas, 2000)

For $n \geqslant 39$ and $F(x, y) = ax^n + bx^ky^{n-k} + cy^n$, the number of solutions to $|F(x, y)| = 1$ is less than or equal to 48.

Types of Solutions

Separating Solutions

- Begin by choosing some (explicit) constants $0 < Y_S < Y_L$ which depend on F.

Types of Solutions

Separating Solutions

- Begin by choosing some (explicit) constants $0 < Y_S < Y_L$ which depend on F.
- Then we say that a solution to $|F(x, y)| \leqslant h$ is...
  - ...small if $\min(|x|, |y|) \leqslant Y_S$.

Types of Solutions

Separating Solutions

- Begin by choosing some (explicit) constants $0 < Y_S < Y_L$ which depend on F.
- Then we say that a solution to $|F(x,y)| \leqslant h$ is...
  - ...<u>small</u> if $\min(|x|,|y|) \leqslant Y_S$.
  - ...<u>medium</u> if $\min(|x|,|y|) > Y_S$ and $\max(|x|,|y|) \leqslant Y_L$.

Types of Solutions

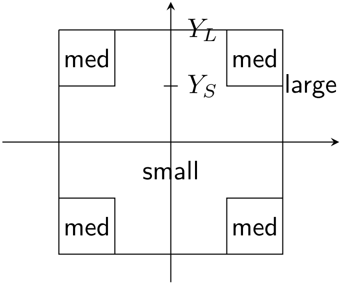
Separating Solutions

- Begin by choosing some (explicit) constants $0 < Y_S < Y_L$ which depend on F.
- Then we say that a solution to $|F(x, y)| \leqslant h$ is...
  - ...small if $\min(|x|, |y|) \leqslant Y_S$.
  - ...medium if $\min(|x|, |y|) > Y_S$ and $\max(|x|, |y|) \leqslant Y_L$.
  - ...large if $\max(|x|, |y|) > Y_L$.

Types of Solutions

Separating Solutions

- Begin by choosing some (explicit) constants $0 < Y_S < Y_L$ which depend on F.
- Then we say that a solution to $|F(x, y)| \leqslant h$ is...
  - ...small if $\min(|x|, |y|) \leqslant Y_S$.
  - ...medium if $\min(|x|, |y|) > Y_S$ and $\max(|x|, |y|) \leqslant Y_L$.
  - ...large if $\max(|x|, |y|) > Y_L$.



The Gap Principle

The Gap Principle

- Medium solutions to $|F(x, y)| \leqslant h$ produce good approximations to some small set of algebraic numbers (Mueller and Schmidt, 1987).

The Gap Principle

The Gap Principle

- Medium solutions to $|F(x,y)| \leqslant h$ produce good approximations to some small set of algebraic numbers (Mueller and Schmidt, 1987).
- Fix one of those algebraic numbers, α, and note that the good rational approximations of α must be close to each other.

The Gap Principle

The Gap Principle

- Medium solutions to $|F(x, y)| \leqslant h$ produce good approximations to some small set of algebraic numbers (Mueller and Schmidt, 1987).
- Fix one of those algebraic numbers, α, and note that the good rational approximations of α must be close to each other.
- Manipulate inequalities to find that the denominators of the rational functions must be exponentially far apart.

Counting Medium Solutions

Our improvement involves efficiently bounding t in the situation where both

$$Y_S \leqslant q_0 < q_1 < \cdots < q_t \leqslant Y_L$$

and the inductive relation

$$q_{i+1} > \frac{q_i^{\frac{n}{s}-1}}{K}$$

hold.

Counting Medium Solutions

Our improvement involves efficiently bounding t in the situation where both

$$Y_S \leqslant q_0 < q_1 < \cdots < q_t \leqslant Y_L$$

and the inductive relation

$$q_{i+1} > \frac{q_i^{\frac{n}{s}-1}}{K}$$

hold.

Lemma (K., 2021)

If $n \geqslant 3s$ and there are $t+1$ medium solutions associated to α, then

$$t \leqslant \frac{\log\left[\frac{\log Y_L K^{-1/(\frac{n}{s}-2)}}{\log Y_S K^{-1/(\frac{n}{s}-2)}}\right]}{\log\left(\frac{n}{s}-1\right)}.$$

Moreover, this bound is as sharp as possible, given existing approximation results.

Counting Solutions

Theorem (K., 2021)

The number of primitive medium solutions to $|F(x, y)| \leqslant h$ when $n \geqslant 3s$ is

$$\ll s\left(1 + \log\left(s + \frac{\log h}{\max(1, \log H)}\right)\right)$$

Counting Solutions

Theorem (K., 2021)

The number of primitive medium solutions to $|F(x,y)| \leqslant h$ when $n \geqslant 3s$ is

$$\ll s\left(1 + \log\left(s + \frac{\log h}{\max(1, \log H)}\right)\right)$$

Bounds for Small and Large Solutions

- The number of large primitive solutions is $\ll s$ (Mueller and Schmidt, 1987).

Counting Solutions

Theorem (K., 2021)

The number of primitive medium solutions to $|F(x,y)| \leqslant h$ when $n \geqslant 3s$ is

$$\ll s\left(1 + \log\left(s + \frac{\log h}{\max(1, \log H)}\right)\right)$$

Bounds for Small and Large Solutions

- The number of large primitive solutions is $\ll s$ (Mueller and Schmidt, 1987).
- The number of small primitive solutions is $\ll se^{\Phi}h^{2/n}$ when $n > 4se^{2\Phi}$ (Saradha and Sharma, 2017).

Note: Φ measures the "sparsity" of F and satisfies $\log^3 s \leqslant e^{\Phi} \ll s$.

Asymptotic Bounds

As a consequence:

Theorem (K., 2023)

When $n > 4se^{2\Phi}$, the number of primitive solutions to $|F(x,y)| \leqslant h$ is

$$\ll se^{\Phi}h^{2/n}.$$

Recall that $\log^3 s \leqslant e^{\Phi} \ll s$.

Asymptotic Bounds

As a consequence:

Theorem (K., 2023)

When $n > 4se^{2\Phi}$, the number of primitive solutions to $|F(x,y)| \leqslant h$ is

$$\ll se^{\Phi}h^{2/n}.$$

Recall that $\log^3 s \leqslant e^{\Phi} \ll s$.

Compare to:

Theorem (Mueller and Schmidt, 1987)

The number of integer pair solutions to $|F(x,y)| \leqslant h$ is

$$\ll s^2 h^{2/n}(1 + \log h^{1/n}).$$

Explicit Bounds for Trinomials

Theorem (Thomas, 2000)

If $F(x,y) = ax^n + bx^k y^{n-k} + cy^n$*, there are no more than* $C_1(n)$ *solutions to* $|F(x,y)| = 1$ *where* $C_1(n)$ *is defined by*

n	6	7	8	9	10-11	12-16	17-37	$\geqslant 38$
$C_1(n)$	136	86	96	62	72	60	56	48

Explicit Bounds for Trinomials

Theorem (Thomas, 2000)

If $F(x,y) = ax^n + bx^ky^{n-k} + cy^n$, there are no more than $C_1(n)$ solutions to $|F(x,y)| = 1$ where $C_1(n)$ is defined by

n	6	7	8	9	10-11	12-16	17-37	$\geqslant 38$
$C_1(n)$	136	86	96	62	72	60	56	48

Theorem (K., 2021)

The above theorem is still true with $C_1(n)$ replaced by $C_2(n)$:

n	6	7	8-216	$\geqslant 217$
$C_2(n)$	128	80	$C_1(n)$	40

Explicit Bounds for Trinomials

Theorem (Thomas, 2000)

If $F(x,y) = ax^n + bx^k y^{n-k} + cy^n$, there are no more than $C_1(n)$ solutions to $|F(x,y)| = 1$ where $C_1(n)$ is defined by

n	6	7	8	9	10-11	12-16	17-37	$\geqslant 38$
$C_1(n)$	136	86	96	62	72	60	56	48

Theorem (K., 2021)

The above theorem is still true with $C_1(n)$ replaced by $C_2(n)$:

n	6	7	8-216	$\geqslant 217$
$C_2(n)$	128	80	$C_1(n)$	40

Question

Is this a good bound?

Trinomial Computations

H	1	2	3	4	5	6	7	8	9	10	$\cdots$	16
$n = 6$	8	6	8	8	6	6	6	6	8	6	-	12
$n = 7$	8	6	8	8	6	6	6	6	8	6	-	8
$n = 8$	8	6	8	8	6	6	6	6	8	6	-	12
$n = 9$	8	6	8	8	6	6	6	6	8	6	-	8
$n = 10$	8	6	8	8	6	6	6	6	8	-	-	-
$n = 11$	8	6	8	8	6	6	6	6	8	-	-	-
$n = 12$	8	6	8	8	6	6	6	-	-	-	-	-
$n = 13$	8	6	8	8	6	6	-	-	-	-	-	-
$n = 14$	8	6	8	8	6	6	-	-	-	-	-	-
$n = 15$	8	6	8	8	6	-	-	-	-	-	-	-
$n = 16$	8	6	8	8	6	-	-	-	-	-	-	-
$n = 17$	8	6	8	8	-	-	-	-	-	-	-	-

Maximum number of solutions to $|F(x, y)| = 1$ for any trinomial of height H and degree n

Thue Equation Summary

New Results

- We improve a counting technique associated with “The Gap Principle.”

Thue Equation Summary

New Results

- We improve a counting technique associated with "The Gap Principle."
- We improve "asymptotic" bounds on the number of solutions to $|F(x,y)| \leqslant h$.

Thue Equation Summary

New Results

- We improve a counting technique associated with "The Gap Principle."
- We improve "asymptotic" bounds on the number of solutions to $|F(x,y)| \leqslant h$.
- We improve explicit bounds on the number of solutions to $|F(x,y)| = 1$ when $F(x,y)$ is a trinomial.

Thue Equation Summary

New Results

- We improve a counting technique associated with "The Gap Principle."
- We improve "asymptotic" bounds on the number of solutions to $|F(x, y)| \leqslant h$.
- We improve explicit bounds on the number of solutions to $|F(x, y)| = 1$ when $F(x, y)$ is a trinomial.

Questions

Any question on Thue equations?

Ingredients

Definitions

Let

$$f(x) = \sum_{i=0}^{n} b_i x^i$$

Ingredients

Definitions

Let

$$f(x) = \sum_{i=0}^{n} b_i x^i = b_n \prod_{j=1}^{n} (x - \alpha_j) \in \mathbb{C}[x].$$

Ingredients

Definitions

Let

$$f(x) = \sum_{i=0}^{n} b_i x^i = b_n \prod_{j=1}^{n} (x - \alpha_j) \in \mathbb{C}[x].$$

Notation	Definition	Name

Ingredients

Definitions

Let

$$f(x) = \sum_{i=0}^{n} b_i x^i = b_n \prod_{j=1}^{n} (x - \alpha_j) \in \mathbb{C}[x].$$

Notation	Definition	Name
$H(f)$	$\max\limits_{0 \leqslant i \leqslant n} \lvert b_i \rvert$	height

Ingredients

Definitions

Let

$$f(x) = \sum_{i=0}^{n} b_i x^i = b_n \prod_{j=1}^{n} (x - \alpha_j) \in \mathbb{C}[x].$$

Notation	Definition	Name
$H(f)$	$\max\limits_{0 \leqslant i \leqslant n} \lvert b_i \rvert$	height
$M(f)$	$\lvert b_n \rvert \prod_{j=1}^{n} \max(1, \lvert \alpha_j \rvert)$	Mahler measure

Ingredients

Definitions

Let

$$f(x) = \sum_{i=0}^{n} b_i x^i = b_n \prod_{j=1}^{n} (x - \alpha_j) \in \mathbb{C}[x].$$

Notation	Definition	Name
$H(f)$	$\max\limits_{0 \leqslant i \leqslant n} \lvert b_i \rvert$	height
$M(f)$	$\lvert b_n \rvert \prod\limits_{j=1}^{n} \max(1, \lvert \alpha_j \rvert)$	Mahler measure
$\operatorname{sep}(f)$	$\min\limits_{\alpha_i \neq \alpha_j} \lvert \alpha_i - \alpha_j \rvert$	separation

Ingredients

Definitions

Let

$$f(x) = \sum_{i=0}^{n} b_i x^i = b_n \prod_{j=1}^{n} (x - \alpha_j) \in \mathbb{C}[x].$$

Notation	Definition	Name
$H(f)$	$\max\limits_{0 \leqslant i \leqslant n} \lvert b_i \rvert$	height
$M(f)$	$\lvert b_n \rvert \prod_{j=1}^{n} \max(1, \lvert \alpha_j \rvert)$	Mahler measure
$\text{sep}(f)$	$\min\limits_{\alpha_i \neq \alpha_j} \lvert \alpha_i - \alpha_j \rvert$	separation
$\lvert \Delta_f \rvert$	$\lvert b_n \rvert^{2n-2} \prod\limits_{1 \leqslant i < j \leqslant n} \lvert \alpha_i - \alpha_j \rvert^2$	discriminant

Useful Fact and Motivating Question

Fact

$$\binom{n}{\lfloor n/2 \rfloor}^{-1} H(f) \leqslant M(f) \leqslant \sqrt{n+1} \cdot H(f)$$

Useful Fact and Motivating Question

Fact

$$\binom{n}{\lfloor n/2 \rfloor}^{-1} H(f) \leqslant M(f) \leqslant \sqrt{n+1} \cdot H(f)$$

Meaning

Up to a constant depending on n, $H(f)$ and $M(f)$ are interchangeable.

Useful Fact and Motivating Question

Fact

$$\binom{n}{\lfloor n/2 \rfloor}^{-1} H(f) \leqslant M(f) \leqslant \sqrt{n+1} \cdot H(f)$$

Meaning

Up to a constant depending on n, $H(f)$ and $M(f)$ are interchangeable.

Question

How are Mahler measure and separation related? Can we find bounds on separation in terms of Mahler measure?

Mahler Measure and Separation

Theorem (Mahler, 1964)

For all monic polynomials $f(x) \in \mathbb{C}[x]$ of degree $n \geqslant 2$,

$$\operatorname{sep}(f) > \frac{\sqrt{3}|\Delta_f|^{1/2}}{n^{(n+2)/2} M(f)^{n-1}}.$$

Mahler Measure and Separation

Theorem (Mahler, 1964)

For all monic polynomials $f(x) \in \mathbb{C}[x]$ *of degree* $n \geqslant 2$,

$$\operatorname{sep}(f) > \frac{\sqrt{3}|\Delta_f|^{1/2}}{n^{(n+2)/2} M(f)^{n-1}}.$$

Corollary (Mahler, 1964)

For separable monic $f(x) \in \mathbb{Z}[x]$ *of degree* $n \geqslant 2$,

$$\operatorname{sep}(f) > \frac{\sqrt{3}}{n^{(n+2)/2} M(f)^{n-1}}.$$

Changing Hypotheses

Theorem (Mahler, 1964)

For all separable polynomials $f(x) \in \mathbb{Z}[x]$ of degree $n \geqslant 2$,

$$\mathrm{sep}(f) > \frac{\sqrt{3}}{n^{(n+2)/2} M(f)^{n-1}}.$$

Changing Hypotheses

Theorem (Mahler, 1964)

For all separable polynomials $f(x) \in \mathbb{Z}[x]$ of degree $n \geqslant 2$,

$$\operatorname{sep}(f) > \frac{\sqrt{3}}{n^{(n+2)/2} M(f)^{n-1}}.$$

Theorem (Rump, 1979)

Let $f(x) \in \mathbb{Z}[x]$ have degree $n \geqslant 2$. Then

$$\operatorname{sep}(f) > \frac{1}{2^{n^2+1} n^{n/2+2} M(f)^n}.$$

Changing Hypotheses

Theorem (Mahler, 1964)

For all separable polynomials $f(x) \in \mathbb{Z}[x]$ of degree $n \geqslant 2$,

$$\operatorname{sep}(f) > \frac{\sqrt{3}}{n^{(n+2)/2} M(f)^{n-1}}.$$

Theorem (Rump, 1979)

Let $f(x) \in \mathbb{Z}[x]$ have degree $n \geqslant 2$. Then

$$\operatorname{sep}(f) > \frac{1}{2^{n^2+1} n^{n/2+2} M(f)^n}.$$

Others (Bugeaud, Dujella, Pejković) have results when $f(x)$ is assumed to be (ir)reducible.

Reversing the Question

Upper Bounds?

Each of these quantities deals with an inequality of the form

$$\operatorname{sep}(f) > \frac{C(n)}{M(f)^e}.$$

Reversing the Question

Upper Bounds?

Each of these quantities deals with an inequality of the form

$$\mathrm{sep}(f) > \frac{C(n)}{M(f)^e}.$$

What about an inequality of the form

$$\mathrm{sep}(f) < C(n) \cdot M(f)^e?$$

Reversing the Question

Theorem (Mahler, 1964)

For all polynomials $f(x) \in \mathbb{C}[x]$ *of degree* $n \geqslant 2$*,*

$$\operatorname{sep}(f) > \frac{\sqrt{3}|\Delta_f|^{1/2}}{n^{(n+2)/2} M(f)^{n-1}}.$$

Reversing the Question

Theorem (Mahler, 1964)

For all polynomials $f(x) \in \mathbb{C}[x]$ of degree $n \geqslant 2$,

$$\operatorname{sep}(f) > \frac{\sqrt{3}|\Delta_f|^{1/2}}{n^{(n+2)/2}M(f)^{n-1}}.$$

Observation

Note, however, that for a monic separable polynomial $f(x)$, $|\Delta_f|$ is bounded below in terms of separation:

Reversing the Question

Theorem (Mahler, 1964)

For all polynomials $f(x) \in \mathbb{C}[x]$ of degree $n \geqslant 2$,

$$\operatorname{sep}(f) > \frac{\sqrt{3}|\Delta_f|^{1/2}}{n^{(n+2)/2} M(f)^{n-1}}.$$

Observation

Note, however, that for a monic separable polynomial $f(x)$, $|\Delta_f|$ is bounded below in terms of separation:

$$|\Delta_f| = \prod_{1 \leqslant i < j \leqslant n} |\alpha_i - \alpha_j|^2$$

Reversing the Question

Theorem (Mahler, 1964)

For all polynomials $f(x) \in \mathbb{C}[x]$ of degree $n \geqslant 2$,

$$\operatorname{sep}(f) > \frac{\sqrt{3}|\Delta_f|^{1/2}}{n^{(n+2)/2} M(f)^{n-1}}.$$

Observation

Note, however, that for a monic separable polynomial $f(x)$, $|\Delta_f|$ is bounded below in terms of separation:

$$\begin{aligned} |\Delta_f| &= \prod_{1 \leqslant i < j \leqslant n} |\alpha_i - \alpha_j|^2 \\ &\geqslant \operatorname{sep}(f)^{n(n-1)} \end{aligned}$$

Motivating Question

Inequality manipulation yields

$$\operatorname{sep}(f) < n^{\frac{1}{n-3}} M(f)^{\frac{2}{n-\frac{1}{2}}} \approx M(f)^{2/n}.$$

Motivating Question

Inequality manipulation yields

$$\operatorname{sep}(f) < n^{\frac{1}{n-3}} M(f)^{\frac{2}{n-\frac{1}{2}}} \approx M(f)^{2/n}.$$

Question

Can we get a better exponent in the relation

$$\operatorname{sep}(f) \ll M(f)^{2/(n-1/2)}?$$

Collecting Data

Algorithm

1. Pick a random monic polynomial of degree n in $\mathbb{R}[x]$.

Collecting Data

Algorithm

1. Pick a random monic polynomial of degree n in $\mathbb{R}[x]$.
2. Compute its separation, $\operatorname{sep}(f)$.

Collecting Data

Algorithm

1. Pick a random monic polynomial of degree n in $\mathbb{R}[x]$.
2. Compute its separation, $\operatorname{sep}(f)$.
3. Compute its Mahler measure, $M(f)$.

Collecting Data

Algorithm

1. Pick a random monic polynomial of degree n in $\mathbb{R}[x]$.
2. Compute its separation, $\mathrm{sep}(f)$.
3. Compute its Mahler measure, $M(f)$.
4. Plot the pair $(M(f), \mathrm{sep}(f))$.

Collecting Data

Algorithm

1. Pick a random monic polynomial of degree n in $\mathbb{R}[x]$.
2. Compute its separation, $\operatorname{sep}(f)$.
3. Compute its Mahler measure, $M(f)$.
4. Plot the pair $(M(f), \operatorname{sep}(f))$.
5. Repeat many times.

Collecting Data

Algorithm

1. Pick a random monic polynomial of degree n in $\mathbb{R}[x]$.
2. Compute its separation, $\operatorname{sep}(f)$.
3. Compute its Mahler measure, $M(f)$.
4. Plot the pair $(M(f), \operatorname{sep}(f))$.
5. Repeat many times.

"Random" Polynomials

A "random" polynomial is a polynomial whose roots are sampled according to a uniform distribution in an appropriate region of $\mathbb{C}$.

Data for Quartics

Cases

- Quartics provide a good case for data collection because they have three distinct signatures:

Data for Quartics

Cases

- Quartics provide a good case for data collection because they have three distinct signatures:
  - Four real roots
    - Signature $(4, 0)$

Data for Quartics

Cases

- Quartics provide a good case for data collection because they have three distinct signatures:
  - Four real roots
    - Signature $(4, 0)$
  - Two real roots and one pair of complex conjugate roots
    - Signature $(2, 1)$

Data for Quartics

Cases

- Quartics provide a good case for data collection because they have three distinct signatures:
  - Four real roots
    - Signature $(4, 0)$
  - Two real roots and one pair of complex conjugate roots
    - Signature $(2, 1)$
  - Two pairs of complex conjugate roots
    - Signature $(0, 2)$

Data for Quartics

Cases

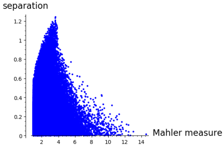
- Quartics provide a good case for data collection because they have three distinct signatures:
  - Four real roots
    - Signature $(4, 0)$
  - Two real roots and one pair of complex conjugate roots
    - Signature $(2, 1)$
  - Two pairs of complex conjugate roots
    - Signature $(0, 2)$
- We can illustrate the difference between these cases as follows.

Data for Quartics

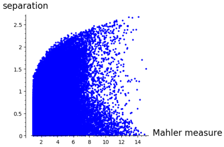
Here are the results of selecting 50,000 random polynomials with real coefficients of a specified signature and plotting their Mahler measure against their separation:

Data for Quartics

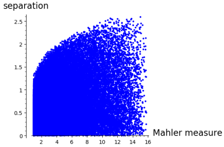
Here are the results of selecting 50,000 random polynomials with real coefficients of a specified signature and plotting their Mahler measure against their separation:



Signature $(4, 0)$



Signature $(2, 1)$



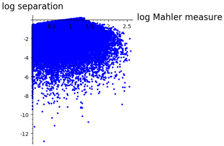
Signature $(0, 2)$

Log-Log Data for Quartics

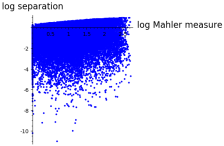
Here are the results of selecting 50,000 random polynomials with real coefficients of a specified signature and plotting their logarithmic Mahler measure against their logarithmic separation:

Log-Log Data for Quartics

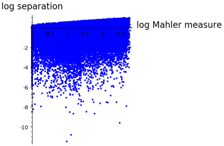
Here are the results of selecting 50,000 random polynomials with real coefficients of a specified signature and plotting their logarithmic Mahler measure against their logarithmic separation:



Signature $(4, 0)$



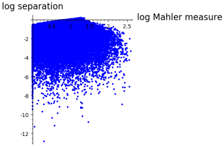
Signature $(2, 1)$



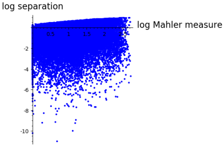
Signature $(0, 2)$

Log-Log Data for Quartics

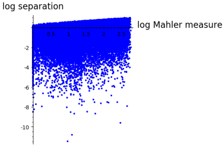
Here are the results of selecting 50,000 random polynomials with real coefficients of a specified signature and plotting their logarithmic Mahler measure against their logarithmic separation:



Signature $(4, 0)$



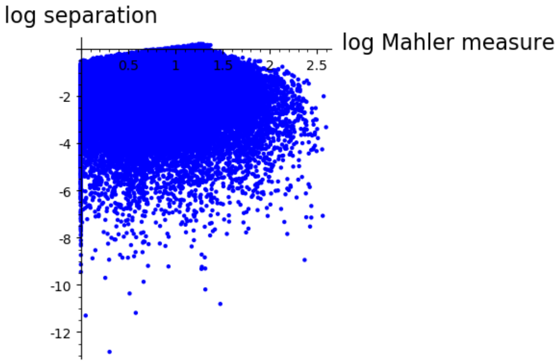
Signature $(2, 1)$



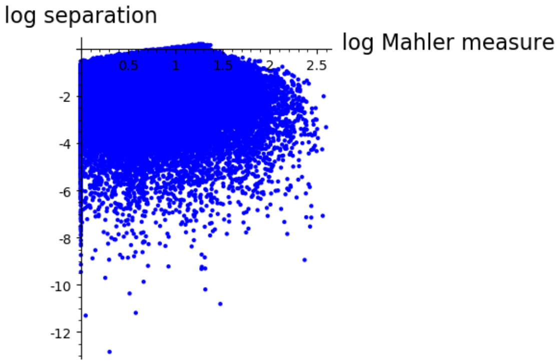
Signature $(0, 2)$

The logarithmic separation appears to be bounded above by a linear function of the logarithmic Mahler measure.

Discerning the Upper Bound: Signature $(4, 0)$



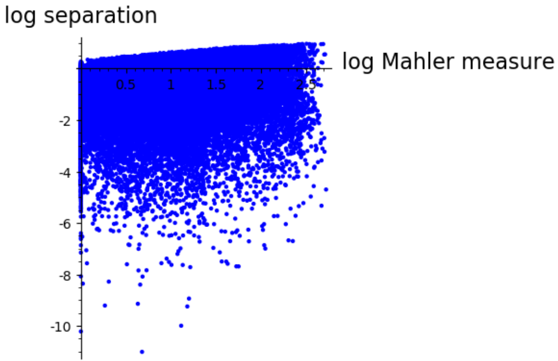
Discerning the Upper Bound: Signature $(4, 0)$



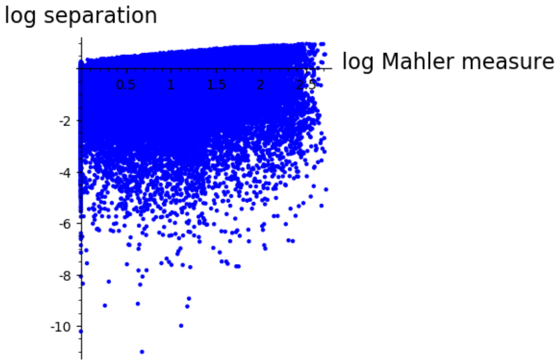
The upper bound here appears to be something like $\log \operatorname{sep}(f) \leqslant \frac{1}{3} \log M(f) - \frac{1}{2}$, i.e.

$$\operatorname{sep}(f) \leqslant e^{-1/2} M(f)^{1/3}.$$

Discerning the Upper Bound: Signature $(2,1)$



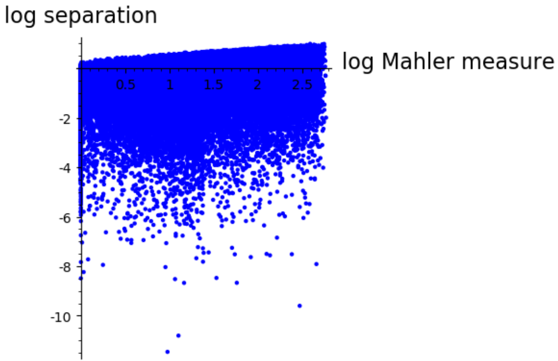
Discerning the Upper Bound: Signature $(2, 1)$



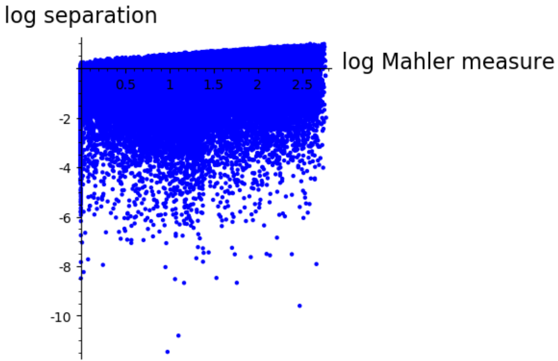
The upper bound in this case appears to be something like $\log \operatorname{sep}(f) \leqslant \frac{1}{3} \log M(f) + \frac{1}{4}$, i.e.

$$\operatorname{sep}(f) \leqslant e^{1/4} M(f)^{1/3}.$$

Discerning the Upper Bounds: Signature $(0, 2)$



Discerning the Upper Bounds: Signature $(0,2)$



The upper bound in this case appears to be something like $\log \operatorname{sep}(f) \leqslant \frac{1}{4}\log M(f) + \frac{1}{4}$, i.e.

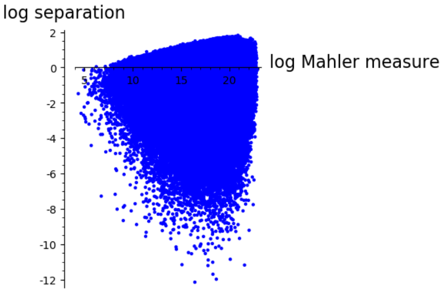
$$\operatorname{sep}(f) \leqslant e^{1/4} M(f)^{1/4}.$$

The Degree 10 Case

Here is a plot of the logarithmic separations and Mahler measures of 2,000,000 degree 10 monic polynomials with 5 pairs of complex conjugate roots:

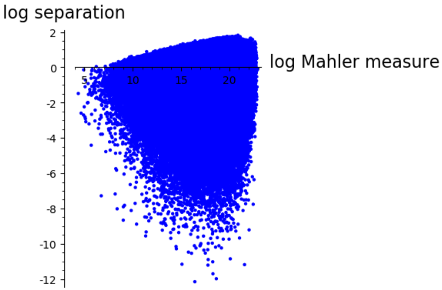
The Degree 10 Case

Here is a plot of the logarithmic separations and Mahler measures of 2,000,000 degree 10 monic polynomials with 5 pairs of complex conjugate roots:



The Degree 10 Case

Here is a plot of the logarithmic separations and Mahler measures of 2,000,000 degree 10 monic polynomials with 5 pairs of complex conjugate roots:



Here, we get something like $\log \operatorname{sep}(f) \leqslant \frac{1}{10}\log M(f) - \frac{1}{2}$, i.e.

$$\operatorname{sep}(f) \leqslant e^{-1/2} M(f)^{1/10}.$$

A Conjecture

Conjecture (K., 2023)

Suppose $f(x) \in \mathbb{R}[x]$ is monic of degree n. If $f(x)$ has any real roots, then

$$\operatorname{sep}(f) \ll_n M(f)^{1/(n-1)}.$$

A Conjecture

Conjecture (K., 2023)

Suppose $f(x) \in \mathbb{R}[x]$ is monic of degree n. If $f(x)$ has any real roots, then

$$\operatorname{sep}(f) \ll_n M(f)^{1/(n-1)}.$$

If $f(x)$ has only nonreal roots, then

$$\operatorname{sep}(f) \ll_n M(f)^{1/n}.$$

The Quadratic Case

As expected, the quadratic case is straightforward:

The Quadratic Case

As expected, the quadratic case is straightforward:

Proposition (K., 2023)

Let $f(x) \in \mathbb{R}[x]$ have degree 2 and leading coefficient a. If $f(x)$ has no real roots, then

$$\operatorname{sep}(f) \leqslant 2\left(\frac{M(f)}{|a|}\right)^{1/2}.$$

The Quadratic Case

As expected, the quadratic case is straightforward:

Proposition (K., 2023)

Let $f(x) \in \mathbb{R}[x]$ have degree 2 and leading coefficient a. If $f(x)$ has no real roots, then

$$\operatorname{sep}(f) \leqslant 2\left(\frac{M(f)}{|a|}\right)^{1/2}.$$

If $f(x)$ has two real roots, then

$$\operatorname{sep}(f) \leqslant \left(\frac{M(f)}{|a|}\right) + 1.$$

Moreover, these bounds are sharp.

The Totally Real Case

The totally real case is also manageable due to the restricted geometry of the root locations:

The Totally Real Case

The totally real case is also manageable due to the restricted geometry of the root locations:

Proposition (K., 2023)

Let $f(x) \in \mathbb{R}[x]$ be separable and monic of degree $n \geqslant 3$ and suppose that all n of the roots of f are real. Then

$$\operatorname{sep}(f) \leqslant \frac{8.2}{n^{\frac{n}{n-1}}} \cdot M(f)^{1/(n-1)}.$$

The Remaining Cubic Case

Proposition (K., 2023)

Let $f(x) \in \mathbb{R}[x]$ have degree 3 and leading coefficient a. If $f(x)$ has exactly one real root, then

$$\operatorname{sep}(f) < \sqrt{3}\left(\frac{M(f)}{|a|}\right)^{1/2}.$$

The Quartic with Signature $(0, 2)$ Case

Proposition (K., 2023)

Suppose that $f(x) \in \mathbb{R}[x]$ has degree 4, leading coefficient a and no real roots. Then

$$\operatorname{sep}(f) \leqslant \sqrt{2}\left(\frac{M(f)}{|a|}\right)^{1/4}.$$

Moreover, this bound is sharp.

Summary

Conjecture (K., 2023)

Suppose $f(x) \in \mathbb{R}[x]$ is monic of degree n. If $f(x)$ has any real roots, then $\operatorname{sep}(f) \ll_n M(f)^{1/(n-1)}$. If $f(x)$ has only nonreal roots, then $\operatorname{sep}(f) \ll_n M(f)^{1/n}$.

Theorem (K., 2023)

This conjecture holds for $f(x) \in \mathbb{R}[x]$ which meet any of the following conditions:

1. $\deg(f) = 2$.
2. $\deg(f) = 3$.
3. $\deg(f) = 4$ *and $f(x)$ has no real roots.*
4. *Every root of $f(x)$ is real.*

Thank you!

Questions?