Towards the Real τ-Conjecture

MSc Thesis

Hitesh Wankhede

The Institute of Mathematical Sciences

July 2025

Outline

1. Real τ-Conjecture and History ($\leq$ 2011)
2. Wronskian Approach (2014)
3. Complex Variant (2013)

Polynomial Evaluation

Given

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

how many $+, \times$ are required to evaluate $f(x)$ at α?

Polynomial Evaluation

Given

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

how many $+$, $\times$ are required to evaluate $f(x)$ at α?

- For instance, when

$$f(x) = 1 + 3x + 5x^2 + 7x^3$$

Polynomial Evaluation

Given

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

how many $+, \times$ are required to evaluate $f(x)$ at α?

- For instance, when

$$f(x) = 1 + 3x + 5x^2 + 7x^3$$

- Naive method $\rightarrow$ 5 multiplications and 3 additions

Polynomial Evaluation

Given

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

how many $+$, $\times$ are required to evaluate $f(x)$ at α?

- For instance, when

$$f(x) = 1 + 3x + 5x^2 + 7x^3$$

- Naive method $\rightarrow$ 5 multiplications and 3 additions
- $1 + \alpha(3 + \alpha(5 + 7\alpha)) \rightarrow$ 3 multiplications and 3 additions

Polynomial Evaluation

In general,

$$\sum_{i=0}^{n} a_i x^i = a_0 + x(a_1 + \cdots + x\,(a_{n-2} + x(a_{n-1} + xa_n))$$

at most n multiplications and n additions suffice.

Polynomial Evaluation

In general,

$$\sum_{i=0}^{n} a_i x^i = a_0 + x(a_1 + \cdots + x\left(a_{n-2} + x(a_{n-1} + xa_n)\right)$$

at most n multiplications and n additions suffice.

- This is Horner's method (1819).

Polynomial Evaluation

In general,

$$\sum_{i=0}^{n} a_i x^i = a_0 + x(a_1 + \cdots + x\left(a_{n-2} + x(a_{n-1} + xa_n)\right)$$

at most n multiplications and n additions suffice.

- This is Horner's method (1819).
- Is this optimal?

Polynomial Evaluation

In general,

$$\sum_{i=0}^{n} a_i x^i = a_0 + x(a_1 + \cdots + x\,(a_{n-2} + x(a_{n-1} + xa_n))$$

at most n multiplications and n additions suffice.

- This is Horner's method (1819).
- Is this optimal? For addition, $f(1) = a_0 + \cdots + a_n$.

Polynomial Evaluation

In general,

$$\sum_{i=0}^{n} a_i x^i = a_0 + x(a_1 + \cdots + x\,(a_{n-2} + x(a_{n-1} + x a_n))$$

at most n multiplications and n additions suffice.

- This is Horner's method (1819).
- Is this optimal? For addition, $f(1) = a_0 + \cdots + a_n$.

  Is there a method that takes less than n multiplications for all polynomials of degree n? (Ostrowski 1954)

Polynomial Evaluation

In general,

$$\sum_{i=0}^{n} a_i x^i = a_0 + x(a_1 + \cdots + x\,(a_{n-2} + x(a_{n-1} + xa_n))$$

at most n multiplications and n additions suffice.

- This is Horner's method (1819).
- Is this optimal? For addition, $f(1) = a_0 + \cdots + a_n$.

  Is there a method that takes less than n multiplications for all polynomials of degree n? (Ostrowski 1954)
- Evaluate x^n at α using only $\times$? (Dellac 1894, Scholz 1937)

Straight Line Program (SLP)

Straight Line Program (SLP)

Given

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad\qquad a_i \in \mathbb{Z},$$

what is the minimum number of $+, -, \times$ *required to build* $f(x)$ *starting from '1' and 'x'?*

Straight Line Program (SLP)

Given

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad a_i \in \mathbb{Z},$$

what is the minimum number of $+, -, \times$ *required to build* $f(x)$ *starting from '1' and 'x'?*

- Denote this number by $\tau(f)$ (τ-Complexity)

Straight Line Program (SLP)

Given

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad\qquad a_i \in \mathbb{Z},$$

what is the minimum number of $+, -, \times$ *required to build* $f(x)$ *starting from '*1*' and '*x*'?*

- Denote this number by $\tau(f)$ (τ-Complexity)
- sequence $1, x, \ldots, f$ is called *scalar-free div-free SLP*

Straight Line Program (SLP)

Given

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad a_i \in \mathbb{Z},$$

what is the minimum number of $+, -, \times$ *required to build* $f(x)$ *starting from '1' and 'x'?*

- Denote this number by $\tau(f)$ (τ-Complexity)
- sequence $1, x, \ldots, f$ is called *scalar-free div-free SLP*
- compute an integer using just addition starting from '1' $\rightarrow$ *addition chain* (Scholz 1937)

Bounds on τ-Complexity

Bounds on τ-Complexity

- By Horner's method, for $f(x) = \sum_{i=0}^{n} a_i x^i$

$$\tau(f) \leq \mathcal{O}(n) + \text{cost to compute all of } a_i\text{'s}$$

Bounds on τ-Complexity

- By Horner's method, for $f(x) = \sum_{i=0}^{n} a_i x^i$

$$\tau(f) \leq \mathcal{O}(n) + \text{cost to compute all of } a_i\text{'s}$$

- By degree argument,

$$\log n \leq \tau(f)$$

Bounds on τ-Complexity

- By Horner's method, for $f(x) = \sum_{i=0}^{n} a_i x^i$

$$\tau(f) \leq \mathcal{O}(n) + \text{cost to compute all of } a_i\text{'s}$$

- By degree argument,

$$\log n \leq \tau(f)$$

$N_f^\circ I :=$ the number of distinct zeros of f in the set I.

Bounds on τ-Complexity

- By Horner's method, for $f(x) = \sum_{i=0}^{n} a_i x^i$

$$\tau(f) \leq \mathcal{O}(n) + \text{cost to compute all of } a_i\text{'s}$$

- By degree argument,

$$\log N_f^\circ \mathbb{Z} \leq \log N_f^\circ \mathbb{R} \leq \log n \leq \tau(f)$$

$N_f^\circ I :=$ the number of distinct zeros of f in the set I.

Bounds on τ-Complexity

- By Horner's method, for $f(x) = \sum_{i=0}^{n} a_i x^i$

$$\tau(f) \leq \mathcal{O}(n) + \text{cost to compute all of } a_i\text{'s}$$

- By degree argument,

$$\log N_f^\circ \mathbb{Z} \leq \log N_f^\circ \mathbb{R} \leq \log n \leq \tau(f)$$

$N_f^\circ I :=$ the number of distinct zeros of f in the set I.

- Strassen (1973) initiated study of lower bounds in terms of number of common zeros of system of equations

Bounds on τ-Complexity

- By Horner's method, for $f(x) = \sum_{i=0}^{n} a_i x^i$

$$\tau(f) \leq \mathcal{O}(n) + \text{cost to compute all of } a_i\text{'s}$$

- By degree argument,

$$\log N_f^{\circ}\mathbb{Z} \leq \log N_f^{\circ}\mathbb{R} \leq \log n \leq \tau(f)$$

$N_f^{\circ} I :=$ the number of distinct zeros of f in the set I.

- Strassen (1973) initiated study of lower bounds in terms of number of common zeros of system of equations
- Borodin & Cook (1976), Risler (1985), Shub & Smale (1995)

τ-Conjecture by Shub and Smale (1995)

- We know $\log N_f^\circ \mathbb{Z} \leq \tau(f) \iff N_f^\circ \mathbb{Z} \leq 2^{\tau(f)}$.

τ-Conjecture by Shub and Smale (1995)

- We know $\log N_f^\circ \mathbb{Z} \leq \tau(f) \iff N_f^\circ \mathbb{Z} \leq 2^{\tau(f)}$.

$$\textit{Conjecture}: N_f^\circ \mathbb{Z} \leq \mathrm{poly}(\tau(f)).$$

τ-Conjecture by Shub and Smale (1995)

- We know $\log N_f^{\circ}\mathbb{Z} \leq \tau(f) \iff N_f^{\circ}\mathbb{Z} \leq 2^{\tau(f)}$.

$$\textit{Conjecture}: N_f^{\circ}\mathbb{Z} \leq \mathrm{poly}(\tau(f)).$$

- Candidate counterexample: Pochhammer-Wilkinson Polynomials

$$PW_n = \prod_{k=1}^{n}(x-k)$$

$N_{PW_n}^{\circ}\mathbb{Z} = n$ and $\tau(PW_n) \leq 2n-1$

τ-Conjecture by Shub and Smale (1995)

- We know $\log N_f^\circ \mathbb{Z} \leq \tau(f) \iff N_f^\circ \mathbb{Z} \leq 2^{\tau(f)}$.

$$\textit{Conjecture}: N_f^\circ \mathbb{Z} \leq \mathrm{poly}(\tau(f)).$$

- Candidate counterexample: Pochhammer-Wilkinson Polynomials

$$PW_n = \prod_{k=1}^{n}(x-k)$$

$N_{PW_n}^\circ \mathbb{Z} = n$ and $\tau(PW_n) \leq 2n-1$

- $\tau(PW_n) \leq \mathrm{polylog}(n) \implies \tau$-Conjecture is false.

τ-Conjecture by Shub and Smale (1995)

- We know $\log N_f^\circ \mathbb{Z} \leq \tau(f) \iff N_f^\circ \mathbb{Z} \leq 2^{\tau(f)}$.

Conjecture : $N_f^\circ \mathbb{Z} \leq \text{poly}(\tau(f))$.

- Candidate counterexample: Pochhammer-Wilkinson Polynomials

$$PW_n = \prod_{k=1}^{n} (x - k)$$

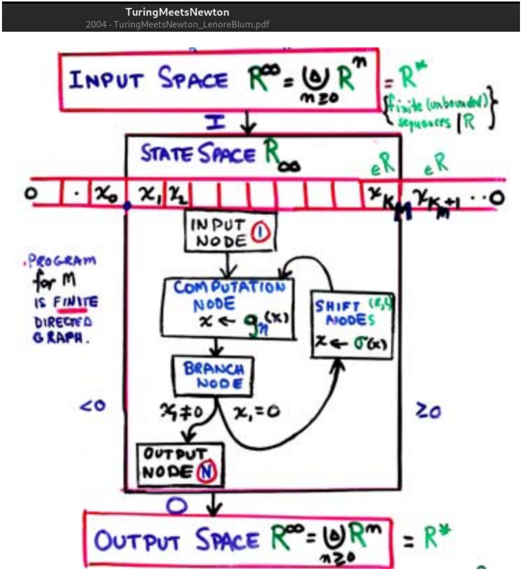
$N_{PW_n}^\circ \mathbb{Z} = n$ and $\tau(PW_n) \leq 2n - 1$

- $\tau(PW_n) \leq \text{polylog}(n) \implies \tau$-Conjecture is false.

Theorem: τ-Conjecture implies $P_{\mathbb{C}} \neq NP_{\mathbb{C}}$ in BSS model over $\mathbb{C}$

BSS model over a ring R

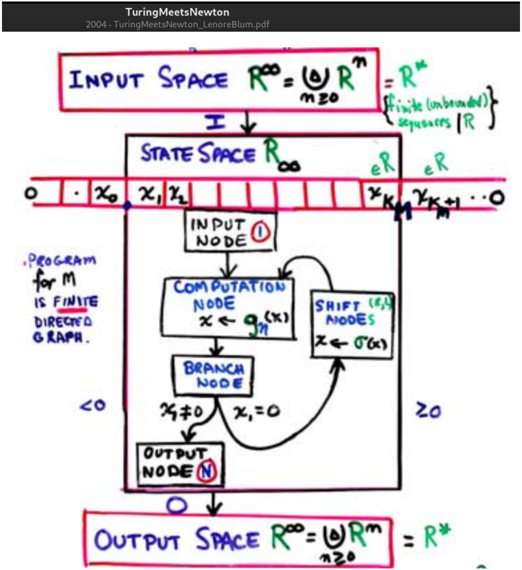
For input $x \in \mathbb{C}^n$, $\text{size}(x) := n$



BSS model over a ring R

For input $x \in \mathbb{C}^n$, $\text{size}(x) := n$

$L \subseteq \mathbb{C}^\infty$ is in $P_{\mathbb{C}}$ if there is a machine over $\mathbb{C}$ computing the characteristic function $\mathbb{1}_L$ and on all valid instances x, the computation length is at most $\text{poly}(\text{size}(x))$.



τ-Conjecture

- We know $\log N_f^\circ \mathbb{Z} \leq \tau(f) \iff N_f^\circ \mathbb{Z} \leq 2^{\tau(f)}$.

Conjecture: $N_f^\circ \mathbb{Z} \leq \mathrm{poly}(\tau(f))$.

- (Shub-Smale 1995)

τ-Conjecture implies $\mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$

τ-Conjecture

- We know $\log N_f^{\circ}\mathbb{Z} \le \tau(f) \iff N_f^{\circ}\mathbb{Z} \le 2^{\tau(f)}$.

Conjecture: $N_f^{\circ}\mathbb{Z} \le \text{poly}(\tau(f))$.

- (Shub-Smale 1995)

τ-Conjecture implies $\text{P}_{\mathbb{C}} \neq \text{NP}_{\mathbb{C}}$ & $\text{P}_{\overline{\mathbb{Q}}} \neq \text{NP}_{\overline{\mathbb{Q}}}$

τ-Conjecture

- We know $\log N_f^\circ \mathbb{Z} \leq \tau(f) \iff N_f^\circ \mathbb{Z} \leq 2^{\tau(f)}$.

  Conjecture: $N_f^\circ \mathbb{Z} \leq \text{poly}(\tau(f))$.

- (Shub-Smale 1995)

  τ-Conjecture implies $\text{P}_{\mathbb{C}} \neq \text{NP}_{\mathbb{C}}$ & $\text{P}_{\overline{\mathbb{Q}}} \neq \text{NP}_{\overline{\mathbb{Q}}}$

- (Bürgisser 2009)

  τ-Conjecture implies $\text{PERM}_n \notin \text{VP}^0$

Straight Line Program (SLP)

Straight Line Program (SLP)

Given

$$f(x) \in \mathbb{Z}[x_1, \ldots, x_k],$$

denote by $\tau(f)$ *the minimum number of* $+, -, \times$ *required to build* f *starting from* 1 *and* $x_1, \ldots, x_k$*?*

- $1, x_1, \ldots, x_k, \ldots, f$ is called *scalar-free div-free SLP*

Straight Line Program (SLP)

Given

$$f(x) \in \mathbb{Z}[x_1, \ldots, x_k],$$

denote by $\tau(f)$ *the minimum number of* $+, -, \times$ *required to build* f *starting from* 1 *and* $x_1, \ldots, x_k$*?*

- $1, x_1, \ldots, x_k, \ldots, f$ is called *scalar-free div-free SLP*
- $(f_n) \in \mathrm{VP}^0$ if (f_n) is computable by such an SLP (φ_n) with $\tau(f_n)$ as well as intermediate coeffs/degree polynomially bounded in n. (Malod 2003)

Straight Line Program (SLP)

Given

$$f(x) \in \mathbb{Z}[x_1, \ldots, x_k],$$

denote by $\tau(f)$ *the minimum number of* $+, -, \times$ *required to build* f *starting from* 1 *and* $x_1, \ldots, x_k$*?*

- $1, x_1, \ldots, x_k, \ldots, f$ is called *scalar-free div-free SLP*
- $(f_n) \in \mathrm{VP}^0$ if (f_n) is computable by such an SLP (φ_n) with $\tau(f_n)$ as well as intermediate coeffs/degree polynomially bounded in n. (Malod 2003)
- $\mathrm{PERM}_n := \mathrm{permanent}([x_{i,j}]_{1 \le i,j \le n})$

Straight Line Program (SLP)

Given

$$f(x) \in \mathbb{Z}[x_1, \ldots, x_k],$$

denote by $\tau(f)$ the minimum number of $+, -, \times$ required to build f starting from 1 and $x_1, \ldots, x_k$?

- $1, x_1, \ldots, x_k, \ldots, f$ is called *scalar-free div-free SLP*
- $(f_n) \in \mathrm{VP}^0$ if (f_n) is computable by such an SLP (φ_n) with $\tau(f_n)$ as well as intermediate coeffs/degree polynomially bounded in n. (Malod 2003)
- $\mathrm{PERM}_n := \mathrm{permanent}([x_{i,j}]_{1 \leq i,j \leq n})$
- VP is defined over some field $\mathbb{F}$ (Valiant 1979).

If the goal is $\mathrm{PERM}_n \notin \mathrm{VP}^0$, what is the most relaxed variant of the τ-conjecture that leads to this conclusion?

Studying real or complex zeros might be more approachable than integer zeros.

Variants by Koiran (2011)

Variants by Koiran (2011)

- (SPS τ-conjecture) For $f_{i,j} \in \mathbb{Z}[x]$ and k-sparse

$$f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j} \qquad \text{implies} \qquad N_f^{\circ}\mathbb{Z} \leq \mathrm{poly}(pqk + s),$$

  where s controls size of exponents and coefficients of $f_{i,j}$

- τ-Conjecture $\implies$ SPS τ-conjecture $\implies$ PERM $\notin \mathrm{VP}^0$

Variants by Koiran (2011)

- (SPS τ-conjecture) For $f_{i,j} \in \mathbb{Z}[x]$ and k-sparse

$$f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j} \qquad \text{implies} \qquad N_f^{\circ}\mathbb{Z} \leq \operatorname{poly}(pqk + s),$$

  where s controls size of exponents and coefficients of $f_{i,j}$

- τ-Conjecture $\implies$ SPS τ-conjecture $\implies$ PERM $\notin$ VP^0
- (Real τ-Conjecture) For $f_{i,j} \in \mathbb{R}[x]$ and k-sparse,

$$f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j} \qquad \text{implies} \qquad N_f^{\circ}\mathbb{R} \leq \operatorname{poly}(pqk).$$

- Real τ-Conjecture $\implies$ SPS τ-conjecture

Variants by Koiran (2011)

- (SPS τ-conjecture) For $f_{i,j} \in \mathbb{Z}[x]$ and k-sparse

$$f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j} \quad \text{implies} \quad N_f^{\circ}\mathbb{Z} \leq \text{poly}(pqk + s),$$

where s controls size of exponents and coefficients of $f_{i,j}$

- τ-Conjecture $\implies$ SPS τ-conjecture $\implies$ PERM $\notin$ VP^0
- (Real τ-Conjecture) For $f_{i,j} \in \mathbb{R}[x]$ and k-sparse,

$$f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j} \quad \text{implies} \quad N_f^{\circ}\mathbb{R} \leq \text{poly}(pqk).$$

- Real τ-Conjecture $\implies$ SPS τ-conjecture
- (Tavenas 2014) $\text{poly}(p2^q k)$ suffices & PERM $\notin$ VP follows

Variant by Tavenas 2014

Variant by Tavenas 2014

Tee following are equivalent:

- Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ be such that each $f_{i,j} \in \mathbb{R}[x]$ is k-sparse. Then, $N_f^{\circ}\mathbb{R} \leq \text{poly}(p2^q k)$.
- Let $f := \sum_{i=1}^{p} a_i f_i^{\alpha_i}$ be such that each $f_i \in \mathbb{R}[x]$ is k-sparse, $a_i \in \mathbb{R}$, and $\alpha_i \leq m$. Then, $N_f^{\circ}\mathbb{R} \leq \text{poly}(p2^m k)$.

Variant by Tavenas 2014

Tee following are equivalent:

- Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ be such that each $f_{i,j} \in \mathbb{R}[x]$ is k-sparse. Then, $N_f^\circ \mathbb{R} \leq \text{poly}(p2^q k)$.
- Let $f := \sum_{i=1}^{p} a_i f_i^{\alpha_i}$ be such that each $f_i \in \mathbb{R}[x]$ is k-sparse, $a_i \in \mathbb{R}$, and $\alpha_i \leq m$. Then, $N_f^\circ \mathbb{R} \leq \text{poly}(p2^m k)$.

Proof idea: ($\Longleftarrow$) Write product as sum of powers (Ryser).

Variant by Tavenas 2014

Tee following are equivalent:

- Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ be such that each $f_{i,j} \in \mathbb{R}[x]$ is k-sparse. Then, $N_f^{\circ}\mathbb{R} \leq \text{poly}(p2^q k)$.
- Let $f := \sum_{i=1}^{p} a_i f_i^{\alpha_i}$ be such that each $f_i \in \mathbb{R}[x]$ is k-sparse, $a_i \in \mathbb{R}$, and $\alpha_i \leq m$. Then, $N_f^{\circ}\mathbb{R} \leq \text{poly}(p2^m k)$.

Proof idea: ($\Longleftarrow$) Write product as sum of powers (Ryser).

$$\text{perm}\begin{bmatrix} x_1 & x_2 & \dots & x_n \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \dots & x_n \end{bmatrix} = (-1)^n \sum_{S \subseteq [n]} (-1)^{|S|} \prod_{i=1}^{n} \sum_{j \in S} x_j$$

$$n! \prod_{i=1}^{n} x_i = \sum_{S \subseteq [n]} (-1)^{|S|+n} \left(\sum_{j \in S} x_j \right)^n$$

How do we count real zeros?

Descartes' Rule

Theorem

A real k-sparse polynomial has at most $(k-1)$ positive zeros.

Descartes' Rule

Theorem

A real k-sparse polynomial has at most $(k-1)$ positive zeros.

Proof by induction:

- Assume $f(x) = a_n x^{\alpha_k} + \cdots + a_1 x^{\alpha_2} + a_0$ has r positive zeros
- By induction, $f'(x)$ has at most $k-2$ positive zeros.
- By Rolle's theorem, $f'(x)$ has at least $r-1$ positive zeros
- $r - 1 \leq k - 2 \implies r \leq k - 1$

Descartes' Rule

Theorem

A real k-sparse polynomial has at most $(k-1)$ positive zeros.

Proof by induction:

- Assume $f(x) = a_n x^{\alpha_k} + \cdots + a_1 x^{\alpha_2} + a_0$ has r positive zeros
- By induction, $f'(x)$ has at most $k-2$ positive zeros.
- By Rolle's theorem, $f'(x)$ has at least $r-1$ positive zeros
- $r-1 \leq k-2 \implies r \leq k-1$

Corollary

at most $2k-1$ distinct real zeros.

Upper Bounds

(Real τ-Conjecture for Powers) For $f_i \in \mathbb{R}[x]$ and k-sparse, $a_i \in \mathbb{R}$, and $\alpha_i \leq m$

$$f := \sum_{i=1}^{p} a_i f_i^{\alpha_i} \qquad \Longrightarrow \quad N_f^{\circ}\mathbb{R} \leq \mathrm{poly}(p2^m k).$$

Upper Bounds

(Real τ-Conjecture for Powers) For $f_i \in \mathbb{R}[x]$ and k-sparse, $a_i \in \mathbb{R}$, and $\alpha_i \leq m$

$$f := \sum_{i=1}^{p} a_i f_i^{\alpha_i} \qquad \Longrightarrow N_f^{\circ}\mathbb{R} \leq \text{poly}(p2^m k).$$

- $N_f^{\circ}\mathbb{R} \leq \mathcal{O}(pk^m) = \mathcal{O}(p2^{m \log k})$ by Descartes' rule.

Upper Bounds

(Real τ-Conjecture for Powers) For $f_i \in \mathbb{R}[x]$ and k-sparse, $a_i \in \mathbb{R}$, and $\alpha_i \leq m$

$$f := \sum_{i=1}^{p} a_i f_i^{\alpha_i} \qquad \implies N_f^{\circ}\mathbb{R} \leq \text{poly}(p2^m k).$$

- $N_f^{\circ}\mathbb{R} \leq \mathcal{O}(pk^m) = \mathcal{O}(p2^{m \log k})$ by Descartes' rule.
- $N_f^{\circ}\mathbb{R} \leq k^{\mathcal{O}(p^2)}$ using Wronskian approach.

Upper Bounds

(Real τ-Conjecture for Powers) For $f_i \in \mathbb{R}[x]$ and k-sparse, $a_i \in \mathbb{R}$, and $\alpha_i \leq m$

$$f := \sum_{i=1}^{p} a_i f_i^{\alpha_i} \qquad \implies N_f^\circ \mathbb{R} \leq \text{poly}(p2^m k).$$

- $N_f^\circ \mathbb{R} \leq \mathcal{O}(pk^m) = \mathcal{O}(p2^{m \log k})$ by Descartes' rule.
- $N_f^\circ \mathbb{R} \leq k^{\mathcal{O}(p^2)}$ using Wronskian approach.
- Conj. holds if any of p or m or k is bounded by a constant.

How do we count real zeros of sum of two polynomials?

How do we count real zeros of sum of two polynomials?

Let $f = \phi_1 + \phi_2$. Then by Rolle's theorem

$$N_f^\circ \mathbb{R} \leq N_{f'}^\circ \mathbb{R} + 1$$

But f' is again sum of two polynomials!

Wronskian approach (for $p = 2$)

Wronskian approach (for $p = 2$)

Koiran, Portier, Tavenas (2015), motivated by Voorhoeve and van der Poorten (1975)

Theorem

Let $f = \phi_1 + \phi_2$ *(e.g.* $\phi_i = f_i^{\alpha_i}$*). Then*

$$N_f^\circ \mathbb{R} \leq 1 + N_{\phi_1}^\circ \mathbb{R} + N_{W(\phi_1,\phi_2)}^\circ \mathbb{R},$$

$$\textit{where } W(\phi_1, \phi_2) = \det \begin{bmatrix} \phi_1 & \phi_2 \\ \phi_1' & \phi_2' \end{bmatrix} = \phi_1 \phi_2' - \phi_1' \phi_2.$$

Wronskian approach (for $p = 2$)

Koiran, Portier, Tavenas (2015), motivated by Voorhoeve and van der Poorten (1975)

Theorem

Let $f = \phi_1 + \phi_2$ *(e.g.* $\phi_i = f_i^{\alpha_i}$*). Then*

$$N_f^\circ \mathbb{R} \leq 1 + N_{\phi_1}^\circ \mathbb{R} + N_{W(\phi_1,\phi_2)}^\circ \mathbb{R},$$

$$\text{where } W(\phi_1, \phi_2) = \det \begin{bmatrix} \phi_1 & \phi_2 \\ \phi_1' & \phi_2' \end{bmatrix} = \phi_1\phi_2' - \phi_1'\phi_2.$$

Idea:

- Prove instead $N_f^\circ \mathbb{R} - (1 + N_{\phi_1}^\circ \mathbb{R}) \leq N_{W(\phi_1,\phi_2)}^\circ \mathbb{R}$

Wronskian approach (for $p = 2$)

Koiran, Portier, Tavenas (2015), motivated by Voorhoeve and van der Poorten (1975)

Theorem

Let $f = \phi_1 + \phi_2$ *(e.g.* $\phi_i = f_i^{\alpha_i}$*). Then*

$$N_f^{\circ}\mathbb{R} \leq 1 + N_{\phi_1}^{\circ}\mathbb{R} + N_{W(\phi_1,\phi_2)}^{\circ}\mathbb{R},$$

$$\text{where } W(\phi_1, \phi_2) = \det \begin{bmatrix} \phi_1 & \phi_2 \\ \phi_1' & \phi_2' \end{bmatrix} = \phi_1\phi_2' - \phi_1'\phi_2.$$

Idea:

- Prove instead $N_f^{\circ}\mathbb{R} - (1 + N_{\phi_1}^{\circ}\mathbb{R}) \leq N_{W(\phi_1,\phi_2)}^{\circ}\mathbb{R} = N_{W(\phi_1,f)}^{\circ}\mathbb{R}$

Wronskian approach (for $p = 2$)

Koiran, Portier, Tavenas (2015), motivated by Voorhoeve and van der Poorten (1975)

Theorem

Let $f = \phi_1 + \phi_2$ *(e.g.* $\phi_i = f_i^{\alpha_i}$*). Then*

$$N_f^\circ \mathbb{R} \leq 1 + N_{\phi_1}^\circ \mathbb{R} + N_{W(\phi_1,\phi_2)}^\circ \mathbb{R},$$

$$\textit{where } W(\phi_1, \phi_2) = \det \begin{bmatrix} \phi_1 & \phi_2 \\ \phi_1' & \phi_2' \end{bmatrix} = \phi_1 \phi_2' - \phi_1' \phi_2.$$

Idea:

- Prove instead $N_f^\circ \mathbb{R} - (1 + N_{\phi_1}^\circ \mathbb{R}) \leq N_{W(\phi_1,\phi_2)}^\circ \mathbb{R} = N_{W(\phi_1,f)}^\circ \mathbb{R}$
- Use $W(\phi_1, f) = \phi_1^2 \left(\frac{f}{\phi_1}\right)'$ on the set $\mathbb{R} \backslash Z(\phi_1)$

For $f = \phi_1 + \phi_2$ where $\phi_i = f_i^{\alpha_i}$ and f_i is k-sparse,

$$\begin{aligned} N_f^\circ \mathbb{R} &\leq 1 + N_{\phi_1}^\circ \mathbb{R} + N_{W(\phi_1,\phi_2)}^\circ \mathbb{R} \\ &\leq 1 + 2k - 1 + N_{W(f_1^{\alpha_1}, f_2^{\alpha_2})}^\circ \mathbb{R} \end{aligned}$$

$$\begin{aligned} W(f_1^{\alpha_1}, f_2^{\alpha_2}) &= f_1^{\alpha_1}(\alpha_2 f_2^{\alpha_2 - 1}) - (\alpha_1 f_1^{\alpha_1 - 1}) f_2^{\alpha_2} \\ &= f_1^{\alpha_1 - 1} f_2^{\alpha_2 - 1} (\alpha_2 f_1 - \alpha_1 f_2) \end{aligned}$$

For $f = \phi_1 + \phi_2$ where $\phi_i = f_i^{\alpha_i}$ and f_i is k-sparse,

$$\begin{aligned} N_f^\circ \mathbb{R} &\leq 1 + N_{\phi_1}^\circ \mathbb{R} + N_{W(\phi_1,\phi_2)}^\circ \mathbb{R} \\ &\leq 1 + 2k - 1 + N_{W(f_1^{\alpha_1}, f_2^{\alpha_2})}^\circ \mathbb{R} \end{aligned}$$

$$\begin{aligned} W(f_1^{\alpha_1}, f_2^{\alpha_2}) &= f_1^{\alpha_1}(\alpha_2 f_2^{\alpha_2 - 1}) - (\alpha_1 f_1^{\alpha_1 - 1}) f_2^{\alpha_2} \\ &= f_1^{\alpha_1 - 1} f_2^{\alpha_2 - 1} (\alpha_2 f_1 - \alpha_1 f_2) \end{aligned}$$

$$\implies N_{W(f_1^{\alpha_1}, f_2^{\alpha_2})}^\circ \mathbb{R} \leq (2k-1) + (2k-1) + (4k-1)$$

Finally,

$$N_f^\circ \mathbb{R} \leq 10k - 3$$

For $f = \phi_1 + \phi_2$ where $\phi_i = f_i^{\alpha_i}$ and f_i is k-sparse,

$$\begin{aligned} N_f^{\circ}\mathbb{R} &\leq 1 + N_{\phi_1}^{\circ}\mathbb{R} + N_{W(\phi_1,\phi_2)}^{\circ}\mathbb{R} \\ &\leq 1 + 2k - 1 + N_{W(f_1^{\alpha_1},f_2^{\alpha_2})}^{\circ}\mathbb{R} \end{aligned}$$

$$\begin{aligned} W(f_1^{\alpha_1}, f_2^{\alpha_2}) &= f_1^{\alpha_1}(\alpha_2 f_2^{\alpha_2-1}) - (\alpha_1 f_1^{\alpha_1-1}) f_2^{\alpha_2} \\ &= f_1^{\alpha_1-1} f_2^{\alpha_2-1}(\alpha_2 f_1 - \alpha_1 f_2) \end{aligned}$$

$$\implies N_{W(f_1^{\alpha_1},f_2^{\alpha_2})}^{\circ}\mathbb{R} \leq (2k-1) + (2k-1) + (4k-1)$$

Finally,

$$N_f^{\circ}\mathbb{R} \leq 10k - 3$$

For $\sum_{i=1}^{p} f_i^{\alpha_i}$, the bound $k^{\mathcal{O}(p^2)}$ can be shown similarly.

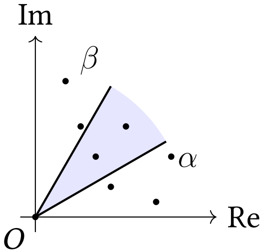
What’s so special about real zeros and real polynomials? Why count only distinct zeros?

Distribution of Zeros

Theorem (Hayman 1972)

$f \in \mathbb{C}[x]$ *be* k*-sparse and of degree* n *with* $f(0) \neq 0$

$$\left| N_f S(\alpha, \beta) - \frac{\beta - \alpha}{2\pi} n \right| \leq k - 1$$



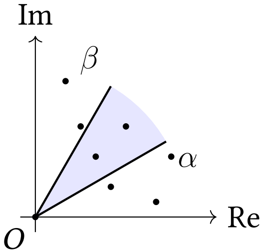
$$S(\alpha, \beta) = \{z \in \mathbb{C} \mid |z| > 0, \alpha < \arg z < \beta\}$$

Distribution of Zeros

Theorem (Hayman 1972)

$f \in \mathbb{C}[x]$ be k-sparse and of degree n with $f(0) \neq 0$

$$\left| N_f S(\alpha, \beta) - \frac{\beta - \alpha}{2\pi} n \right| \leq k - 1$$



$$S(\alpha, \beta) = \{z \in \mathbb{C} \mid |z| > 0, \alpha < \arg z < \beta\}$$

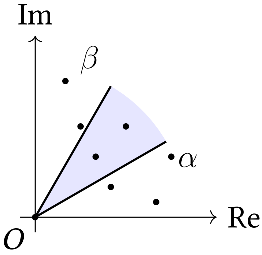
- Motivating case: $x^n - 1$

Distribution of Zeros

Theorem (Hayman 1972)

$f \in \mathbb{C}[x]$ be k-sparse and of degree n with $f(0) \neq 0$

$$\left| N_f S(\alpha, \beta) - \frac{\beta - \alpha}{2\pi} n \right| \leq k - 1$$



$$S(\alpha, \beta) = \{z \in \mathbb{C} \mid |z| > 0, \alpha < \arg z < \beta\}$$

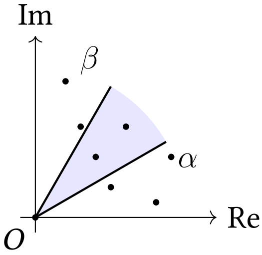
- Motivating case: $x^n - 1$
- Choose $\beta = 0^+$ and $\alpha = 0^-$ to get Descartes' rule

Distribution of Zeros

Theorem (Hayman 1972)

$f \in \mathbb{C}[x]$ be k-sparse and of degree n with $f(0) \neq 0$

$$\left| N_f S(\alpha, \beta) - \frac{\beta - \alpha}{2\pi} n \right| \leq k - 1$$



$$S(\alpha, \beta) = \{z \in \mathbb{C} \mid |z| > 0, \alpha < \arg z < \beta\}$$

- Motivating case: $x^n - 1$
- Choose $\beta = 0^+$ and $\alpha = 0^-$ to get Descartes' rule

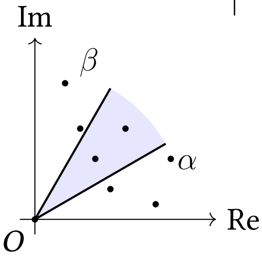
Corollary: *Can also count zeros along any ray from the origin.*

Complex τ-Conjecture by Hrubeš 2013

TFAE:

- Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ be such that each $f_{i,j} \in \mathbb{R}[x]$ is k-sparse. Then $N_f^{\circ}\mathbb{R} \leq \text{poly}(pqk)$
- Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ be of degree n with $f(0) \neq 0$ and each $f_{i,j} \in \mathbb{C}[x]$ be k-sparse. Then

$$\left| N_f S(\alpha, \beta) - \frac{\beta - \alpha}{2\pi} n \right| \leq \text{poly}(pqk)$$

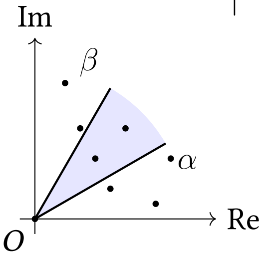


Complex τ-Conjecture by Hrubeš 2013

TFAE:

- Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ be such that each $f_{i,j} \in \mathbb{R}[x]$ is k-sparse. Then $N_f^\circ \mathbb{R} \le \text{poly}(pqk)$
- Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ be of degree n with $f(0) \neq 0$ and each $f_{i,j} \in \mathbb{C}[x]$ be k-sparse. Then

$$\left| N_f S(\alpha, \beta) - \frac{\beta - \alpha}{2\pi} n \right| \le \text{poly}(pqk)$$



Proof idea: (Generalized Hayman)

1. Discrepancy $\le \#$ distinct zeros of $\Re(f)$ on the boundary of the sector
2. $\Re(f)$ has small representation if f does

How to Falsify Real τ-Conjecture?

Conjecture: *Let* $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ *be of degree n with* $f(0) \neq 0$ *and each* $f_{i,j} \in \mathbb{C}[x]$ *be k-sparse. Then*

$$\left| N_f S(\alpha, \beta) - \frac{\beta - \alpha}{2\pi} n \right| \leq \mathrm{poly}(pqk).$$

- Candidate counterexample: $(x+1)^n$.
- Choose $\beta = \pi + \epsilon$ and $\alpha = \pi - \epsilon$
- Conjecture $\implies$ $pqk = \Omega(n^c)$ for some $c > 0$
- Can $(x+1)^n$ be expressed by a small complex SPS representation?

Summary

- Integer / Real / Complex τ-Conjecture are hard problems
- Hrubeš: Study distribution of zeros
- Tavenas: Study sum of powers

Summary

- Integer / Real / Complex τ-Conjecture are hard problems
- Hrubeš: Study distribution of zeros
- Tavenas: Study sum of powers

Possible directions:

- Does $gh + t$ have $\mathcal{O}(k)$ real zeros? (Chattopadhyay)
- Bivariate (Koiran, Portier, Tavenas, Thomassé 2015)
- Random (Briquel, Bürgisser 2020)
- SOS, SOC, …(Dutta 2021)

Thank you for you attention! Any questions?