Bounds on Autocorrelation Coefficients of Rudin-Shapiro Polynomials

Stephen Choi
(joint work with J.P. Allouche, T. Erdélyi, A. Denise, B. Saffari)

AMS, San Diego
Special Session on Diophantine Approximation and Analytic Number Theory in Honor of
Jeffrey Vaaler

Polynomials with Restricted coefficients

Let N be positive integer. Then we denote

$$\mathcal{U}_N := \left\{ P(z) = a_0 + a_1 z + \cdots + a_{N-1} z^{N-1} : |a_\ell| = 1, \ \ \forall \ell . \right\}$$

We call these polynomials, **Unimodular Polynomials of degree $N-1$.**

$$\mathcal{L}_N := \left\{ P(z) = a_0 + a_1 z + \cdots + a_{N-1} z^{N-1} : a_\ell \in \{-1, +1\}, \ \ \forall \ell . \right\}$$

We call these polynomials, **Littlewood Polynomials of degree $N-1$.**

Polynomials with Restricted coefficients

Let N be positive integer. Then we denote

$$\mathcal{U}_N := \left\{ P(z) = a_0 + a_1 z + \cdots + a_{N-1} z^{N-1} : |a_\ell| = 1, \ \forall \ell. \right\}$$

We call these polynomials, **Unimodular Polynomials of degree $N-1$.**

$$\mathcal{L}_N := \left\{ P(z) = a_0 + a_1 z + \cdots + a_{N-1} z^{N-1} : a_\ell \in \{-1, +1\}, \ \forall \ell. \right\}$$

We call these polynomials, **Littlewood Polynomials of degree $N-1$.**

Polynomials with Restricted coefficients

Let N be positive integer. Then we denote

$$\mathcal{U}_N := \left\{ P(z) = a_0 + a_1 z + \cdots + a_{N-1} z^{N-1} : |a_\ell| = 1, \ \ \forall \ell. \right\}$$

We call these polynomials, **Unimodular Polynomials of degree $N-1$.**

$$\mathcal{L}_N := \left\{ P(z) = a_0 + a_1 z + \cdots + a_{N-1} z^{N-1} : a_\ell \in \{-1, +1\}, \ \ \forall \ell. \right\}$$

We call these polynomials, **Littlewood Polynomials of degree $N-1$.**

Polynomials with Restricted coefficients

Let N be positive integer. Then we denote

$$\mathcal{U}_N := \left\{ P(z) = a_0 + a_1 z + \cdots + a_{N-1} z^{N-1} : |a_\ell| = 1, \ \forall \ell. \right\}$$

We call these polynomials, **Unimodular Polynomials of degree $N-1$.**

$$\mathcal{L}_N := \left\{ P(z) = a_0 + a_1 z + \cdots + a_{N-1} z^{N-1} : a_\ell \in \{-1, +1\}, \ \forall \ell. \right\}$$

We call these polynomials, **Littlewood Polynomials of degree $N-1$.**

Polynomials with Restricted coefficients

Let N be positive integer. Then we denote

$$\mathcal{U}_N := \left\{ P(z) = a_0 + a_1 z + \cdots + a_{N-1} z^{N-1} : |a_\ell| = 1, \ \forall \ell. \right\}$$

We call these polynomials, **Unimodular Polynomials of degree $N-1$.**

$$\mathcal{L}_N := \left\{ P(z) = a_0 + a_1 z + \cdots + a_{N-1} z^{N-1} : a_\ell \in \{-1, +1\}, \ \forall \ell. \right\}$$

We call these polynomials, **Littlewood Polynomials of degree $N-1$.**

Ultra-Flat Polynomials

A sequences of polynomial $P_N(z) \in \mathbb{C}[z]$ of degree $N-1$ is called **Ultra-Flat** if there are absolute constants $0 < c_1 < c_2$ such that

Ultra-Flat Polynomials

$$c_1 ||P_N||_2 \le \left|P_N(e^{i\theta})\right| \le c_2 ||P_N||_2, \quad \forall \theta \in [0, 2\pi), \forall N.$$

Here $||P||_p := \left\{\frac{1}{2\pi}\int_0^{2\pi} \left|P(e^{i\theta})\right|^p d\theta\right\}^{\frac{1}{p}}$ for $p > 0$.

Question: When do sequences of ultra-flat polynomials exist?

Note that if $P(z) \in \mathscr{U}_N$ or $P(z) \in \mathscr{L}_N$, then $||P||_2 = \sqrt{N}$.

Ultra-Flat Polynomials

A sequences of polynomial $P_N(z) \in \mathbb{C}[z]$ of degree $N-1$ is called **Ultra-Flat** if there are absolute constants $0 < c_1 < c_2$ such that

Ultra-Flat Polynomials

$$c_1 ||P_N||_2 \le \left|P_N(e^{i\theta})\right| \le c_2 ||P_N||_2, \quad \forall \theta \in [0, 2\pi), \forall N.$$

Here $||P||_p := \left\{ \frac{1}{2\pi} \int_0^{2\pi} \left|P(e^{i\theta})\right|^p d\theta \right\}^{\frac{1}{p}}$ for $p > 0$.

Question: When do sequences of ultra-flat polynomials exist?

Note that if $P(z) \in \mathcal{U}_N$ or $P(z) \in \mathcal{L}_N$, then $||P||_2 = \sqrt{N}$.

Ultra-Flat Polynomials

A sequences of polynomial $P_N(z) \in \mathbb{C}[z]$ of degree $N-1$ is called **Ultra-Flat** if there are absolute constants $0 < c_1 < c_2$ such that

Ultra-Flat Polynomials

$$c_1 ||P_N||_2 \leq \left| P_N(e^{i\theta}) \right| \leq c_2 ||P_N||_2, \quad \forall \theta \in [0, 2\pi), \forall N.$$

Here $||P||_p := \left\{ \frac{1}{2\pi} \int_0^{2\pi} \left| P(e^{i\theta}) \right|^p d\theta \right\}^{\frac{1}{p}}$ for $p > 0$.

Question: When do sequences of ultra-flat polynomials exist?

Note that if $P(z) \in \mathscr{U}_N$ or $P(z) \in \mathscr{L}_N$, then $||P||_2 = \sqrt{N}$.

Kahane's Theorem and Erdös' Conjecture

Kahane's Theorem.

For any sequence of real number $\varepsilon_N \to 0$ as $N \to \infty$, there is a sequence of unimodular polynomials $P_N(z) \in \mathscr{U}_N$ such that

$$(1-\varepsilon_N)\sqrt{N} \leq \left|P_N(e^{i\theta})\right| \leq (1+\varepsilon_N)\sqrt{N}, \ \ \forall \theta \in [0,2\pi), \forall N$$

Sequences of ultra-flat **unimodular** polynomials exist!

Question: Do sequences of ultra-flat **Littlewood** polynomials exist?

Littlewood's and Eröds' Conjecture.

There is an absolute constant $c_3 > 0$ such that for all $P(z) \in \mathscr{L}_N$, we have

$$\max\{|P(z)| : \forall |z| = 1\} \geq (1+c_3)\sqrt{N}.$$

Kahane's Theorem and Erdös' Conjecture

Kahane's Theorem.

For any sequence of real number $\varepsilon_N \to 0$ as $N \to \infty$, there is a sequence of unimodular polynomials $P_N(z) \in \mathcal{U}_N$ such that

$$(1-\varepsilon_N)\sqrt{N} \leq \left|P_N(e^{i\theta})\right| \leq (1+\varepsilon_N)\sqrt{N}, \ \ \forall \theta \in [0, 2\pi), \forall N$$

Sequences of ultra-flat **unimodular** polynomials exist!

Question: Do sequences of ultra-flat **Littlewood** polynomials exist?

Littlewood's and Eröds' Conjecture.

There is an absolute constant $c_3 > 0$ such that for all $P(z) \in \mathcal{L}_N$, we have

$$\max\{|P(z)| : \forall |z| = 1\} \geq (1+c_3)\sqrt{N}.$$

Kahane's Theorem and Erdös' Conjecture

Kahane's Theorem.

For any sequence of real number $\varepsilon_N \to 0$ as $N \to \infty$, there is a sequence of unimodular polynomials $P_N(z) \in \mathcal{U}_N$ such that

$$(1-\varepsilon_N)\sqrt{N} \leq \left|P_N(e^{i\theta})\right| \leq (1+\varepsilon_N)\sqrt{N}, \ \ \forall\theta \in [0,2\pi), \forall N$$

Sequences of ultra-flat **unimodular** polynomials exist!

Question: Do sequences of ultra-flat **Littlewood** polynomials exist?

Littlewood's and Eröds' Conjecture.

There is an absolute constant $c_3 > 0$ such that for all $P(z) \in \mathcal{L}_N$, we have

$$\max\{|P(z)| : \forall |z| = 1\} \geq (1+c_3)\sqrt{N}.$$

Kahane's Theorem and Erdös' Conjecture

Kahane's Theorem.

For any sequence of real number $\varepsilon_N \to 0$ as $N \to \infty$, there is a sequence of unimodular polynomials $P_N(z) \in \mathcal{U}_N$ such that

$$(1-\varepsilon_N)\sqrt{N} \leq \left|P_N(e^{i\theta})\right| \leq (1+\varepsilon_N)\sqrt{N}, \quad \forall \theta \in [0, 2\pi), \forall N$$

Sequences of ultra-flat **unimodular** polynomials exist!

Question: Do sequences of ultra-flat **Littlewood** polynomials exist?

Littlewood's and Eröds' Conjecture.

There is an absolute constant $c_3 > 0$ such that for all $P(z) \in \mathcal{L}_N$, we have

$$\max\{|P(z)| : \forall |z| = 1\} \geq (1+c_3)\sqrt{N}.$$

Rudin-Shapiro Polynomials

Let $P_0(z) = 1$ and $Q_0(z) = 1$. For any integer $n \geq 1$, define

Rudin-Shapiro Polynomials

$$\begin{cases} P_n(z) := P_{n-1}(z) + z^{2^{n-1}} Q_{n-1}(z), \\ Q_n(z) := P_{n-1}(z) - z^{2^{n-1}} Q_{n-1}(z). \end{cases}$$

Polynomials $P_n(z)$ and $Q_n(z)$ are called **Rudin-Shapiro polynomials.** Note that $P_n(z)$ and $Q_n(z)$ are polynomials with ± 1 coefficients of degree $L_n - 1$ where $L_n = 2^n$.

$$P_n(z), Q_n(z) \in \mathcal{L}_N, \quad N = 2^n.$$

Rudin-Shapiro Polynomials

Let $P_0(z) = 1$ and $Q_0(z) = 1$. For any integer $n \geq 1$, define

Rudin-Shapiro Polynomials

$$\begin{cases} P_n(z) := P_{n-1}(z) + z^{2^{n-1}} Q_{n-1}(z), \\ Q_n(z) := P_{n-1}(z) - z^{2^{n-1}} Q_{n-1}(z). \end{cases}$$

Polynomials $P_n(z)$ and $Q_n(z)$ are called **Rudin-Shapiro polynomials.** Note that $P_n(z)$ and $Q_n(z)$ are polynomials with ± 1 coefficients of degree $L_n - 1$ where $L_n = 2^n$.

$$P_n(z), Q_n(z) \in \mathscr{L}_N, \quad N = 2^n.$$

Rudin-Shapiro Polynomials

Let $P_0(z) = 1$ and $Q_0(z) = 1$. For any integer $n \geq 1$, define

Rudin-Shapiro Polynomials

$$\begin{cases} P_n(z) := P_{n-1}(z) + z^{2^{n-1}} Q_{n-1}(z), \\ Q_n(z) := P_{n-1}(z) - z^{2^{n-1}} Q_{n-1}(z). \end{cases}$$

Polynomials $P_n(z)$ and $Q_n(z)$ are called **Rudin-Shapiro polynomials.**

Note that $P_n(z)$ and $Q_n(z)$ are polynomials with ± 1 coefficients of degree $L_n - 1$ where $L_n = 2^n$.

$$P_n(z), Q_n(z) \in \mathcal{L}_N, \quad N = 2^n.$$

Rudin-Shapiro Polynomials

Let $P_0(z) = 1$ and $Q_0(z) = 1$. For any integer $n \geq 1$, define

Rudin-Shapiro Polynomials

$$\begin{cases} P_n(z) := P_{n-1}(z) + z^{2^{n-1}} Q_{n-1}(z), \\ Q_n(z) := P_{n-1}(z) - z^{2^{n-1}} Q_{n-1}(z). \end{cases}$$

Polynomials $P_n(z)$ and $Q_n(z)$ are called **Rudin-Shapiro polynomials.** Note that $P_n(z)$ and $Q_n(z)$ are polynomials with ± 1 coefficients of degree $L_n - 1$ where $L_n = 2^n$.

$$P_n(z), Q_n(z) \in \mathscr{L}_N, \quad N = 2^n.$$

Rudin-Shapiro Polynomials

Let $P_0(z) = 1$ and $Q_0(z) = 1$. For any integer $n \geq 1$, define

Rudin-Shapiro Polynomials

$$\begin{cases} P_n(z) := P_{n-1}(z) + z^{2^{n-1}} Q_{n-1}(z), \\ Q_n(z) := P_{n-1}(z) - z^{2^{n-1}} Q_{n-1}(z). \end{cases}$$

Polynomials $P_n(z)$ and $Q_n(z)$ are called **Rudin-Shapiro polynomials.** Note that $P_n(z)$ and $Q_n(z)$ are polynomials with ± 1 coefficients of degree $L_n - 1$ where $L_n = 2^n$.

$$P_n(z), Q_n(z) \in \mathscr{L}_N, \quad N = 2^n.$$

Rudin-Shapiro Polynomials

It is well-known and easy to show that

$$\left|P_n(e^{it})\right|^2 + \left|Q_n(e^{it})\right|^2 = L_{n+1} = 2^{n+1}, \quad \text{for any } t \in [0, 2\pi).$$

Hence

$$\left|P_n(e^{it})\right| \le 2^{\frac{n+1}{2}} = \sqrt{2}\sqrt{N}, \quad \text{for any } t \in [0, 2\pi).$$

Rudin-Shapiro polynomials satisfy the upper bound in the form of Kahane's theorem.

We don't know Rudin-Shapiro polynomials satisfy the lower bound in the form of Kahane's theorem or not.

Rudin-Shapiro Polynomials

It is well-known and easy to show that

$$\left|P_n(e^{it})\right|^2 + \left|Q_n(e^{it})\right|^2 = L_{n+1} = 2^{n+1}, \quad \text{for any } t \in [0, 2\pi).$$

Hence

$$\left|P_n(e^{it})\right| \leq 2^{\frac{n+1}{2}} = \sqrt{2}\sqrt{N}, \quad \text{for any } t \in [0, 2\pi).$$

Rudin-Shapiro polynomials satisfy the upper bound in the form of Kahane's theorem.

We don't know Rudin-Shapiro polynomials satisfy the lower bound in the form of Kahane's theorem or not.

Rudin-Shapiro Polynomials

It is well-known and easy to show that

$$\left|P_n(e^{it})\right|^2 + \left|Q_n(e^{it})\right|^2 = L_{n+1} = 2^{n+1}, \quad \text{for any } t \in [0, 2\pi).$$

Hence

$$\left|P_n(e^{it})\right| \le 2^{\frac{n+1}{2}} = \sqrt{2}\sqrt{N}, \quad \text{for any } t \in [0, 2\pi).$$

Rudin-Shapiro polynomials satisfy the upper bound in the form of Kahane's theorem.

We don't know Rudin-Shapiro polynomials satisfy the lower bound in the form of Kahane's theorem or not.

Rudin-Shapiro Polynomials

It is well-known and easy to show that

$$\left|P_n(e^{it})\right|^2 + \left|Q_n(e^{it})\right|^2 = L_{n+1} = 2^{n+1}, \quad \text{for any } t \in [0, 2\pi).$$

Hence

$$\left|P_n(e^{it})\right| \le 2^{\frac{n+1}{2}} = \sqrt{2}\sqrt{N}, \quad \text{for any } t \in [0, 2\pi).$$

Rudin-Shapiro polynomials satisfy the upper bound in the form of Kahane's theorem.

We don't know Rudin-Shapiro polynomials satisfy the lower bound in the form of Kahane's theorem or not.

Rudin-Shapiro Polynomials

By the Fourier coefficients of f at k, we mean the coefficient for the term z^k, or simply

$$\widehat{f}(k) = (f)^{\wedge}(k) := \frac{1}{2\pi}\int_0^{2\pi} f(e^{it})e^{-ikt}dt.$$

By the recursive relation of the definition we have

$$|P_n|^2(z) = z^{2^{n-1}}\overline{P_{n-1}(z)}Q_{n-1}(z) + \overline{z}^{2^{n-1}}P_{n-1}(z)\overline{Q_{n-1}(z)} + 2^n,$$

$$(\overline{P_n}Q_n)(z) = 2|P_{n-1}(z)|^2 - z^{2^{n-1}}\overline{P_{n-1}(z)}Q_{n-1}(z) + \overline{z}^{2^{n-1}}P_{n-1}(z)\overline{Q_{n-1}(z)} - 2^n$$

$$(P_n\overline{Q_n})(z) = 2|P_{n-1}(z)|^2 + z^{2^{n-1}}\overline{P_{n-1}(z)}Q_{n-1}(z) - \overline{z}^{2^{n-1}}P_{n-1}(z)\overline{Q_{n-1}(z)} - 2^n$$

Main Results

We are interested in estimating $\max_k \left|\left(|P_n|^2\right)^\wedge(k)\right|$. If we write

$$|P_n(e^{it})|^2 = \sum_{k=-L_n+1}^{L_n-1} a_k z^k,$$

then

$$\begin{cases} \left(|P_n|^2\right)^\wedge(k) = a_k, & \text{when } -L_n+1 \le k \le L_n-1, \\ \left(|P_n|^2\right)^\wedge(k) = 0, & \text{when } |k| > L_n. \end{cases}$$

Main Results

We are interested in estimating $\max_k \left|\left(|P_n|^2\right)^\wedge(k)\right|$. If we write

$$|P_n(e^{it})|^2 = \sum_{k=-L_n+1}^{L_n-1} a_k z^k,$$

then

$$\begin{cases} \left(|P_n|^2\right)^\wedge(k) = a_k, & \text{when } -L_n+1 \le k \le L_n-1, \\ \left(|P_n|^2\right)^\wedge(k) = 0, & \text{when } |k| > L_n. \end{cases}$$

Main Results

We are interested in estimating $\max_k \left|\left(|P_n|^2\right)^\wedge(k)\right|$. If we write

$$|P_n(e^{it})|^2 = \sum_{k=-L_n+1}^{L_n-1} a_k z^k,$$

then

$$\begin{cases} \left(|P_n|^2\right)^\wedge(k) = a_k, & \text{when } -L_n+1 \le k \le L_n-1, \\ \left(|P_n|^2\right)^\wedge(k) = 0, & \text{when } |k| > L_n. \end{cases}$$

Main Results

Theorem 1.

If P_n and Q_n are the n-th Rudin-Shapiro polynomials and

$$|P_n(z)|^2 = \sum_{k=-L_n+1}^{L_n-1} a_k z^k, \quad |z| = 1$$

then

$$C_1 2^{\frac{n \log \lambda}{2 \log 2}} \leq \max_{1 \leq k \leq L_n - 1} |a_k| \leq C_2 2^{(0.7302859812\cdots)n}$$

with absolute constants $C_1, C_2 > 0$ and

$$\lambda := \frac{(71+6\sqrt{177})^{1/3}+(71-6\sqrt{177})^{1/3}+5}{3} = 2.75217177\cdots$$

is the real root of $x^3 - 5x^2 + 12x - 16 = 0$.
Note that $\frac{\log \lambda}{2 \log 2} = 0.7302852598\cdots$.

Main Results

Theorem 1 (Cont.).

Also, if we let

$$\left(\overline{P_n}Q_n\right)(z) = \left(P_n\overline{Q_n}\right)(1/z) = \sum_{k=-L_n+1}^{L_n-1} b_k z^k, \quad |z| = 1$$

then

$$C_3 2^{\frac{n\log\lambda}{2\log 2}} \le \max_{-L_n+1\le k\le L_n-1} |b_k| \le C_4 2^{(0.7302859812\cdots)n}$$

with absolute constants $C_3, C_4 > 0$.

Application

Littlewood Theorem [J. London Math. Soc. **41** (1966) 336-342].

Let $n \geq 1$. If $f(t) = \sum_{m=0}^{L_n - 1} b_m \cos(mt + \alpha_m)\,, b_m, \alpha_m \in \mathbb{R}\,, b_0 = 0$ satisfies

$$\|f\|_1 \geq c\mu\,, \qquad \mu := \|f\|_2\,, \qquad \sum_{m=1}^{\lfloor (L_n - 1)/h \rfloor} b_m^2 \leq 2^{-9} c^6 \mu^2$$

for some constants $c, h > 0$, and $|v| \leq 2^{-5} c^3$, then

$$\mathcal{N}(f, v) > Ah^{-1} c^5 2^n,$$

where $\mathcal{N}(f, v)$ denotes the number of real zeros of $f - v\mu$ in $(-\pi, \pi)$, and $A > 0$ is an absolute constant.

Application

Theorem 2.

If P_n and Q_n are the n-th Rudin-Shapiro polynomials,

$$R(t) := |P_n(e^{it})|^2 = \sum_{k=-L_n+1}^{L_n-1} a_k e^{ikt}$$

and

$$\max_{1 \le k \le L_n - 1} |a_k| \le C 2^{(\lambda - \varepsilon)n}$$

with absolute constants $C > 0$, $\lambda \ge 1/2$ and $\varepsilon > 0$, then there are absolute constants $A > 0$ and $B > 0$ such that the equation $R(t) = (1+\eta)2^n$ has at least $A 2^{(2-2\lambda)n}$ distinct solutions in $(-\pi, \pi)$ whenever $\eta \in [-B, B]$.

Main Results

In view of Theorem Theorem 1, we have

Corollary.

There is absolute constant $A > 0$ such that the equation $R(t) = (1 + \eta)2^n$ has at least $A2^{0.5394282n}$ distinct solutions in $(-\pi, \pi)$ whenever $|\eta| \leq 2^{-11}$.

Sketch of the Proofs

M Taghavi in1997 first claimed

$$\max_{1 \le k \le L_n - 1} |a_k| \le (3.2134) 2^{0.7303n}.$$

However, as Allouche and Saffari observed, in his proof Taghavi used an incorrect statement saying that the spectral radius of the product of some matrices is independent of the order of the factors.

Sketch of the Proofs

By induction, we have

$$(|P_n|^2)^\wedge(2k) = \left(\overline{P_n}Q_n\right)^\wedge(2k) = \left(P_n\overline{Q_n}\right)^\wedge(2k) = 0.$$

For $n \geq 1$, let S_n be the set of all **odd integers** k with $-L_n < k < L_n$ and let

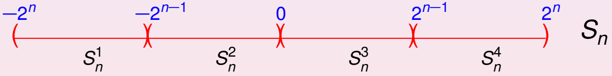
so that S_n is the disjoint union of S_n^1, S_n^2, S_n^3 and S_n^4.

Sketch of the Proofs

By induction, we have

$$\left(|P_n|^2\right)^{\wedge}(2k) = \left(\overline{P_n}Q_n\right)^{\wedge}(2k) = \left(P_n\overline{Q_n}\right)^{\wedge}(2k) = 0.$$

For $n \geq 1$, let S_n be the set of all **odd integers** k with $-L_n < k < L_n$ and let



so that S_n is the disjoint union of S_n^1, S_n^2, S_n^3 and S_n^4.

Sketch of the Proofs

For $n \geq 2$, let k_n be an odd integer in S_n. We define k_{n-1} and k'_n from k_n as follows

$$k'_n := \begin{cases} k_n + 2^n & \text{if } k_n \in S_n^1 \cup S_n^2, \\ k_n - 2^n & \text{if } k_n \in S_n^3 \cup S_n^4, \end{cases}$$

and

$$k_{n-1} := \begin{cases} k_n & \text{if } k_n \in S_n^2 \cup S_n^3, \\ k'_n & \text{if } k_n \in S_n^1 \cup S_n^4. \end{cases}$$

It is easily to see that if $k_n \in S_n$, then $k_{n-1} \in S_{n-1}$ and $k'_n \in S_n$.

$$|P_n|^2(z) = z^{2^{n-1}} \overline{P_{n-1}(z)} Q_{n-1}(z) + \overline{z}^{2^{n-1}} P_{n-1}(z) \overline{Q_{n-1}(z)} + 2^n,$$

Sketch of the Proofs

For $n \geq 2$, let k_n be an odd integer in S_n. We define k_{n-1} and k'_n from k_n as follows

$$k'_n := \begin{cases} k_n + 2^n & \text{if } k_n \in S_n^1 \cup S_n^2, \\ k_n - 2^n & \text{if } k_n \in S_n^3 \cup S_n^4, \end{cases}$$

and

$$k_{n-1} := \begin{cases} k_n & \text{if } k_n \in S_n^2 \cup S_n^3, \\ k'_n & \text{if } k_n \in S_n^1 \cup S_n^4. \end{cases}$$

It is easily to see that if $k_n \in S_n$, then $k_{n-1} \in S_{n-1}$ and $k'_n \in S_n$.

$$|P_n|^2(z) = z^{2^{n-1}} \overline{P_{n-1}(z)} Q_{n-1}(z) + \bar{z}^{2^{n-1}} P_{n-1}(z) \overline{Q_{n-1}(z)} + 2^n,$$

Sketch of the Proofs

For $n \geq 2$, let k_n be an odd integer in S_n. We define k_{n-1} and k_n' from k_n as follows

$$k_n' := \begin{cases} k_n + 2^n & \text{if } k_n \in S_n^1 \cup S_n^2, \\ k_n - 2^n & \text{if } k_n \in S_n^3 \cup S_n^4, \end{cases}$$

and

$$k_{n-1} := \begin{cases} k_n & \text{if } k_n \in S_n^2 \cup S_n^3, \\ k_n' & \text{if } k_n \in S_n^1 \cup S_n^4. \end{cases}$$

It is easily to see that if $k_n \in S_n$, then $k_{n-1} \in S_{n-1}$ and $k_n' \in S_n$.

$$|P_n|^2(z) = z^{2^{n-1}} \overline{P_{n-1}(z)} Q_{n-1}(z) + \bar{z}^{2^{n-1}} P_{n-1}(z) \overline{Q_{n-1}(z)} + 2^n,$$

Sketch of the Proofs

For $n \geq 2$, let k_n be an odd integer in S_n. We define k_{n-1} and k'_n from k_n as follows

$$k'_n := \begin{cases} k_n + 2^n & \text{if } k_n \in S_n^1 \cup S_n^2, \\ k_n - 2^n & \text{if } k_n \in S_n^3 \cup S_n^4, \end{cases}$$

and

$$k_{n-1} := \begin{cases} k_n & \text{if } k_n \in S_n^2 \cup S_n^3, \\ k'_n & \text{if } k_n \in S_n^1 \cup S_n^4. \end{cases}$$

It is easily to see that if $k_n \in S_n$, then $k_{n-1} \in S_{n-1}$ and $k'_n \in S_n$.

$$|P_n|^2(z) = z^{2^{n-1}} \overline{P_{n-1}(z)} Q_{n-1}(z) + \bar{z}^{2^{n-1}} P_{n-1}(z) \overline{Q_{n-1}(z)} + 2^n,$$

Sketch of the Proofs

$$
\begin{aligned}
|P_n|^2(z) &= z^{2^{n-1}}\overline{P_{n-1}(z)}Q_{n-1}(z) + \overline{z}^{2^{n-1}}P_{n-1}(z)\overline{Q_{n-1}(z)} + 2^n, \\
\left(\overline{P_n}Q_n\right)(z) &= 2|P_{n-1}(z)|^2 - z^{2^{n-1}}\overline{P_{n-1}(z)}Q_{n-1}(z) + \overline{z}^{2^{n-1}}P_{n-1}(z)\overline{Q_{n-1}(z)} - 2^n \\
\left(P_n\overline{Q_n}\right)(z) &= 2|P_{n-1}(z)|^2 + z^{2^{n-1}}\overline{P_{n-1}(z)}Q_{n-1}(z) - \overline{z}^{2^{n-1}}P_{n-1}(z)\overline{Q_{n-1}(z)} - 2^n
\end{aligned}
$$

Let

$$
\omega_n(k_n) := \begin{pmatrix} \left(|P_n|^2\right)^\wedge(k_n) \\ \left(\overline{P_n}Q_n\right)^\wedge(k_n') \\ \left(P_n\overline{Q_n}\right)^\wedge(k_n') \end{pmatrix}.
$$

Sketch of the Proofs

Recursive Formula.

For $n \geq 2$, we have

$$\omega_n(k_n) = \begin{cases} A\omega_{n-1}(k_{n-1}), & \text{if } k_n \in S_n^1, \\ B\omega_{n-1}(k_{n-1}), & \text{if } k_n \in S_n^2, \\ C\omega_{n-1}(k_{n-1}), & \text{if } k_n \in S_n^3, \\ D\omega_{n-1}(k_{n-1}), & \text{if } k_n \in S_n^4, \end{cases} \tag{1}$$

where

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 2 & -1 & 0 \\ 2 & 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & -1 \end{pmatrix}, D = \begin{pmatrix} 0 & 1 & 0 \\ 2 & 0 & 1 \\ 2 & 0 & -1 \end{pmatrix}.$$

Sketch of the Proofs

Applying Recursive relation repeatly , we get

$$\omega_n(k_n) = \mathcal{M}_{n-1} \cdots \mathcal{M}_2 \mathcal{M}_1 \omega_1(k_1)$$

with $\omega_1(k_1) = \pm \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}$, $k_1 = \pm 1$, and

$$\mathcal{M}_i \in T_1 := \{A, B, C, D\} \quad i = 1, \ldots, n-1.$$

Sketch of the Proofs

Applying Recursive relation repeatly , we get

$$\omega_n(k_n) = \mathcal{M}_{n-1} \cdots \mathcal{M}_2 \mathcal{M}_1 \omega_1(k_1)$$

with $\omega_1(k_1) = \pm \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, k_1 = \pm 1$, and

$$\mathcal{M}_i \in T_1 := \{A, B, C, D\} \quad i = 1, \ldots, n-1.$$

Sketch of the Proofs

Applying Recursive relation repeatly , we get

$$\omega_n(k_n) = \mathscr{M}_{n-1} \cdots \mathscr{M}_2 \mathscr{M}_1 \omega_1(k_1)$$

with $\omega_1(k_1) = \pm \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, k_1 = \pm 1$, and

$$\mathscr{M}_i \in T_1 := \{A, B, C, D\} \quad i = 1, \ldots, n-1.$$

Sketch of the Proofs

Let T_n be the set of all matrices which are a product of n matrices in $\{A, B, C, D\}$ according to recursive relation (**??**).

$$T_2 := \left\{AC, AD, B^2, BA, C^2, CD, DA, DB\right\}.$$

Sketch of the Proofs

Let T_n be the set of all matrices which are a product of n matrices in $\{A, B, C, D\}$ according to recursive relation (**??**).

$$T_2 := \left\{AC, AD, B^2, BA, C^2, CD, DA, DB\right\}.$$

Sketch of the Proofs

We let

$$T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad M_1 = AT.$$

Factorization.

For even n, every $M \in T_n$ can be written in the form of

$$M = T^{\delta_1} B^{k_0} \left(M_1^{\ell_1} B^{k_1} \right) \left(M_1^{\ell_2} B^{k_2} \right) \cdots \left(M_1^{\ell_L} B^{k_L} \right) \left(M_1^{\ell_{L+1}} B^{k_{L+1}} \right) T^{\delta_2}$$

for $\ell_1, \ell_2, \ldots, \ell_{L+1} \geq 1$, $k_1, k_2, \cdots, k_L \in \{1,2,3\}$, $k_0, k_{L+1} \in \{0,1,2,3\}$, $\delta_1, \delta_2 \in \{0,1\}$ and $\sum_{j=0}^{L+1} (\ell_j + k_j) \leq n/2$.

Sketch of the Proofs

We let

$$T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad M_1 = AT.$$

Factorization.

For even n, every $M \in T_n$ can be written in the form of

$$M = T^{\delta_1} B^{k_0} \left(M_1^{\ell_1} B^{k_1}\right)\left(M_1^{\ell_2} B^{k_2}\right) \cdots \left(M_1^{\ell_L} B^{k_L}\right)\left(M_1^{\ell_{L+1}} B^{k_{L+1}}\right) T^{\delta_2}$$

for $\ell_1, \ell_2, \ldots, \ell_{L+1} \geq 1,\ k_1, k_2, \cdots, k_L \in \{1,2,3\},\ k_0, k_{L+1} \in \{0,1,2,3\}$, $\delta_1, \delta_2 \in \{0,1\}$ and $\sum_{j=0}^{L+1} (\ell_j + k_j) \leq n/2$.

Sketch of the Proofs

The characteristic polynomial of $M_1^2 = AD$ is

$$g(x) = x^3 - 5x^2 + 12x - 16.$$

Then $g(x) = 0$ has one real root λ and two complex roots λ' and $\overline{\lambda'}$ with $|\lambda| > |\lambda'|$. Since these eigenvalues are distinct, so there is a nonsingular matrix S such that $S^{-1} M_1^2 S = \Lambda$ with $\Lambda = \mathrm{diag}[\lambda, \lambda', \overline{\lambda'}]$. Since

$$M_1^{2\ell} = S \Lambda^\ell S^{-1}$$

Therefore, we have proved that

$$||M_1^{2\ell}|| \le ||S|| ||\Lambda^\ell|| ||S^{-1}|| \le \left(||S|| ||S^{-1}|| \right) \lambda^\ell$$

where $||M|| = \sqrt{\max\{\text{ eigenvalues of } M^* M\ \}}$ is the spectral radius of M and it is known that $||AB|| \le ||A|| ||B||$.

Sketch of the Proofs

The characteristic polynomial of $M_1^2 = AD$ is

$$g(x) = x^3 - 5x^2 + 12x - 16.$$

Then $g(x) = 0$ has one real root λ and two complex roots λ' and $\overline{\lambda'}$ with $|\lambda| > |\lambda'|$. Since these eigenvalues are distinct, so there is a nonsingular matrix S such that $S^{-1}M_1^2S = \Lambda$ with $\Lambda = \text{diag}[\lambda, \lambda', \overline{\lambda'}]$. Since

$$M_1^{2\ell} = S\Lambda^{\ell}S^{-1}$$

Therefore, we have proved that

$$||M_1^{2\ell}|| \le ||S||||\Lambda^{\ell}||||S^{-1}|| \le \left(||S||||S^{-1}||\right)\lambda^{\ell}$$

where $||M|| = \sqrt{\max\{\text{ eigenvalues of } M^*M\ \}}$ is the spectral radius of M and it is known that $||AB|| \le ||A||||B||$.

Sketch of the Proofs

The characteristic polynomial of $M_1^2 = AD$ is

$$g(x) = x^3 - 5x^2 + 12x - 16.$$

Then $g(x) = 0$ has one real root λ and two complex roots λ' and $\overline{\lambda'}$ with $|\lambda| > |\lambda'|$. Since these eigenvalues are distinct, so there is a nonsingular matrix S such that $S^{-1}M_1^2 S = \Lambda$ with $\Lambda = \text{diag}[\lambda, \lambda', \overline{\lambda'}]$.

Since

$$M_1^{2\ell} = S\Lambda^\ell S^{-1}$$

Therefore, we have proved that

$$||M_1^{2\ell}|| \leq ||S|| ||\Lambda^\ell|| ||S^{-1}|| \leq \left(||S|| ||S^{-1}||\right)\lambda^\ell$$

where $||M|| = \sqrt{\max\{\text{ eigenvalues of } M^*M\ \}}$ is the spectral radius of M and it is known that $||AB|| \leq ||A|| ||B||$.

Sketch of the Proofs

The characteristic polynomial of $M_1^2 = AD$ is

$$g(x) = x^3 - 5x^2 + 12x - 16.$$

Then $g(x) = 0$ has one real root λ and two complex roots λ' and $\overline{\lambda'}$ with $|\lambda| > |\lambda'|$. Since these eigenvalues are distinct, so there is a nonsingular matrix S such that $S^{-1}M_1^2S = \Lambda$ with $\Lambda = \mathrm{diag}[\lambda, \lambda', \overline{\lambda'}]$. Since

$$M_1^{2\ell} = S\Lambda^\ell S^{-1}$$

Therefore, we have proved that

$$||M_1^{2\ell}|| \leq ||S|| ||\Lambda^\ell|| ||S^{-1}|| \leq \left(||S|| ||S^{-1}||\right)\lambda^\ell$$

where $||M|| = \sqrt{\max\{\text{ eigenvalues of } M^*M \}}$ is the spectral radius of M and it is known that $||AB|| \leq ||A|| ||B||$.

Sketch of the Proofs

The characteristic polynomial of $M_1^2 = AD$ is

$$g(x) = x^3 - 5x^2 + 12x - 16.$$

Then $g(x) = 0$ has one real root λ and two complex roots λ' and $\overline{\lambda'}$ with $|\lambda| > |\lambda'|$. Since these eigenvalues are distinct, so there is a nonsingular matrix S such that $S^{-1}M_1^2S = \Lambda$ with $\Lambda = \mathrm{diag}[\lambda, \lambda', \overline{\lambda'}]$. Since

$$M_1^{2\ell} = S\Lambda^\ell S^{-1}$$

Therefore, we have proved that

$$||M_1^{2\ell}|| \leq ||S||||\Lambda^\ell||||S^{-1}|| \leq \left(||S||||S^{-1}||\right)\lambda^\ell$$

where $||M|| = \sqrt{\max\{\text{ eigenvalues of } M^*M\ \}}$ is the spectral radius of M and it is known that $||AB|| \leq ||A||||B||$.

Sketch of the Proofs

We hope from

$$||M_1^\ell B^k|| \le C_5 \lambda^{\frac{1}{2}(\ell+k)}, \text{ for } 0 \le k \le 3.$$

we can prove that for every $M \in T_n$,

$$||M|| \ll \lambda^{n/2}$$

and finish our proof of main result.

However, there may be many of ℓ_j are small so that we have a high power of C_5 in the upper bound.

Sketch of the Proofs

We hope from

$$||M_1^{\ell} B^k|| \leq C_5 \lambda^{\frac{1}{2}(\ell+k)}, \text{ for } 0 \leq k \leq 3.$$

we can prove that for every $M \in T_n$,

$$||M|| \ll \lambda^{n/2}$$

and finish our proof of main result.
However, there may be many of ℓ_j are small so that we have a high power of C_5 in the upper bound.

Sketch of the Proofs

Instead, we will prove our result by induction on L.

In the initial step, we prove

$$||M_1^{\ell} B^k|| \leq ((1.0000005)^2 \lambda)^{\frac{1}{2}(\ell+k)} \quad (2)$$

for all $0 \leq k \leq 3, 1 \leq \ell$ and $(\ell, k) \neq (1,1)$. Namely, for $\ell + k \geq \frac{\log(C_5)}{\log(1.0000005)}$, we have

$$||M_1^{\ell} B^k|| \leq C_5 \lambda^{\frac{1}{2}(\ell+k)} \leq ((1.0000005)^2 \lambda)^{\frac{1}{2}(\ell+k)}$$

but for $\ell + k < \frac{\log(C_5)}{\log(1.0000005)}$, we need to use computer to check the inequality (1) is true.

Sketch of the Proofs

Instead, we will prove our result by induction on L.
In the initial step, we prove

$$||M_1^\ell B^k|| \le ((1.0000005)^2\lambda)^{\frac{1}{2}(\ell+k)} \qquad (2)$$

for all $0 \le k \le 3, 1 \le \ell$ and $(\ell, k) \ne (1,1)$. Namely, for $\ell + k \ge \frac{\log(C_5)}{\log(1.0000005)}$, we have

$$||M_1^\ell B^k|| \le C_5\lambda^{\frac{1}{2}(\ell+k)} \le ((1.0000005)^2\lambda)^{\frac{1}{2}(\ell+k)}$$

but for $\ell + k < \frac{\log(C_5)}{\log(1.0000005)}$, we need to use computer to check the inequality (1) is true.

Sketch of the Proofs

Instead, we will prove our result by induction on L.
In the initial step, we prove

$$||M_1^{\ell} B^k|| \le ((1.0000005)^2 \lambda)^{\frac{1}{2}(\ell+k)} \qquad (2)$$

for all $0 \le k \le 3, 1 \le \ell$ and $(\ell, k) \ne (1,1)$. Namely, for $\ell + k \ge \frac{\log(C_5)}{\log(1.0000005)}$, we have

$$||M_1^{\ell} B^k|| \le C_5 \lambda^{\frac{1}{2}(\ell+k)} \le ((1.0000005)^2 \lambda)^{\frac{1}{2}(\ell+k)}$$

but for $\ell + k < \frac{\log(C_5)}{\log(1.0000005)}$, we need to use computer to check the inequality (1) is true.

Sketch of the Proofs

Instead, we will prove our result by induction on L.
In the initial step, we prove

$$||M_1^\ell B^k|| \leq ((1.0000005)^2\lambda)^{\frac{1}{2}(\ell+k)} \tag{2}$$

for all $0 \leq k \leq 3, 1 \leq \ell$ and $(\ell, k) \neq (1,1)$. Namely, for $\ell + k \geq \frac{\log(C_5)}{\log(1.0000005)}$, we have

$$||M_1^\ell B^k|| \leq C_5\lambda^{\frac{1}{2}(\ell+k)} \leq ((1.0000005)^2\lambda)^{\frac{1}{2}(\ell+k)}$$

but for $\ell + k < \frac{\log(C_5)}{\log(1.0000005)}$, we need to use computer to check the inequality (1) is true.

Sketch of the Proofs

The term $M_1 B$ is bad since $||M_1 B|| > (1.0000005)^2 \lambda$.

We also need to prove

$$||M_1 B M_1^{\ell} B^k|| \leq ((1.0000005)^2 \lambda)^{\frac{1}{2}(\ell+k+2)}$$

for all $0 \leq k \leq 3$ and $1 \leq \ell$.

Sketch of the Proofs

The term $M_1 B$ is bad since $||M_1 B|| > (1.0000005)^2 \lambda$.
We also need to prove

$$||M_1 B M_1^\ell B^k|| \leq ((1.0000005)^2 \lambda)^{\frac{1}{2}(\ell+k+2)}$$

for all $0 \leq k \leq 3$ and $1 \leq \ell$.

Sketch of the Proofs

Using induction on L for the factorization:

$$M = T^{\delta_1} B^{k_0} \left(M_1^{\ell_1} B^{k_1} \right) \left(M_1^{\ell_2} B^{k_2} \right) \cdots \left(M_1^{\ell_L} B^{k_L} \right) \left(M_1^{\ell_{L+1}} B^{k_{L+1}} \right) T^{\delta_2}$$

Proposition.

We have

$$||M|| \ll ((1.0000005)^2 \lambda)^{n/2} = e^{0.73028598 \cdots n}$$

for any $M \in T_n$.

Theorem 1 now follows from the proposition.

Sketch of the Proofs

Using induction on L for the factorization:

$$M = T^{\delta_1} B^{k_0} \left(M_1^{\ell_1} B^{k_1}\right)\left(M_1^{\ell_2} B^{k_2}\right)\cdots\left(M_1^{\ell_L} B^{k_L}\right)\left(M_1^{\ell_{L+1}} B^{k_{L+1}}\right) T^{\delta_2}$$

Proposition.

We have

$$\|M\| \ll ((1.0000005)^2\lambda)^{n/2} = e^{0.73028598\cdots n}$$

for any $M \in T_n$.

Theorem 1 now follows from the proposition.

Sketch of the Proofs

Using induction on L for the factorization:

$$M = T^{\delta_1} B^{k_0} \left(M_1^{\ell_1} B^{k_1} \right) \left(M_1^{\ell_2} B^{k_2} \right) \cdots \left(M_1^{\ell_L} B^{k_L} \right) \left(M_1^{\ell_{L+1}} B^{k_{L+1}} \right) T^{\delta_2}$$

Proposition.

We have

$$||M|| \ll ((1.0000005)^2 \lambda)^{n/2} = e^{0.73028598 \cdots n}$$

for any $M \in T_n$.

Theorem 1 now follows from the proposition.

THE END!