Double roots of random Littlewood polynomials

Arnab Sen

University of Minnesota

Disordered Models in Mathematical Physics
Valparaíso, July 21, 2015

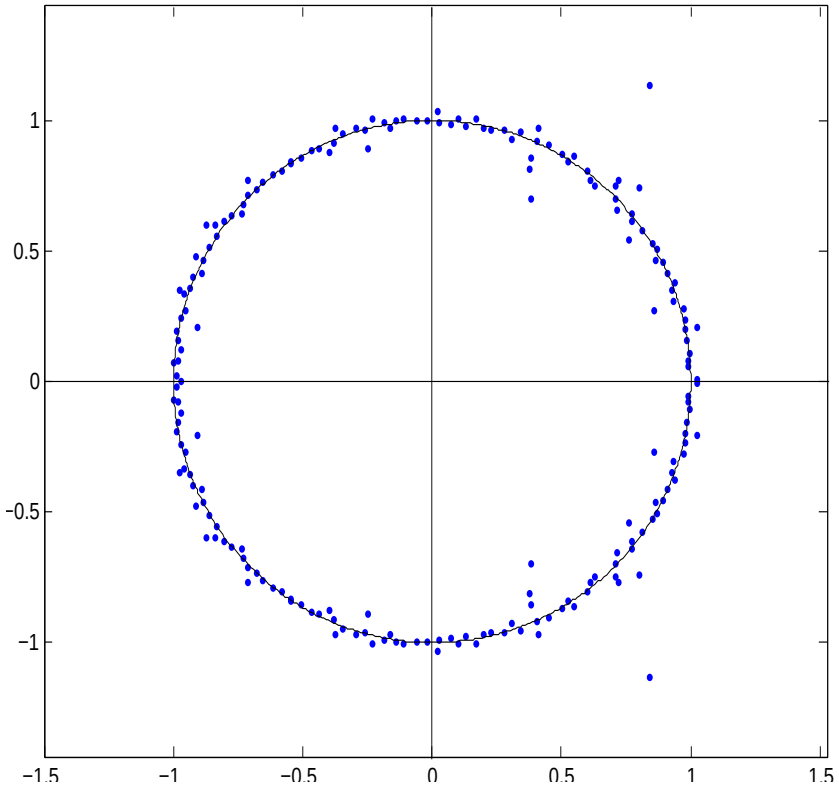
Joint with Ohad Feldheim (IMA), Ron Peled (Tel Aviv) and Ofer Zeitouni (Weizmann and NYU).

- Random Littlewood Polynomial of degree n:

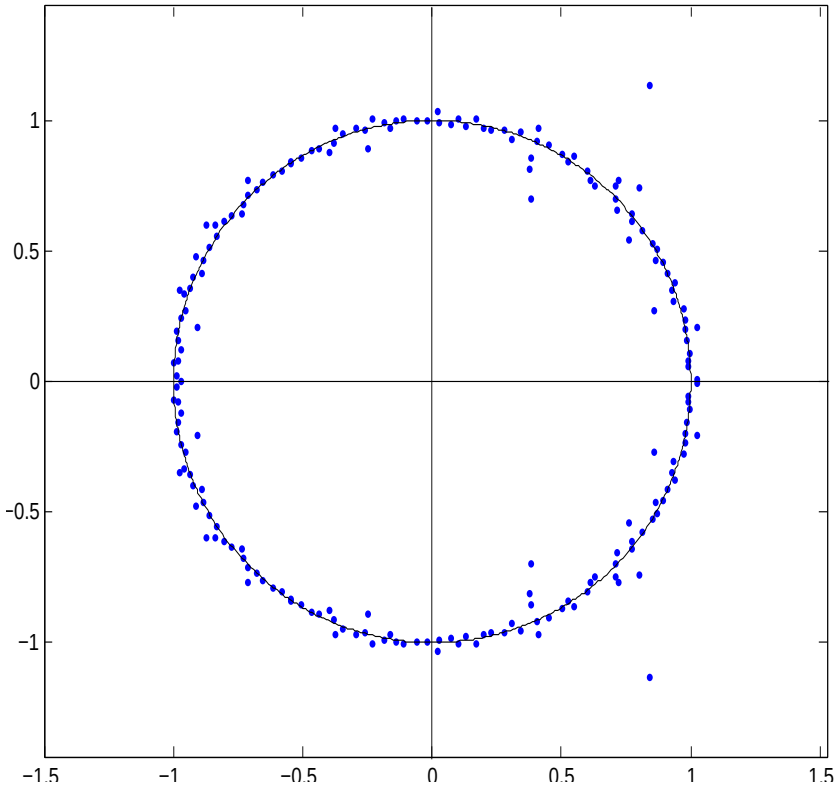
$$P(z) = \xi_0 + \xi_1 z + \xi_2 z^2 + \cdots + \xi_n z^n,$$

ξ_i's are i.i.d. with $\mathbb{P}(\xi_0 = -1) = \mathbb{P}(\xi_0 = +1) = \frac{1}{2}$.

Roots of a random Littlewood polynomial of degree 200



Roots of a random Littlewood polynomial of degree 200



- The limiting distribution of the roots is uniform on the unit circle.
- The number of real roots is $\approx \frac{2}{\pi} \log n$.

Double roots

- What is the probability that P has a double root in $\mathbb{C}$?

Double roots

- What is the probability that P has a double root in $\mathbb{C}$?

- Intuition: The double root probability should go to zero as $n \to \infty$ since the roots of random polynomials tend to repel each other.

- Let $p(z) = z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \ldots + a_0 = \prod_{i=1}^{n}(z - z_i)$ and $T : \mathbb{C}^n \to \mathbb{C}^n$ such that $(z_1, \ldots, z_n) \mapsto (a_0, a_1, \ldots, a_{n-1})$. Then T has Jacobian

$$\prod_{i<j} |z_i - z_j|^2.$$

Double roots

- What is the probability that P has a double root in $\mathbb{C}$?
- Intuition: The double root probability should go to zero as $n \to \infty$ since the roots of random polynomials tend to repel each other.
- Let $p(z) = z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \ldots + a_0 = \prod_{i=1}^{n}(z - z_i)$ and $T : \mathbb{C}^n \to \mathbb{C}^n$ such that $(z_1, \ldots, z_n) \mapsto (a_0, a_1, \ldots, a_{n-1})$. Then T has Jacobian
$$\prod_{i<j} |z_i - z_j|^2.$$
- Another related question (will not be addressed in this talk): what is the minimum separation between the roots of P in the complex plane?

P = random Littlewood polynomial of degree n.

Theorem (Peled-S.-Zeitouni'14)

$$\mathbb{P}(P \text{ has a double root}) = \begin{cases} \frac{8\sqrt{3}}{\pi n^2} + o(n^{-2}) & \text{if} \quad 4 \mid (n+1) \\ o(n^{-2}) & \text{otherwise.} \end{cases}$$

Random polynomials with (biased) ±1 coefficients.

- Let ξ_i be i.i.d. supported on $\{-1, 1\}$ such that

$$\max_{x \in \{-1,1\}} \mathbb{P}(\xi_0 = x) < \frac{1}{\sqrt{2}} = 0.707...$$

Theorem

$$\mathbb{P}(P \text{ has a double root}) = \mathbb{P}(P \text{ has a double root at } \pm 1) + o(n^{-2}).$$

$\mathbb{P}(P \text{ has a double root at } \pm 1)$

- When $\mathbb{P}(\xi_0 = -1) = \mathbb{P}(\xi_0 = +1) = \frac{1}{2}$:

$$\mathbb{P}(P \text{ has a double root at } \pm 1) = \begin{cases} \frac{8\sqrt{3}}{\pi n^2} + o(n^{-2}) & \text{if } \quad 4 \mid (n+1) \\ 0 & \text{otherwise.} \end{cases}$$

- Heuristics:

$$\mathbb{P}(P(1) = 0, P'(1) = 0) \approx \mathbb{P}\Big(P_{Gau}(1) \in [-\tfrac{1}{2}, \tfrac{1}{2}], P'_{Gau}(1) \in [-\tfrac{1}{2}, \tfrac{1}{2}]\Big)$$
$$\asymp \frac{1}{\sqrt{\mathrm{var}(P(1))}\sqrt{\mathrm{var}(P'(1))}}$$
$$\asymp \frac{1}{n^{1/2}} \frac{1}{n^{3/2}}.$$

$\mathbb{P}(P \text{ has a double root at } \pm 1)$

- When $\mathbb{P}(\xi_0 = -1) = \mathbb{P}(\xi_0 = +1) = \frac{1}{2}$:

$$\mathbb{P}(P \text{ has a double root at } \pm 1) = \begin{cases} \frac{8\sqrt{3}}{\pi n^2} + o(n^{-2}) & \text{if } \quad 4 \mid (n+1) \\ 0 & \text{otherwise.} \end{cases}$$

- Heuristics:

$$\mathbb{P}(P(1) = 0, P'(1) = 0) \approx \mathbb{P}\Big(P_{Gau}(1) \in [-\tfrac{1}{2}, \tfrac{1}{2}], P'_{Gau}(1) \in [-\tfrac{1}{2}, \tfrac{1}{2}]\Big)$$
$$\asymp \frac{1}{\sqrt{\mathrm{var}(P(1))}\sqrt{\mathrm{var}(P'(1))}}$$
$$\asymp \frac{1}{n^{1/2}} \frac{1}{n^{3/2}}.$$

- The above estimate can be proved by comparing the characteristic functions of the random vector $(P(1), P'(1))$ and its Gaussianized version.

Some basic algebraic terminologies

- algebraic numbers = roots of integral polynomial
- algebraic integers = roots of monic integral polynomial
- degree of an algebraic number = the degree of its minimal polynomial.

Better error term

Theorem

Suppose $\xi_i \in \{-1, 1\}$ *i.i.d. such that* $\max_{x \in \{-1,1\}} \mathbb{P}(\xi_0 = x) < \frac{1}{\sqrt{2}}$. *Then*

$$\mathbb{P}(P \text{ has a double root}) = \mathbb{P}(P \text{ has a double root at } \pm 1) + o(n^{-2}).$$

- ± 1 are the only roots of unity of degree 1.
- The same proof gives

  $\mathbb{P}(P$ has a double root$) =$

  $\mathbb{P}(P$ has a double root at some root of unity of degree $\leq d) + o(n^{-2d})$.

Let ξ_i be i.i.d. integer-valued random variables.

Theorem (Feldheim-Peled-S-Zeitouni' 15+)

If ξ_0 has bounded support and if

$$\max_{x \in \mathbb{Z}} \mathbb{P}(\xi_0 = x) \leq \tfrac{1}{2},$$

then

$$\mathbb{P}(P \text{ has a double root}) = \mathbb{P}(P \text{ has a double root at } 0, \pm 1) + o(n^{-2}),$$

and if $\mathbb{P}(\xi_0 = 0) = 0$, then

$$\mathbb{P}(P \text{ has a double root}) = O(n^{-2}).$$

Related results : I

- Kozma-Zeitouni '13 : Let P and Q be two independent random Littlewood polynomials of degree n. Then the probability that P and Q have a common root is

$$\underbrace{\mathbb{P}(P \text{ and } Q \text{ have a common root at } \pm 1)}_{O(n^{-1})} + o(n^{-1}).$$

Related results : I

- Kozma-Zeitouni '13 : Let P and Q be two independent random Littlewood polynomials of degree n. Then the probability that P and Q have a common root is

$$\underbrace{\mathbb{P}(P \text{ and } Q \text{ have a common root at } \pm 1)}_{O(n^{-1})} + o(n^{-1}).$$

- Main step:

$$\begin{aligned}
&\sum_{\alpha \in \mathbb{C}, \deg(\alpha) \geq D} \mathbb{P}(P(\alpha) = Q(\alpha) = 0) \\
&= \sum_{\alpha \in \mathbb{C}, \deg(\alpha) \geq D} \mathbb{P}(P(\alpha) = 0)\mathbb{P}(Q(\alpha) = 0) \\
&\leq \sup_{\alpha \in \mathbb{C}, \deg(\alpha) \geq D} \mathbb{P}(P(\alpha) = 0) \sum_{\alpha} \mathbb{P}(Q(\alpha) = 0) \\
&= n \sup_{\alpha \in \mathbb{C}, \deg(\alpha) \geq D} \mathbb{P}(P(\alpha) = 0),
\end{aligned}$$

Related results : I

- Kozma-Zeitouni '13 : Let P and Q be two independent random Littlewood polynomials of degree n. Then the probability that P and Q have a common root is

$$\underbrace{\mathbb{P}(P \text{ and } Q \text{ have a common root at } \pm 1)}_{O(n^{-1})} + o(n^{-1}).$$

- Main step:

$$\begin{aligned}
&\sum_{\alpha \in \mathbb{C}, \deg(\alpha) \geq D} \mathbb{P}(P(\alpha) = Q(\alpha) = 0) \\
&= \sum_{\alpha \in \mathbb{C}, \deg(\alpha) \geq D} \mathbb{P}(P(\alpha) = 0)\mathbb{P}(Q(\alpha) = 0) \\
&\leq \sup_{\alpha \in \mathbb{C}, \deg(\alpha) \geq D} \mathbb{P}(P(\alpha) = 0) \sum_{\alpha} \mathbb{P}(Q(\alpha) = 0) \\
&= n \sup_{\alpha \in \mathbb{C}, \deg(\alpha) \geq D} \mathbb{P}(P(\alpha) = 0), \\
&\leq n \cdot O(n^{-\frac{D}{2}}),
\end{aligned}$$

by inverse Littlewood-Offord type bounds.

Related results : II

- Do-Nguyen-Vu' 14: Let ξ_i's be i.i.d of following two types.

discrete ξ_i uniform on $\{\pm 1, \pm 2, \ldots, \pm k\}$.

continuous ξ_i has p-integrable density with $p > 1$ and $\mathbb{E}|\xi_i|^{2+\epsilon} < \infty$.

Theorem

Given any $C > 0$, there exists $B > 0$ such that

$\mathbb{P}(P$ *has a pair of real roots* $\leq n^{-B}$ *apart*$) = \mathbb{P}(P$ *has a double root at* $\pm 1) + n^{-C}$.

- Their method does not readily extend to complex roots.

Sketch of the proof

- Suppose $\xi_i \in \{-1, 1\}$ i.i.d. such that $\max_{x \in \{-1,1\}} \mathbb{P}(\xi_0 = x) < \frac{1}{\sqrt{2}}$. Then

$$\mathbb{P}(P \text{ has a double root}) = \mathbb{P}(P \text{ has a double root at } \pm 1) + o(n^{-2}).$$

- We need to show

$$\mathbb{P}(P \text{ has a double root at some } \alpha \text{ with } \deg(\alpha) \geq 2) = o(n^{-2}).$$

Lemma

Given $B > 0$ *there exists* $C > 0$ *such that*

$$\mathbb{P}\big(\exists \alpha \text{ with } \deg(\alpha) \geq C \log n \text{ such that } P \text{ has a double root at } \alpha\big) = O(n^{-B}).$$

Lemma

Given $B > 0$ there exists $C > 0$ such that

$$\mathbb{P}\big(\exists \alpha \text{ with } \deg(\alpha) \geq C \log n \text{ such that } P \text{ has a double root at } \alpha\big) = O(n^{-B}).$$

- **Proof of Lemma.** Suppose P has a double root at α with $\deg(\alpha) = d$.

  Let P_1 = minimal poly. of α in $\mathbb{Z}[x]$. Then

  $$P(z) = P_1(z)^2 P_2(z) \cdots P_m(z)$$

  where $P_i \in \mathbb{Z}[x]$ are irreducible and $P_1(\alpha) = 0$ with $\deg(P_1) = d \geq C \log n$.

- Thus $P(\pm 2)$ is divisible by the integer $P_1(\pm 2)^2$.

Claim: $\max\big(P_1(-2), P_1(2)\big)$ *has to be large if* d *is large*

- $|P_1(2)| = \prod_{i=1}^{d} |\alpha_i - 2|$ and $|P_1(-2)| = \prod_{i=1}^{d} |\alpha_i + 2|$, where $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ are conjugates of α.
- Fact: The number of roots of P outside the ball $\{z : |z| \le 3/2\}$ is $O(1)$, deterministically. [Jensen's formula]
- Hence $\#\{i : |\alpha_i| > 3/2\} = O(1)$.
-

$$
\begin{aligned}
|P_1(-2)P_1(2)| &= \prod_{i=1}^{d} |\alpha_i + 2||\alpha_i - 2| \\
&= \prod_{i:|\alpha_i|\le 3/2} |\alpha_i^2 - 4| \prod_{i:|\alpha_i|>3/2} |\alpha_i + 2||\alpha_i - 2| \\
&= \left(\tfrac{7}{4}\right)^{d-O(1)} \prod_{i:|\alpha_i|>3/2} |\alpha_i + 2||\alpha_i - 2|
\end{aligned}
$$

Claim contd.

- Let $\mathcal{E} := \{P \text{ has a root inside } B(\pm 2, n^{-K})\}$.
- Fact: For $K > 0$ big enough, $\mathbb{P}(\mathcal{E}) = O(n^{-B})$.
- On $\mathcal{E}^c$,

$$|P_1(-2)P_1(2)| = \left(\frac{7}{4}\right)^{d-O(1)} \prod_{i:|\alpha_i|>3/2} |\alpha_i + 2||\alpha_i - 2|$$
$$= \left(\frac{7}{4}\right)^{d-O(1)} n^{-2K\cdot O(1)} \geq e^{\Omega(d)} n^{-O(1)}.$$

- Thus, on $\mathcal{E}^c$, when $d \geq C \log n$,

$$\max\left(P_1(-2), P_1(2)\right) \geq n^{C_1}.$$

Proof of the lemma

- $$\mathbb{P}(P \text{ has a double root } \alpha \text{ with } \deg(\alpha) \geq C \log n)$$
$$\leq \sum_{k \geq n^{C_1}} \mathbb{P}(P(\pm 2) \text{ is divisible by } k^2) + \mathbb{P}(\mathcal{E})$$

Proof of the lemma

- $$\mathbb{P}(P \text{ has a double root } \alpha \text{ with } \deg(\alpha) \geq C \log n) \leq \sum_{k \geq n^{C_1}} \mathbb{P}(P(\pm 2) \text{ is divisible by } k^2) + \mathbb{P}(\mathcal{E})$$

- Choose r satisfying $2^r \leq k^2 < 2^{r+1}$. Note that $|\sum_{j=0}^{r-1} \xi_j 2^j| < 2^r/2$.

$$\mathbb{P}\left(P(2) \bmod k^2 = 0\right) \leq \max_{m \in \mathbb{Z}} \mathbb{P}\left(\sum_{j=0}^{r-1} \xi_j 2^j \bmod k^2 = m\right) = \max_{m \in \mathbb{Z}} \mathbb{P}\left(\sum_{j=0}^{r-1} \xi_j 2^j = m\right).$$

- The mapping $(a_0, \ldots, a_{r-1}) \mapsto \sum_{j=0}^{r-1} a_j 2^j$ is one-to-one on $\{-1, 1\}^r$.

- $$\max_{m \in \mathbb{Z}} \mathbb{P}\left(\sum_{j=0}^{r-1} \xi_j 2^j = m\right) \leq \left(\max_{x \in \{-1,1\}} \mathbb{P}(\xi_0 = x)\right)^r := \left(\frac{1}{\sqrt{2}} - \delta\right)^r.$$

$$\leq \left(\frac{1}{\sqrt{2}} - \delta\right)^{\frac{2 \log k}{\log 2}} = k^{-\gamma}, \quad \text{for some } \gamma > 1.$$

P cannot have low degree roots far away from the unit circle

Lemma

For any algebraic integer $\alpha \neq 0$,

$$\mathbb{P}(\alpha \text{ is a root of } P) \leq e^{-c\left|1-|\alpha|\right|n}.$$

P cannot have low degree roots far away from the unit circle

Lemma

For any algebraic integer $\alpha \neq 0$,

$$\mathbb{P}(\alpha \text{ is a root of } P) \leq e^{-c\left|1-|\alpha|\right|n}.$$

- **Fact.**

$$\#\Big\{\text{algebraic integers with algebraic degree} = O(\log n)$$
$$\text{such that all of their conjugates are inside } \{\tfrac{1}{2} < |z| < 2\}\Big\} \leq e^{C(\log n)^2}.$$

- A simple union bound implies that

$$\mathbb{P}\Big(P(\alpha) = 0 \text{ for some } \alpha \text{ with } \deg(\alpha) = O(\log n),$$
$$\text{and } \underbrace{|1-|\alpha||}_{\text{or any conjugate of } \alpha} = \Omega((\log n)^3/n)\Big) = O(n^{-3}).$$

- Let $\alpha = \exp(\frac{2\pi i}{k})$ and let $d := \deg(\alpha)$.

Lemma

$$\mathbb{P}(\alpha \text{ is a double root of } P) \leq \left(\frac{cn}{k}\right)^{-2d}.$$

- Example: When $\alpha = \sqrt{-1}$, then $k = 4$ and $d = 2$. So,

$$\mathbb{P}(P \text{ has a double root at } \sqrt{-1}) = O(n^{-4}).$$

- If $d \geq 2$ and $k \ll n$, then

$$\mathbb{P}(\alpha \text{ is a double root of } P) = O(n^{-4(1+o(1))}).$$

Counting low degree roots of unity

- Let α be kth primitive root of unity with $\deg(\alpha) = d$.
- The minimal polynomial of α is given by the kth cyclotomic polynomial

$$\Phi_k(x) := \prod_{\substack{1 \le j \le k, \\ \gcd(j,k)=1}} (1 - e^{2\pi i j/k}) \in \mathbb{Z}[x]$$

- The number of cyclotomic polynomials of degree $\le d$ is $O(d \log\log d)$.

Low degree roots of unity can not be a double root of P

The probability that some roots of unity of degree between 2 and $O(\log n)$ is a double root of P is at most

$$O(\log n \log\log\log n) \times O(n^{-4(1+o(1))}) = o(n^{-2}).$$

α = algebraic integer.

- High algebraic degree, i.e., $\deg(\alpha) \geq C \log n$. Done.
- Low algebraic degree, i.e., $\deg(\alpha) \leq C \log n$.

  Case I. Roots far off unit circle. α has a conjugate root β such that $|1 - |\beta|| = \Omega\left(\frac{(\log n)^3}{n}\right)$. Done.

  Case II. Roots of unity (of $\deg \geq 2$). Done.

  Case III. Intermediate case. α is NOT a root of unity and ALL conjugates of α are within distance $O\left(\frac{(\log n)^3}{n}\right)$ from the unit circle. Needs to be done.

Intermediate case does not arise!

- If α is an algebraic integer having minimal polynomial

$$g(z) = \prod_{\beta \in C(\alpha)} (z - \beta) \qquad [\text{monic}]$$

- The Mahler measure of α :

$$M(\alpha) := \prod_{\substack{\beta \in C(\alpha) \\ |\beta| \geq 1}} |\beta| \quad \geq 1.$$

Intermediate case does not arise!

- If α is an algebraic integer having minimal polynomial

$$g(z) = \prod_{\beta \in C(\alpha)} (z - \beta) \qquad [\text{monic}]$$

- The Mahler measure of α :

$$M(\alpha) := \prod_{\substack{\beta \in C(\alpha) \\ |\beta| \geq 1}} |\beta| \quad \geq 1.$$

- $M(\alpha) = 1 \Leftrightarrow \quad \alpha = 0 \quad$ OR $\quad \alpha$ is a root of unity.

Intermediate case does not arise!

- If α is an algebraic integer having minimal polynomial

$$g(z) = \prod_{\beta \in C(\alpha)} (z - \beta) \qquad [\text{monic}]$$

- The Mahler measure of α :

$$M(\alpha) := \prod_{\substack{\beta \in C(\alpha) \\ |\beta| \geq 1}} |\beta| \quad \geq 1.$$

- $M(\alpha) = 1 \Leftrightarrow \quad \alpha = 0 \quad$ OR $\quad \alpha$ is a root of unity.

- Lehmer's conjecture (1933): there exists an absolute constant $\mu > 1$ such that

$$\text{either} \quad M(\alpha) = 1 \quad \text{or} \quad M(\alpha) \geq \mu.$$

A partial result on Lehmer's conjecture

- Dobrowolski' 79:

$$M(\alpha) = 1 \text{ or } M(\alpha) \geq \exp\left(c\left(\frac{\log\log d}{\log d}\right)^3\right) \forall \text{ alg. integer } \alpha \text{ with } \deg(\alpha) = d.$$

A partial result on Lehmer's conjecture

- Dobrowolski' 79:

$$M(\alpha) = 1 \text{ or } M(\alpha) \geq \exp\left(c\left(\frac{\log\log d}{\log d}\right)^3\right) \forall \text{ alg. integer } \alpha \text{ with } \deg(\alpha) = d.$$

- If $\alpha \neq 0$ or α is not a root of unity, then

$$\exists \beta \in C(\alpha) \text{ such that } |\beta| \geq 1 + \frac{c}{d}\left(\frac{\log\log d}{\log d}\right)^3.$$

- Dobrowolski' 79:

  $$M(\alpha) = 1 \text{ or } M(\alpha) \geq \exp\left(c\left(\frac{\log\log d}{\log d}\right)^3\right) \forall \text{ alg. integer } \alpha \text{ with } \deg(\alpha) = d.$$

- If $\alpha \neq 0$ or α is not a root of unity, then

  $$\exists \beta \in C(\alpha) \text{ such that } |\beta| \geq 1 + \frac{c}{d}\left(\frac{\log\log d}{\log d}\right)^3.$$

- If $\alpha \neq 0$ or α is not a root of unity and $\deg(\alpha) \leq C \log n$, then there exists a conjugate β of α which is at least

  $$c(\log n)^{-1}(\log\log n)^{-3} \gg \frac{(\log n)^3}{n}$$

  away from the unit circle.

- Hence intermediate case does not arise.

Difficulties in the general case

- A key ingredient in the earlier proof of lemma concerning high algebraic degree:

  When $\xi_i \in \{-1, +1\}$ with $\max_{x \in \{-1,+1\}} \mathbb{P}(\xi_i = x) = \frac{1}{\sqrt{2}} - \delta$, then

$$\max_{m \in \mathbb{Z}} \mathbb{P}\left(P(\pm 2) = m\right) \leq \left(\max_{x \in \{-1,+1\}} \mathbb{P}(\xi_0 = x) \right)^{n+1} \leq \left(\frac{1}{\sqrt{2}} \right)^{n(1+\epsilon)}.$$

- Let ξ_i be i.i.d. $\mathbb{Z}$-valued with $\max_{x\in\mathbb{Z}} \mathbb{P}(\xi_0 = x) \le \frac{1}{2}$, then

$$\max_{m\in\mathbb{Z}} \mathbb{P}\left(P(\pm 2) = m\right) \le \left(\frac{1}{\sqrt{2}}\right)^{n(1+\epsilon)}.$$

- Example: If $\mathbb{P}(\xi_0 = 0) = \frac{1}{2}, \mathbb{P}(\xi_0 = -1) = \frac{1}{4}$ and $\mathbb{P}(\xi_0 = 2) = \frac{1}{4}$, then one can check

$$\mathbb{P}(P(2) = 0) \ge 0.6^n$$

- The proof of the result is rather long, but it starts with ...

ξ_0 is integer-valued $+ \max_x \mathbb{P}(\xi_0 = x) \le \frac{1}{2} \Leftrightarrow \xi_0$ is a mixture of Bernoulli

$$\text{mixture of Bernoulli} \ : \quad \sum_i t_i \left(\tfrac{1}{2}\delta_{a_i} + \tfrac{1}{2}\delta_{b_i}\right),$$

where $t_i \ge 0, \quad \sum_i t_i = 1, \quad a_i \ne b_i \in \mathbb{Z}$.

Difficulties in the general case: II

- The roots of P are now algebraic numbers instead of algebraic integers. Let $a_d z^d + \ldots + a_1 z + a_0 \in \mathbb{Z}[x]$ be the minimal polynomial of α.

- The Mahler measure of α :

$$M(\alpha) := |a_d| \prod_{\substack{\beta \in C(\alpha) \\ |\beta| \geq 1}} |\beta| \quad \geq 1.$$

- Lehmer's conjecture trivially holds for the non-monic case $|a_d| > 1$

A replacement for Dobrowolski's result

- Using a result of Dubickas'99, we can show that

Theorem

Let $\epsilon > 0$ and a_0 be a non-zero integer. Then, for all d sufficiently large, the number of polynomials $f \in \mathbb{Z}[x]$ of degree d with leading coefficient a_0 such that

$$\text{max modulus of the roots of } f < 1 + \frac{\epsilon \log d}{|a_0| d}$$

is less than $\exp((|a_0|d)^{2/3+\epsilon})$.

- The number of all possible polynomial factors in the 'intermediate' case $o(n^{\epsilon})$.

An open question

- **Conjecture.** The probability that a random Littlewood polynomial of degree n is reducible goes to zero as $n \to \infty$.

- Konyagin (1999): If the coefficient distribution is uniform on $\{0, 1\}$, then whp any irreducible factor of the random polynomial P has degree at least $cn/\log n$.

Thank you!