ISRAEL JOURNAL OF MATHEMATICS **213** (2016), 55–77
DOI: 10.1007/s11856-016-1328-3

DOUBLE ROOTS OF RANDOM LITTLEWOOD POLYNOMIALS

BY

Ron Peled*

School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
e-mail: peledron@post.tau.ac.il

AND

Arnab Sen**

Department of Mathematics, University of Minnesota
206 Church st. SE, Minneapolis, MN 55455, USA
e-mail: arnab@umn.edu

AND

Ofer Zeitouni†

Department of Mathematics, The Weizmann Institute of Science
POB 26, Rehovot 76100, Israel
and
Courant Institute, 251 Mercer Street, New York, NY 10012, USA
e-mail: ofer.zeitouni@weizmann.ac.il

* Supported by an ISF grant and an IRG grant.

** Supported by NSF grant 1406247.

† Supported by an ISF grant and by the Herman P. Taubman professorial chair of Mathematics at WIS.

Received September 6, 2014 and in revised form January 15, 2015.

ABSTRACT

We consider random polynomials whose coefficients are independent and uniform on $\{-1,1\}$. We prove that the probability that such a polynomial of degree n has a double root is $o(n^{-2})$ when $n+1$ is not divisible by 4 and asymptotic to $\frac{8\sqrt{3}}{\pi n^2}$ otherwise. This result is a corollary of a more general theorem that we prove concerning random polynomials with independent, identically distributed coefficients having a distribution which is supported on $\{-1,0,1\}$ and whose largest atom is strictly less than $1/\sqrt{3}$. In this general case, we prove that the probability of having a double root equals the probability that either -1, 0 or 1 are double roots up to an $o(n^{-2})$ factor and we find the asymptotics of the latter probability.

1. Introduction

A Littlewood polynomial is a polynomial whose coefficients are all in $\{-1,1\}$. By a random Littlewood polynomial of degree n we mean a Littlewood polynomial chosen uniformly among all the 2^{n+1} Littlewood polynomials of degree n. In this paper we investigate the probability that a random Littlewood polynomial has a double root and show that it is $O(n^{-2})$, and compute it up to an error of order $o(n^{-2})$.

Our result concerning random Littlewood polynomials is a corollary of a more general theorem that we now state. Let (ξ_j), $j\geq 0$, be an independent, identically distributed sequence of random variables taking values in $\{-1,0,1\}$. Let $n\geq 1$ and define the random polynomial P by

$$P(z) := \sum_{j=0}^{n} \xi_j z^j.$$

For a complex number z define the event

$$D_z := \{z \text{ is a double root of } P\}.$$

Theorem 1.1: *If*

$$\max_{x\in\{-1,0,1\}} \mathbb{P}(\xi_0 = x) < \frac{1}{\sqrt{3}} \tag{1}$$

then

$$\mathbb{P}(P \text{ has a double root}) = \mathbb{P}(\cup_z D_z) = \mathbb{P}(D_{-1}\cup D_0\cup D_1) + o(n^{-2}) \quad \text{as } n\to\infty. \tag{2}$$

Thus, up to a $o(n^{-2})$ factor, the probability of having a double root is dominated by the probability that either $-1, 0$ or 1 are double roots. Here and later in the paper we write $o(a_n)$ to denote a term δ_n, where the sequence (δ_n) depends only on the distribution of ξ_0 and satisfies $\lim_{n\to\infty} \delta_n/a_n = 0$. Similarly, $\delta_n = O(a_n)$ means that $\limsup_{n\to\infty} |\delta_n|/a_n < \infty$.

Our next theorem calculates the asymptotics of the double root probability.

Theorem 1.2: *Assume condition* (1). *First,*

$$\lim_{n\to\infty} \mathbb{P}(P \textit{ has a double root}) = \mathbb{P}(\xi_0 = 0)^2. \tag{3}$$

Second, if

$$\mathbb{P}(\xi_0 = 0) = 0 \tag{4}$$

then

$$\mathbb{P}(P \textit{ has a double root}) = \frac{L_n}{n^2} + o(n^{-2}) \quad \textit{as } n \to \infty, \tag{5}$$

where L_n denotes the periodic sequence

$$L_n := \begin{cases} \frac{8\sqrt{3}}{\pi \operatorname{Var}(\xi_0)} & \textit{if } \mathbb{E}(\xi_0) = 0 \textit{ and } n+1 \textit{ is divisible by } 4, \\ \frac{4\sqrt{3}}{\pi \operatorname{Var}(\xi_0)} & \textit{if } \mathbb{E}(\xi_0) \neq 0 \textit{ and } n+1 \textit{ is divisible by } 4, \\ 0 & \textit{if } n+1 \textit{ is not divisible by } 4. \end{cases} \tag{6}$$

We make a few remarks regarding the theorems.

(1) The event that P possesses a double root is the same as the event that P and P' have a common root, which necessarily must lie in the annulus $\mathcal{A} = \{1/2 \leq |z| \leq 2\}$ or at 0. Since the correlation coefficient between $P(z)$ and $P'(z)$ is bounded away from 1 as $n \to \infty$ uniformly in $\mathcal{A}$, a natural heuristic is that the probability that P possesses a double root is up to a multiplicative constant asymptotically the same as the probability that P and an independent copy of P' possess a common root, which by local CLT considerations and some analysis should be at most of order n^{-2} when $\mathbb{P}(\xi_0 = 0) = 0$ (in case one considers P and an independent copy $\tilde{P}$ of P, such an analysis was carried out in [KZ13]). Directly carrying out this heuristic seems, however, challenging.

(2) We do not know if condition (1), or a condition of a similar kind, is necessary for the conclusion (2) of Theorem 1.1 to hold; the theorem does cover the interesting cases where the distribution of the coefficients ξ_i is uniform on all three of $\{-1, 0, 1\}$ or uniform on any two of these values. See the open problems section for further information.

(3) In case $n+1$ is not divisible by 4, our results for $\mathbb{P}(\xi_0 = 0) = 0$ do not yield the leading term in the asymptotic expansion of the left side of (2); by parity consideration, in that situation, ± 1 cannot be a double root of P. In that situation, one needs to consider also roots of unity of algebraic degree larger than 1. The asymptotics then depend on further arithmetic properties of n. While our methods could in principle be adapted to yield such results, we do not attempt to do so. We note, however, that under certain number theoretic assumptions, there exist infinitely many n for which the polynomial P is deterministically irreducible, indeed, even the deterministic polynomial P mod 2 is irreducible mod 2; see [MO09].

(4) Our methods could also be used in evaluating the probability that P possesses a root of multiplicity k. We expect that under the condition (1), the probability of having a root of multiplicity $k \geq 2$ (fixed) equals $\mathbb{P}(\text{either } -1, 0 \text{ or } +1 \text{ is a root of order of } k) + o(n^{-k^2/2})$. We have, however, not verified the details of this assertion. Note that, as described in the next remark, it is known [FL99] that the probability that 1 is a root of multiplicity k is of order $O(n^{-k^2/2})$ for random Littlewood polynomials.

(5) When dealing with random Littlewood polynomials and when $n+1$ is divisible by 4, the asymptotic probability that -1 or 1 are double roots of P is already known and has an interesting history which we briefly sketch. It suffices, as one may check simply (see (24) and (25)), to show that

$$\mathbb{P}(P(1) = P'(1) = 0) = \frac{4\sqrt{3}}{\pi n^2} + o(n^{-2}). \tag{7}$$

That is, one needs to count the number of ± 1 sequences $\{a_i\}_{i=0}^n$ such that $\sum_{i=0}^n a_i = 0$ and $\sum_{i=1}^n i a_i = 0$. Setting $b_i = a_{i-1}$, this is the same as counting the number of solutions of the system of equations $\sum_{i=1}^{n+1} b_i = 0$ and $\sum_{i=1}^{n+1} i b_i = 0$, with $b_i \in \{-1, 1\}$. The latter is a quantity appearing in coding theory, namely, the number of spectral-null codes of second order and length $n+1$, denoted $\mathcal{S}(n+1, 2)$, which was evaluated (non-rigorously, and with a slightly different motivation) already in [SN86], and rigorously in [FL99]. Both derivations start from the substitution $X_i = (b_i + 1)/2$ to show that $\mathcal{S}(n+1, 2)$ equals the number of partitions with distinct parts of $(n+1)(n+2)/4$ into

$(n+1)/2$ parts with largest part at most $n+1$. The authors in [FL99] then derive a local CLT, which implies the required asymptotics. Our proof proceeds with a somewhat different approach to the local CLT, using some ideas from [KLP13].

1.1. Overview of the proof of Theorem 1.1. Recall that the minimal polynomial of an algebraic integer α is the monic polynomial in $\mathbb{Z}[x]$ of least degree such that α is a root of that polynomial. We denote by $\deg(\alpha)$ the algebraic degree of an algebraic integer α, i.e., the degree of its minimal polynomial.

The first and perhaps most crucial step of our argument is the following lemma which allows us to discard the algebraic integers with sufficiently high degrees. The proof of the lemma is based on an idea appearing in a work of Filaseta and Konyagin [FK96].

Lemma 1.3 (High degree): *Under the assumption* (1) *there exist constants* $C, c > 0$ *such that for any* $1 \le d \le n$,

$$\mathbb{P}(P \textit{ has a double root } \alpha \textit{ with } \deg(\alpha) \ge d) \le C\exp(-cd).$$

As we are aiming for an error of size $o(n^{-2})$, as in (2), the lemma allows us to restrict attention to algebraic integers α with $\deg(\alpha) = O(\log n)$. We shall then make use of Dobrowolski's result on Lehmer's conjecture [D79] to further restrict attention to two cases: the case when α is a root of unity or $\alpha = 0$ and the case when there is a conjugate β of α such that β lies a bit far away from the unit circle, more precisely

$$|\beta| > 1 + \frac{c}{\log n}\Big(\frac{\log\log n}{\log n}\Big)^3.$$

The first case is addressed in the following lemma whose proof relies on a classical anti-concentration result of Sárközi and Szemerédi [SS65].

Lemma 1.4 (Roots of unity): *Under the assumption* (1) *there exists a constant* $C > 0$ *such that if* α *satisfies* $\alpha^k = 1$ *for some* $k \ge 1$ *then*

$$\mathbb{P}(\alpha \textit{ is a root of } P') \le \Big(\frac{C}{\lfloor\frac{n}{k}\rfloor}\Big)^{\frac{3\deg(\alpha)}{2}}.$$

Using Lemma 1.4, we will show that if α is a root of unity with $\deg(\alpha) = O(\log n)$ and $\deg(\alpha) \ge 2$, then

$$\mathbb{P}(\alpha \text{ is a root of } P') \le O\Big(\Big(\frac{\log n \log\log\log n}{n}\Big)^3\Big).$$

Since there are not many such roots of unity, in fact $O((\log n \log\log\log n)^2)$ of them, a simple union bound implies that

$$\begin{aligned}\mathbb{P}(P' \text{ has a root } \alpha \text{ such that } \alpha \text{ is a root of unity and } 2 \leq \deg(\alpha) = O(\log n))\\ = o(n^{-2}).\end{aligned}$$

Finally, we deal with the second case as follows. We will show that the probability that α is a root of P decreases very rapidly with the distance of α from the unit circle.

Lemma 1.5 (Far from the unit circle): *Under the assumption* (1), *for any algebraic integer* $\alpha \neq 0$,

$$\mathbb{P}(\alpha \textit{ is a root of } P) \leq e^{-\frac{n\log 3}{2\lceil \log 3/|\log|\alpha||\rceil}}.$$

The proof of the above lemma is elementary and is based on a sparsification argument. We shall apply the lemma for α satisfying

$$|\alpha| > 1 + \frac{c}{\log n}\Big(\frac{\log\log n}{\log n}\Big)^3.$$

Since there are only $\exp(O((\log n)^2))$ potential roots of P with algebraic degree $O(\log n)$ (see Lemma 5.1), a union bound yields an error estimate of $o(n^{-2})$ for the second case too. Therefore, we conclude that the probability that P has a double root is the same as the probability that P has a double root at $-1, 0$ or 1 up to an error of $o(n^{-2})$.

1.2. Structure of the paper. Section 2 is dedicated to handling roots of high algebraic degrees, i.e., to the proof of Lemma 1.3. Section 3 treats roots of unity and provides the proof of Lemma 1.4. Section 4 handles roots that are far away from the unit circle, providing the proof of Lemma 1.5. Section 5 is dedicated to the deduction of Theorem 1.1. Section 6 is dedicated to the local CLT and proof of Theorem 1.2. The paper ends with a few open questions.

Acknowledgements. We are grateful to Van Vu for mentioning the relevance of Lehmer's conjecture and Hoi H. Nguyen for the reference to Filaseta and Konyagin [FK96]. Also, AS is indebted to Manjunath Krishnapur for many insightful discussions. We thank an anonymous referee for spotting an error in our original proof of Proposition 6.1, and Mei–Chu Chang for correspondence [Ch14] concerning Assumption (1).

2. High algebraic degree

In this section we prove Lemma 1.3. We start with two preliminary claims.

Claim 2.1: *There exists a constant M such that for any $n \geq 1$ and any nonzero polynomial f of the form $f(z) = \sum_{i=0}^{n} a_i z^i$ with $a_i \in \{-1, 0, 1\}$ for all $0 \leq i \leq n$, the number of $z \in \mathbb{C}$ for which $f(z) = 0$ and $|z| \geq \frac{3}{2}$ is at most M.*

Proof. Assume, without loss of generality, that $|a_n| = 1$. Let

$$\tilde{f}(z) = z^n f(z^{-1}) = \sum_{i=0}^{n} a_i z^{n-i}$$

be the reciprocal polynomial of f. Denote by $N(f)$ the number of $z \in \mathbb{C}$ for which $f(z) = 0$ and $|z| \geq \frac{3}{2}$. Then $N(f)$ is also the number of $z \in \mathbb{C}$ for which $\tilde{f}(z) = 0$ and $|z| \leq \frac{2}{3}$. Noting that $|\tilde{f}(0)| = 1$ we may apply Jensen's formula (see, e.g., [A78, Chapter 5.3.1]) and obtain for any $r > \frac{2}{3}$ that

$$\begin{aligned}\max_{0\leq\theta\leq 2\pi} \log|\tilde{f}(re^{i\theta})| \geq & \frac{1}{2\pi}\int_0^{2\pi} \log|\tilde{f}(re^{i\theta})| d\theta \\ = & \log|\tilde{f}(0)| + \sum_{z:\ \tilde{f}(z)=0,\ |z|\leq r} \log\left(\frac{r}{|z|}\right) \\ \geq & N(f)\log\left(\frac{r}{2/3}\right).\end{aligned}$$

Observe that when $r < 1$ we have $|\tilde{f}(re^{i\theta})| \leq \frac{1}{1-r}$ for all θ. Thus

$$N(f) \leq \frac{1}{(1-r)\log(3r/2)}, \quad \frac{2}{3} < r < 1$$

and substituting $r = 0.82$, say, yields that $N(f) \leq 26$, finishing the proof. ∎

Claim 2.2: *Let P be the random polynomial from Theorem 1.1 and assume (1). There exist constants $C, c > 0$ such that for any $B > 0$ we have*

$$\mathbb{P}(\textit{P(3) is divisible by } k^2 \textit{ for some integer } k \geq B) \leq CB^{-c}.$$

Proof. Let $k \geq 1$ be an integer and let r be the integer satisfying $3^r \leq k^2 < 3^{r+1}$. By conditioning on $\xi_r, \xi_{r+1}, \ldots, \xi_n$ we have

$$\mathbb{P}(P(3) \bmod k^2{=}0) \leq \max_{m\in\mathbb{Z}} \mathbb{P}\Bigg(\sum_{j=0}^{r-1}\xi_j 3^j \bmod k^2{=}m\Bigg) = \max_{m\in\mathbb{Z}} \mathbb{P}\Bigg(\sum_{j=0}^{r-1}\xi_j 3^j = m\Bigg), \tag{8}$$

where the last equality follows from the fact that

$$\left|\sum_{j=0}^{r-1}\xi_j 3^j\right| \le \frac{1}{2}(3^r - 1)$$

deterministically and $k^2 \ge 3^r$ by the definition of r. Write

$$\max_{x\in\{-1,0,1\}} \mathbb{P}(\xi_0 = x) = \frac{1}{\sqrt{3}} - \delta \in [\frac{1}{3}, \frac{1}{\sqrt{3}})$$

by the assumption (1). Observe that

$$\text{(9)} \qquad \text{the mapping } (a_0,\dots,a_{r-1}) \mapsto \sum_{j=0}^{r-1} a_j 3^j \text{ is one-to-one on } \{-1,0,1\}^r$$

as the ternary expansion of an integer is unique. Thus,

$$\text{(10)} \qquad \max_{m\in\mathbb{Z}} \mathbb{P}\Big(\sum_{j=0}^{r-1}\xi_j 3^j = m\Big) \le \Big(\frac{1}{\sqrt{3}} - \delta\Big)^r.$$

Combining (8) and (10) with the fact that $r > \frac{2\log k}{\log 3} - 1$ we deduce that

$$\mathbb{P}(P(3) \bmod k^2 = 0) \le 3\Big(\frac{1}{\sqrt{3}} - \delta\Big)^{\frac{2\log k}{\log 3}} = 3k^{-\gamma},$$

where

$$\gamma := -\log\Big(\frac{1}{\sqrt{3}} - \delta\Big)/\log\sqrt{3} > 1.$$

Summing over $k \ge B$ we obtain

$$\mathbb{P}(\text{P(3) is divisible by } k^2 \text{ for some integer } k \ge B) \le CB^{-(\gamma-1)},$$

for some suitable constant $C > 0$, as required. ∎

We now complete the proof of Lemma 1.3. Let P be the random polynomial from Theorem 1.1 and assume (1). Fix $1 \le d \le n$. Let α be an algebraic integer of degree d with (monic) minimal polynomial g. Denote by $C(\alpha)$ the set of algebraic conjugates of α (i.e., the set of roots of g). Suppose that α is a double root of P. Then, necessarily g divides P and therefore $|\beta| \le 2$ for all $\beta \in C(\alpha)$ and, by Claim 2.1, all but at most M of the $\beta \in C(\alpha)$ satisfy $|\beta| \le \frac{3}{2}$. We conclude that

$$|g(3)| = \prod_{\beta\in C(\alpha)} |3 - \beta| \ge (\tfrac{3}{2})^{d-M} \ge c_1(\tfrac{3}{2})^d,$$

where $c_1 := (\frac{3}{2})^{-M} > 0$. In addition, the facts that α is a double root of P and that α cannot be a multiple root of g, since in that case α is also a root of g' violating the minimality of g, imply that g^2 divides P in $\mathbb{Z}[x]$ so that, in particular, the integer $P(3)$ is divisible by $g(3)^2$. Putting the above facts together we arrive at the inclusion of events

$$\begin{aligned}&\{\alpha \text{ is a double root of } P\}\\ &\qquad\subseteq \{P(3) \text{ is divisible by } k^2 \text{ for some integer } k \geq c_1(\tfrac{3}{2})^d\}.\end{aligned}$$

Lemma 1.3 now follows from Claim 2.2.

3. Roots of unity

In this section we prove Lemma 1.4. We make use of the following anti-concentration result of Sárközi and Szemerédi [SS65].

Theorem 3.1: *Let (ε_j), $1 \leq j \leq N$, be independent random variables with $\mathbb{P}(\varepsilon_j = 0) = \mathbb{P}(\varepsilon_j = 1) = \frac{1}{2}$. There exists a constant $C > 0$ such that for any* distinct *integers (a_j), $1 \leq j \leq N$, we have*

$$\max_{m\in\mathbb{Z}} \mathbb{P}\bigg(\sum_{j=1}^{N} \varepsilon_j a_j = m\bigg) \leq \frac{C}{N^{3/2}}.$$

Clearly, by a linear change of variable, the theorem continues to hold when $\mathbb{P}(\varepsilon_j = a) = \mathbb{P}(\varepsilon_j = b) = \frac{1}{2}$ for any $\{a, b\} \subset \mathbb{Z}$. The following corollary extends this to our non-symmetric setting.

Corollary 3.2: *Let (ξ_j) be as in Theorem 1.1. There exists a constant $C > 0$ such that for any distinct integers (a_j), $1 \leq j \leq N$, we have*

$$\max_{m\in\mathbb{Z}} \mathbb{P}\bigg(\sum_{j=1}^{N} \xi_j a_j = m\bigg) \leq \frac{C}{N^{3/2}}.$$

Proof. Using the assumption (1) there exists some $p > (1 - \frac{1}{\sqrt{3}})$, $a \neq b \in \{-1, 0, 1\}$ and a random variable η supported in $\{-1, 0, 1\}$ such that if we let ε be uniform on $\{a, b\}$ then the distribution of ξ_1 has the distribution of the mixture obtained by sampling ε with probability p and sampling η with probability $1 - p$. Let (ε_j), (η_j), $j \geq 1$, be independent identically distributed sequences with the distributions of ε and η respectively. Independently, couple each ξ_j to (ε_j, η_j)

as the above mixture. Let T be the random set of indices $1 \le j \le N$ in which we sampled ε_j to obtain ξ_j. Thus $|T|$ is distributed as a binomial with N trials and success probability p. Using Theorem 3.1 we have

$$\begin{aligned}\max_{m\in\mathbb{Z}} \mathbb{P}\Big(\sum_{j=1}^{N} \xi_j a_j = m\Big) &= \max_{m\in\mathbb{Z}} \mathbb{E}\mathbb{P}\Big(\sum_{j=1}^{N} \xi_j a_j = m \,\Big|\, T, (\xi_j)_{j\notin T}\Big)\\ &\le \mathbb{E} \max_{m\in\mathbb{Z}} \mathbb{P}\Big(\sum_{j\in T} \xi_j a_j = m \,\Big|\, T\Big)\\ &= \mathbb{E} \max_{m\in\mathbb{Z}} \mathbb{P}\Big(\sum_{j\in T} \varepsilon_j a_j = m \,\Big|\, T\Big) \le \mathbb{E}\Big(\min\Big(1, \frac{C}{|T|^{3/2}}\Big)\Big).\end{aligned}$$

It remains to note that by standard concentration estimates for binomial random variables there exists some universal constant $c > 0$ for which

$$\mathbb{P}\Big(|T| \le \frac{1}{2}Np\Big) \le \exp(-cNp).$$

Thus

$$\mathbb{E}\Big(\min\Big(1, \frac{C}{|T|^{3/2}}\Big)\Big) \le \exp(-cNp) + \frac{C}{(\frac{1}{2}Np)^{3/2}}. \qquad \blacksquare$$

We complete now the proof of Lemma 1.4. Let α be such that $\alpha^k = 1$ for some $k \ge 1$. Observe that necessarily $\deg(\alpha) \le k$. Set

$$\begin{aligned} J &:= \{j \colon 1 \le j \le n \text{ and } 0 \le (j-1) \bmod k \le \deg(\alpha) - 1\},\\ \bar{J} &:= \{1, \dots, n\} \setminus J.\end{aligned}$$

Define the random variables (S_r), $0 \le r \le \deg(\alpha) - 1$, by

$$S_r := \sum_{\substack{j\in J\\ j-1 \bmod k = r}} \xi_j j \alpha^{j-1} = \alpha^r \sum_{\substack{j\in J\\ j-1 \bmod k = r}} \xi_j j$$

and

$$\bar{S} := \sum_{j\in\bar{J}} \xi_j j \alpha^{j-1}.$$

Observe that

$$P'(\alpha) = \sum_{j=1}^{n} \xi_j j \alpha^{j-1} = \sum_{j\in J} \xi_j j \alpha^{j-1} + \sum_{j\in\bar{J}} \xi_j j \alpha^{j-1} = \sum_{r=0}^{\deg(\alpha)-1} S_r + \bar{S}.$$

Now, by definition, (S_r), $0 \le r \le \deg(\alpha) - 1$, are independent and also independent of $\bar{S}$. In addition, (α^r), $0 \le r \le \deg(\alpha) - 1$, are linearly independent over the rational numbers, and therefore the equation $\sum_{i=0}^{\deg(\alpha)-1} a_i\alpha^i = z$ has at most one integral solution $(a_0, \ldots, a_{\deg(\alpha)-1})$ for a given $z \in \mathbb{C}$. Hence

$$\begin{aligned}\mathbb{P}(P'(\alpha) = 0) =&\mathbb{E}\mathbb{P}\Big(\sum_{r=0}^{\deg(\alpha)-1} S_r = -\bar{S}\,\Big|\,\bar{S}\Big)\\ \le&\max_{z\in\mathbb{C}}\mathbb{P}\Big(\sum_{r=0}^{\deg(\alpha)-1} S_r = z\Big)\\ =&\prod_{r=0}^{\deg(\alpha)-1}\max_{z\in\mathbb{C}}\mathbb{P}(S_r = z)\\ =&\prod_{r=0}^{\deg(\alpha)-1}\max_{m\in\mathbb{Z}}\mathbb{P}\Big(\sum_{\substack{j\in J\\ j-1 \bmod k=r}} \xi_j j = m\Big).\end{aligned}$$

Applying Corollary 3.2 and the fact that $|J| \ge \lfloor n/k\rfloor$ we conclude that

$$\mathbb{P}(P'(\alpha) = 0) \le \Big(\frac{C}{\lfloor\frac{n}{k}\rfloor}\Big)^{\frac{3\deg(\alpha)}{2}}.$$

4. Roots off the unit circle

In this section we prove Lemma 1.5. Let $\alpha \neq 0$ be an algebraic integer. We assume $|\alpha| \neq 1$ as otherwise the lemma is trivial. We note also that the probability that α is a root of P is the same as the probability that $1/\alpha$ is a root of P since $P(\alpha)$ has the same distribution as $\alpha^n P(1/\alpha)$. Thus we assume without loss of generality that $|\alpha| > 1$. Define j_0 as the minimal positive integer for which

$$|\alpha|^{j_0} \ge 3. \tag{11}$$

Write $P(z) = P_1(z) + P_2(z)$ with

$$P_1(z) := \sum_{k=0}^{\lfloor n/j_0\rfloor} \xi_{kj_0} z^{kj_0} \quad \text{and} \quad P_2(z) := P(z) - P_1(z).$$

The assumption (11) implies that the mapping $T : \{-1, 0, 1\}^{\lfloor n/j_0\rfloor+1} \to \mathbb{C}$ defined by

$$(a_0, \ldots, a_{\lfloor n/j_0\rfloor}) \mapsto \sum_{k=0}^{\lfloor n/j_0\rfloor} a_k\alpha^{kj_0}$$

is one-to-one (similarly to (9)). Thus, as $P_1(\alpha)$ and $P_2(\alpha)$ are independent,

$$\begin{aligned}\mathbb{P}(\alpha \text{ is a root of } P) &= \mathbb{E}[\mathbb{P}(\alpha \text{ is a root of } P \mid P_2(\alpha))] \\ &= \mathbb{E}[\mathbb{P}(P_1(\alpha) = -P_2(\alpha) \mid P_2(\alpha))] \\ &\leq \Big(\max_{x \in \{-1,0,1\}} \mathbb{P}(\xi_0 = x) \Big)^{\lfloor n/j_0 \rfloor + 1}.\end{aligned}$$

Finally, assumption (1) and the definition of j_0 imply that

$$\mathbb{P}(\alpha \text{ is a root of } P) < \Big(\frac{1}{\sqrt{3}}\Big)^{\lfloor n/j_0 \rfloor + 1} \leq e^{-\frac{n \log 3}{2 j_0}} = e^{-\frac{n \log 3}{2 \lceil \log 3 / \log |\alpha| \rceil}}.$$

5. Probability of double root

In this section we prove Theorem 1.1.

By definition, any root of a monic polynomial with integer coefficients is an algebraic integer. Thus, unless all coefficients of P are zero, the equation $P(z) = 0$ is satisfied only by algebraic integers z. We note this explicitly for later reference,

$$\mathbb{P}(P \text{ has a root which is not an algebraic integer}) = \mathbb{P}(\xi_0 = 0)^{n+1} < 3^{-n/2} \tag{12}$$

by assumption (1).

Let c be the constant appearing in Lemma 1.3 and note first that this lemma implies that

$$\mathbb{P}\Big(P \text{ has a double root } \alpha \text{ with } \deg(\alpha) \geq \frac{3 \log n}{c}\Big) \leq C n^{-3}. \tag{13}$$

Thus we may restrict attention to the following set of potential roots,

$$A := \Big\{\alpha \in \mathbb{C} \colon \alpha \text{ is a root of a monic polynomial} \\ \text{with coefficients in } \{-1,0,1\} \text{ and } \deg(\alpha) < \frac{3 \log n}{c}\Big\}.$$

We now use use another argument of Filaseta and Konyagin [FK96] to bound the cardinality of A.

Lemma 5.1: *There exists a constant $C > 0$ such that*

$$|A| \leq C^{(\log n)^2}.$$

Proof. Let $\alpha \in A$ and denote by $C(\alpha)$ the set of its algebraic conjugates (including α itself). Since α is a root of a monic polynomial with coefficients in $\{-1,0,1\}$ it follows immediately that

$$|\beta| < 2 \quad \text{for each } \beta \in C(\alpha). \tag{14}$$

Now suppose $\deg(\alpha) = d$, let g be the minimal polynomial of α and denote

$$g(z) = z^d + \sum_{j=0}^{d-1} a_j z^j = \prod_{\beta \in C(\alpha)} (z - \beta).$$

From this representation and (14) we deduce that $|a_j| \le 4^d$ for each j, whence the integral vector $(a_0, \ldots, a_{d-1})$ has at most 4^{d^2} possibilities. We conclude that the number of $\alpha \in A$ with $\deg(\alpha) = d$ is at most 4^{d^2} and the lemma follows by summing over d. ∎

We continue by recalling the Mahler measure of an algebraic integer. If α is an algebraic integer having minimal polynomial

$$g(z) = \prod_{\beta \in C(\alpha)} (z - \beta),$$

where $C(\alpha)$ is the set of algebraic conjugates of α, then the Mahler measure $M(\alpha)$ of α is

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

In particular, if α is an algebraic integer then $M(\alpha) = 1$ if and only if $\alpha = 0$ or $|\beta| = 1$ for all $\beta \in C(\alpha)$. Moreover, it follows from a classical theorem of Kronecker [K57] that if α is an algebraic integer with $|\beta| = 1$ for all $\beta \in C(\alpha)$ then α is a root of unity. Finally, Lehmer's conjecture [L33] states that there exists some absolute constant $\mu > 1$ such that

$$M(\alpha) = 1 \text{ or } M(\alpha) \ge \mu \quad \text{for all algebraic integers } \alpha.$$

We will make use of Dobrowolski's result on Lehmer's conjecture [D79] which says that

$$M(\alpha) = 1 \text{ or } \log(M(\alpha)) \ge c' \Big(\frac{\log\log(\deg(\alpha) + 2)}{\log(\deg(\alpha) + 2)} \Big)^3$$
$$\text{for some } c' > 0 \text{ and all algebraic integers } \alpha.$$

We remark that earlier weaker results on Lehmer's conjecture such as those of Blanksby and Montgomery [BM71] or Stewart [S78] would also have sufficed for our purposes.

Now let $\alpha \in A$ and denote $d := \deg(\alpha)$. Assume that α is neither 0 nor a root of unity. It follows from the preceding discussion that

$$\log(M(\alpha)) \geq c'\Big(\frac{\log\log(d+2)}{\log(d+2)}\Big)^3$$

and hence, using that $e^x \geq 1 + x$ for $x \geq 0$, one concludes that α has some algebraic conjugate β satisfying

$$|\beta| \geq 1 + \frac{c'}{d}\Big(\frac{\log\log(d+2)}{\log(d+2)}\Big)^3.$$

Since $P(\alpha) = 0$ if and only if $P(\beta) = 0$ we may apply Lemma 1.5 to deduce that

$$\mathbb{P}(\alpha \text{ is a root of } P) \leq e^{-\frac{n\log 3}{2\lceil \log 3/\log|\beta|\rceil}} \leq e^{-c''\frac{n(\log\log(d+2))^3}{d(\log(d+2))^3}}$$

for some $c'' > 0$. Putting this estimate together with Lemma 5.1 and the fact that $\deg(\alpha) < \frac{3\log n}{c}$ for $\alpha \in A$ yields that

$$\begin{aligned}(15)\qquad &\mathbb{P}(P \text{ has a root } \alpha \in A \text{ with } \alpha \neq 0 \text{ and } \alpha \text{ not a root of unity}) \\ &\qquad\qquad \leq C^{(\log n)^2} e^{-c'''\frac{n(\log\log\log n)^3}{\log n(\log\log n)^3}}\end{aligned}$$

for some $c''' > 0$. It remains to consider the probability that P has a root which is a root of unity. Let α be a root of unity with k being the minimal positive integer for which $\alpha^k = 1$ and $d := \deg(\alpha)$. By Lemma 1.4,

$$(16)\qquad \mathbb{P}(\alpha \text{ is a double root of } P) \leq \Big(\frac{C}{\lfloor \frac{n}{k} \rfloor}\Big)^{\frac{3d}{2}}.$$

Since the minimal polynomial of α is given by the kth cyclotomic polynomial

$$\Phi_k(x) := \prod_{\substack{1\leq j\leq k,\\ \gcd(j,k)=1}} (1 - e^{2\pi i j/k})$$

(see, for example, Lemma 7.6 and Theorem 7.7 of [M96]), we have that $d = \deg(\Phi_k) = \varphi(k)$ where φ is Euler's totient function, i.e.,

$$\varphi(k) = |\{1 \leq j \leq k\colon\ \gcd(j,k) = 1\}|.$$

By standard estimates (see [MV07, Theorem 2.9]) there exists some constant $c_1 > 0$ for which

$$d = \varphi(k) \geq \frac{c_1 k}{\log\log(k+2)}.$$

Thus if $\alpha \in A$, so that in particular $\deg(\alpha) < \frac{3\log n}{c}$, then

$$k \leq C_1 \log n \log\log\log n \tag{17}$$

for some $C_1 > 0$. Substituting back in (16) yields

$$\mathbb{P}(\alpha \text{ is a double root of } P) \leq \Big(\frac{C_2 \log n \log\log\log n}{n}\Big)^{\frac{3d}{2}}$$

for some $C_2 > 0$. In particular, since there are at most k numbers α for which k is the minimal positive integer such that $\alpha^k = 1$, we conclude from the last two inequalities that

$$\begin{aligned}&\mathbb{P}(P \text{ has a double root } \alpha \in A \setminus \{-1,1\} \text{ which is a root of unity})\\ &\qquad\leq (C_1 \log n \log\log\log n)^2 \Big(\frac{C_2 \log n \log\log\log n}{n}\Big)^3 = o(n^{-2}).\end{aligned} \tag{18}$$

Theorem 1.1 now follows by putting together (12), (13), (15) and (18).

6. Asymptotics of the double root probability

In this section we find asymptotics in many cases for the probability that the random polynomial P has a double root, proving Theorem 1.2.

We start with the proof of (3). By Theorem 1.1 we may focus on the probability that either $-1, 0$ or 1 are double roots of P. We have

$$\mathbb{P}(0 \text{ is a double root of } P) = \mathbb{P}(\xi_0 = 0)^2 \tag{19}$$

since 0 is a double root of P if and only if the free coefficients of P and P' vanish. Thus, (3) follows by noting that the probability that either -1 or 1 are double roots of P tends to zero with n by Lemma 1.4.

In the rest of the section we assume (4) and proceed to prove (5). By Theorem 1.1 it suffices to find the asymptotics of the probability that either -1 or 1 are double roots of P.

We start with some simple observations. Note that

$$\begin{aligned} P(1) &\equiv P(-1) \equiv n+1 \bmod 2,\\ P'(1) &\equiv P'(-1) \equiv \Big\lceil \frac{n}{2} \Big\rceil \bmod 2.\end{aligned} \tag{20}$$

Thus,

$$\mathbb{P}(-1 \text{ or } 1 \text{ are double roots of } P) = 0 \quad \text{if } n+1 \text{ is not divisible by 4.} \tag{21}$$

Together with Theorem 1.1 this establishes the case $L_n = 0$ in (5) and (6). We henceforth make the assumption that

$$n+1 \text{ is divisible by 4.} \tag{22}$$

Next we note that $P(1) = 0$ if and only if exactly half of the $(\xi_j)_{0\le j\le n}$ are 1. Thus, by standard large deviation estimates for binomial random variables,

$$\text{if } \mathbb{E}(\xi_0) \neq 0 \text{ then } \mathbb{P}(P(1) = 0) \le C\exp(-cn) \tag{23}$$

for some constants $C, c > 0$. Additionally, it is straightforward to check that

$$\text{if } \mathbb{E}(\xi_0) = 0 \text{ then } (P(1), P'(1)) \overset{d}{=} (P(-1), P'(-1)). \tag{24}$$

Lastly, since we have the equality of events

$$\{P'(1) = P'(-1) = 0\} = \left\{ \sum_{k=1}^{\lceil \frac{n}{2} \rceil} (2k-1)\xi_{2k-1} = \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} 2k\xi_{2k} = 0 \right\},$$

it follows from Corollary 3.2 that

$$\begin{aligned} \mathbb{P}(P'(1) =& P'(-1) = 0) \\ =& \mathbb{P}\Bigg(\sum_{k=1}^{\lceil \frac{n}{2} \rceil} (2k-1)\xi_{2k-1} = 0 \Bigg) \mathbb{P}\Bigg(\sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} 2k\xi_{2k} = 0 \Bigg) \le \frac{C}{n^3} \end{aligned} \tag{25}$$

for some constant $C > 0$. Putting together Theorem 1.1, (23), (24) and (25) we see that the remaining parts of Theorem 1.2 will follow by showing that

$$\left| \mathbb{P}(-1 \text{ is a double root of } P) - \frac{4\sqrt{3}}{\pi \operatorname{Var}(\xi_0) n^2} \right| = o(n^{-2}). \tag{26}$$

These asymptotics will be established via a local central limit theorem. We rely on some ideas from [KLP13], but aim to give a short proof tailored for our case rather than a general statement.

We wish to compare the probability distribution of $(P(-1), P'(-1))$ to the density of a Gaussian random vector with the same expectation and covariance matrix. To this end we denote

$$X := (P(-1), P'(-1)) = \Bigg(\sum_{j=0}^{n} \xi_j (-1)^j, \sum_{j=0}^{n} j\xi_j (-1)^{j-1} \Bigg) = \sum_{j=0}^{n} (1, -j)\xi_j (-1)^j. \tag{27}$$

A short calculation, using our standing assumption (22), yields the expectation μ and covariance matrix Σ of X,

$$\begin{aligned}\mu &= \left(0, \frac{n+1}{2}\mathbb{E}(\xi_0)\right),\\ \Sigma &= \begin{pmatrix} \mathrm{Var}(\xi_0)(n+1) & -\frac{\mathrm{Var}(\xi_0)}{2}n(n+1) \\ -\frac{\mathrm{Var}(\xi_0)}{2}n(n+1) & \frac{\mathrm{Var}(\xi_0)}{6}n(n+1)(2n+1)\end{pmatrix}.\end{aligned} \tag{28}$$

We also let Y denote a Gaussian random vector in $\mathbb{R}^2$ having expectation μ and covariance matrix Σ. By standard facts regarding Gaussian random vectors, the characteristic function $\hat{Y} : \mathbb{R}^2 \to \mathbb{C}$ of Y is

$$\hat{Y}(\theta) = \mathbb{E}e^{2\pi i\langle\theta,Y\rangle} = e^{2\pi i\langle\theta,\mu\rangle - 2\pi^2\theta^t\Sigma\theta} \tag{29}$$

and the density $f_Y : \mathbb{R}^2 \to \mathbb{R}$ of Y is

$$f_Y(y) = \frac{1}{2\pi\sqrt{\det(\Sigma)}}e^{-\frac{1}{2}(y-\mu)^t\Sigma^{-1}(y-\mu)} = \int_{\mathbb{R}^2} e^{-2\pi i\langle\theta,y\rangle}\hat{Y}(\theta)d\theta. \tag{30}$$

The characteristic function $\hat{X} : \mathbb{R}^2 \to \mathbb{C}$ of X is also simple to calculate, as X is given in (27) as a sum of independent random vectors,

$$\begin{aligned}\hat{X}(\theta) =& \mathbb{E}e^{2\pi i\langle\theta,X\rangle}\\ =& \prod_{j=0}^{n}(pe^{2\pi i((-1)^j\theta_1 + j(-1)^{j-1}\theta_2)} + (1-p)e^{-2\pi i((-1)^j\theta_1 + j(-1)^{j-1}\theta_2)}).\end{aligned} \tag{31}$$

where we denote $\theta = (\theta_1, \theta_2)$ and let

$$p := \mathbb{P}(\xi_0 = 1).$$

In addition, we note that by the parity restrictions (20) the values of X lie in the lattice $2\mathbb{Z}^2$ (again, using our standing assumption (22)). Therefore we have the representation

$$\mathbb{P}(-1 \text{ is a double root of } P) = \mathbb{P}(X = (0,0)) = 4\int_{[-\frac{1}{4},\frac{1}{4}]^2}\hat{X}(\theta)d\theta. \tag{32}$$

The following proposition relates $\hat{X}$ to $\hat{Y}$ near zero and shows that both are small away from zero.

Proposition 6.1: *Denote*

$$D := [-n^{-5/12}, n^{-5/12}] \times [-n^{-17/12}, n^{-17/12}].$$

There exists an absolute constant $C > 0$ and constants $C_p, c_p > 0$ depending only on p such that:

1. *For every $\theta \in D$ we have $|\hat{X}(\theta) - \hat{Y}(\theta)| \le Cn^{-1/4}$.*
2. *For every $\theta \in [-1/4, 1/4]^2 \setminus D$ we have $|\hat{X}(\theta)| \le C\exp(-c_p n^{1/6})$.*
3. *$\int_{\mathbb{R}^2 \setminus D} |\hat{Y}(\theta)| d\theta \le C_p \exp(-c_p n^{1/6})$.*

Proof. We start with the proof of part 1. Define a function $f : \mathbb{R} \to \mathbb{C}$ by

$$f(x) := pe^{ix} + (1-p)e^{-ix}.$$

A simple calculation using the Taylor expansion of the logarithm (see [KLP13, Claim 4.10] for a similar claim) shows that for $0 \le p \le 1$ and $|x| \le \frac{\pi}{4}$ we have

$$f(x) = e^{(2p-1)ix - 2p(1-p)x^2 + \delta(p,x)}$$

where $|\delta(p,x)| \le C'|x|^3$ for some absolute constant $C' > 0$. Plugging this into (31) for $\theta \in D$ yields

$$\begin{aligned}\hat{X}(\theta) =& \exp\Bigg(2\pi(2p-1)i\sum_{j=0}^{n}((-1)^j\theta_1 + j(-1)^{j-1}\theta_2) \\ &\qquad - 8\pi^2 p(1-p)\sum_{j=0}^{n}((-1)^j\theta_1 + j(-1)^{j-1}\theta_2)^2 + \delta'\Bigg) \\ =& \exp(2\pi i\langle\theta,\mu\rangle - 2\pi^2\theta^t\Sigma\theta + \delta') = \hat{Y}(\theta)e^{\delta'},\end{aligned}$$

where the error term $\delta' = \sum_{j=0}^{n} \delta(p, 2\pi((-1)^j\theta_1 + j(-1)^{j-1}\theta_2))$ satisfies

$$|\delta'| \le C''\sum_{j=0}^{n} |(-1)^j\theta_1 + j(-1)^{j-1}\theta_2|^3 \le C'''n^{-1/4}$$

and $C'', C''' > 0$ denote absolute constants. This finishes the proof of part 1.

We now continue with the proof of part 3. It is useful to proceed by finding a diagonal matrix which Σ dominates. Since, for all $(\theta_1, \theta_2) \in \mathbb{R}^2$,

$$n\theta_1\theta_2 = \Big(\frac{\sqrt{7}}{2}\theta_1\Big)\Big(\frac{2n}{\sqrt{7}}\theta_2\Big) \le \frac{1}{2}\Big(\frac{7}{4}\theta_1^2 + \frac{4n^2}{7}\theta_2^2\Big) \le \frac{7}{8}\theta_1^2 + \frac{1}{7}n(2n+1)\theta_2^2,$$

we conclude that

$$\begin{aligned}\theta^t\Sigma\theta =& \mathrm{Var}(\xi_0)(n+1)\Big(\theta_1^2 + \frac{1}{6}n(2n+1)\theta_2^2 - n\theta_1\theta_2\Big) \\ \ge& \mathrm{Var}(\xi_0)(n+1)\Big(\frac{1}{8}\theta_1^2 + \frac{n(2n+1)}{42}\theta_2^2\Big).\end{aligned}$$

Thus, by (29), we have

$$\begin{aligned}\int_{\mathbb{R}^2\setminus D}|\hat{Y}(\theta)|d\theta &= \int_{\mathbb{R}^2\setminus D} e^{-2\pi^2\theta^t\Sigma\theta}d\theta\\ &\le \int_{\mathbb{R}^2\setminus D} e^{-2\pi^2\operatorname{Var}(\xi_0)(n+1)(\frac{1}{8}\theta_1^2+\frac{n(2n+1)}{42}\theta_2^2)}d\theta.\end{aligned}$$

Now, letting G_1, G_2 be independent centered normal random variables with $\operatorname{Var}(G_1) = \sigma_1^2 := \frac{2}{\pi^2\operatorname{Var}(\xi_0)(n+1)}$ and $\operatorname{Var}(G_2) = \sigma_2^2 := \frac{21}{2\pi^2\operatorname{Var}(\xi_0)n(n+1)(2n+1)}$ we have that

$$\begin{aligned}\int_{\mathbb{R}^2\setminus D}|\hat{Y}(\theta)|d\theta \le& 2\pi\sigma_1\sigma_2\mathbb{P}((G_1,G_2)\notin D)\\ \le& 2\pi\sigma_1\sigma_2(\mathbb{P}(|G_1|>n^{-5/12})+\mathbb{P}(|G_2|>n^{-17/12}))\\ \le& \frac{C}{\operatorname{Var}(\xi_0)^2}e^{-c\operatorname{Var}(\xi_0)n^{1/6}}\end{aligned}$$

for some absolute constants $C, c > 0$. This finishes the proof of part 3.

Finally we turn to part 2. By taking the constant C sufficiently large we may assume that n is large. Fix $\theta \in [-\frac{1}{4}, \frac{1}{4}]^2$. Write

$$x_j := 2((-1)^j\theta_1 + j(-1)^{j-1}\theta_2), \quad 0 \le j \le n.$$

For a real number x, denote by $d(x, \mathbb{Z})$ its distance to the nearest integer. Let

$$J = J(\theta) := \Big\{0 \le j \le n\colon d(x_j, \mathbb{Z}) \le \frac{1}{8}n^{-5/12}\Big\}.$$

Using (31), if $|J| \le 9(n+1)/10$ then

$$\begin{aligned}|\hat{X}(\theta)| =& \prod_{j=0}^{n}|pe^{2\pi i x_j}+(1-p)| = \prod_{j=0}^{n}\sqrt{1-2p(1-p)(1-\cos(2\pi x_j))}\\ \le& \Big(1-2p(1-p)\Big(1-\cos\Big(\frac{\pi}{4}n^{-5/12}\Big)\Big)\Big)^{\frac{n+1-|J|}{2}}\\ \le& (1-20c_pn^{-5/6})^{\frac{n+1}{20}} \le \exp(-c_pn^{1/6})\end{aligned}$$

for some constant $c_p > 0$ depending only on p. Hence it suffices to show that if

$$|J| \ge 9(n+1)/10 \tag{33}$$

then $\theta \in D$.

Assume (33). We claim that there necessarily exist j_1, j_2 such that j_1, j_2, $j_1 + j_2 \in J$. Indeed, we may take $j_1 := \min J \le \frac{n+1}{10}$ and we then have

$J \cap (j_1 + J) \neq \emptyset$ by (33) and the pigeonhole principle since both J and $j_1 + J$ are contained in $[0, \frac{n+1}{10} + n]$. Thus,

$$\begin{aligned} d(2\theta_1, \mathbb{Z}) &= d((-1)^{j_1+j_2-1} x_{j_1+j_2} + (-1)^{j_1} x_{j_1} + (-1)^{j_2} x_{j_2}), \mathbb{Z}) \\ &\leq d(x_{j_1+j_2}, \mathbb{Z}) + d(x_{j_1}, \mathbb{Z}) + d(x_{j_2}, \mathbb{Z}) \leq \frac{3}{8} n^{-5/12}, \end{aligned} \tag{34}$$

whence, as $|\theta_1| \leq \frac{1}{4}$,

$$|\theta_1| = \frac{1}{2} d(2\theta_1, \mathbb{Z}) \leq \frac{3}{16} n^{-5/12}.$$

Now, if $|\theta_2| \leq n^{-17/12}$ then $\theta \in D$ and we are done. Assume, in order to obtain a contradiction, that $|\theta_2| > n^{-17/12}$.

Let $I := \{0 \leq j \leq n \colon d(2j\theta_2, \mathbb{Z}) > \frac{1}{2} n^{-5/12}\}$. We claim that $|I| \geq n/3$. To see this let k be the minimal positive integer for which $2k|\theta_2| > n^{-5/12}$. Since $|\theta_2| \leq 1/4$ it follows that $2k|\theta_2| \leq 1/2$. Thus, if $j \notin I$ and $j \leq n - k$ then necessarily $j + k \in I$. In addition, $k \leq \frac{1}{2n^{5/12}|\theta_2|} + 1 < n/2 + 1$. In particular, $|I| \geq k$ which shows the claim when $k \geq n/3$. Otherwise, assume $k < n/3$ and define

$$T := \{j \in [0, n-k] \cap \mathbb{Z} : \lfloor j/k \rfloor \text{ is even}\}.$$

We have that T and $T + k$ are disjoint subsets of $\{0, \ldots, n\}$ and for each $j \in T$, either j or $j + k$ belong to I. Hence $|I| \geq |T| \geq (n - k + 1)/2 > n/3$, as claimed.

Now the assumption (33) and the above claim imply that there exists some $j_3 \in J$ for which $d(2j_3\theta_2, \mathbb{Z}) > \frac{1}{2} n^{-5/12}$, whence by (34), $d(x_{j_3}, \mathbb{Z}) > \frac{1}{8} n^{-5/12}$, contradicting the fact that $j_3 \in J$. ∎

The asymptotics (26) are an immediate consequence of Proposition 6.1. Indeed, by (30) and (32), and the proposition,

$$\begin{aligned} &|\mathbb{P}(-1 \text{ is a double root of } P) - 4 f_Y((0,0))| \\ &\quad = 4 \left| \int_{[-\frac{1}{4}, \frac{1}{4}]^2} \hat{X}(\theta) d\theta - \int_{\mathbb{R}^2} \hat{Y}(\theta) d\theta \right| \\ &\quad \leq 4 \left(\int_D |\hat{X}(\theta) - \hat{Y}(\theta)| d\theta + \int_{[-\frac{1}{4}, \frac{1}{4}]^2 \setminus D} |\hat{X}(\theta)| d\theta + \int_{\mathbb{R}^2 \setminus D} |\hat{Y}(\theta)| d\theta \right) \\ &\quad \leq 4 C n^{-1/4} \operatorname{Area}(D) + C \exp(-c_p n^{1/6}) + \frac{4C}{\operatorname{Var}(\xi_0)^2} e^{-c \operatorname{Var}(\xi_0) n^{1/6}} = o(n^{-2}). \end{aligned}$$

In addition, by (30) and (28) we have

$$\begin{aligned} f_Y((0,0)) &= \frac{1}{2\pi\sqrt{\det(\Sigma)}} e^{-\frac{1}{2}\mu^t\Sigma^{-1}\mu} \\ &= \frac{\sqrt{12}}{2\pi \operatorname{Var}(\xi_0)(n+1)\sqrt{n(n+2)}} e^{-\frac{3(n+1)^2}{2n(n^2+3n+2)}} \\ &= \frac{\sqrt{3}}{4\pi p(1-p)n^2} + o(n^{-2}). \end{aligned}$$

This finishes the proof of (26) and completes the proof of Theorem 1.2. ∎

7. Open questions

We conclude the paper by listing several open questions.

(1) As mentioned in the introduction, we do not know if the assumption (1) or any similar condition is necessary for Theorem 1.1 to hold. Recall that the assumption enters into the proof mainly through Claim 2.2 which, in turn, is used to obtain the crucial Lemma 1.3.

Remark: Mei-Chu Chang [Ch14] has kindly pointed out to the authors that for Claim 2.2 to hold, in Assumption (1) the constant $1/\sqrt{3} = 0.5774\ldots$ can be replaced by the supremum of ρs so that there exists $q \in (1,\infty)$ such that $3^{(q-1)/2q} < \rho^q + (1-\rho)^q$, leading to the value $0.7615\ldots$. This still leaves open the question of whether any assumption of the type (1) is needed for Theorem 1.1 to hold.

(2) It is natural to try and extend Theorem 1.1 to more general coefficient distributions. This would require a non-trivial modification of our approach as we relied in several places on the fact that the potential roots of our random polynomial are algebraic integers rather than the more general algebraic numbers. A significant issue is to deal with potential roots of high degree, providing an analogue of Lemma 1.3.

Remark added during galley proofs: This question is partially answered in the subsequent work [FS16]. The latter deals with a general coefficient distribution on the integers that has bounded support with maximum atom at most 1/2.

(3) The following question does not involve any probability. Are there examples of Littlewood polynomials with at least one non-cyclotomic double root? The same question had been asked by Odlyzko and Poonen [OP93] for polynomials with 0/1 coefficients with the constant term equal to one. That question was later answered by Mossinghoff [M03] who found examples of several such polynomials with non-cyclotomic repeated roots.

(4) Another interesting question is to bound the probability that a random Littlewood polynomial is reducible. This is somewhat related to our original question regarding double roots—note that the probability of having a double root is dominated by the probability of being reducible. But handling irreducibility seems to be much harder. To the best of our knowledge, it is open whether this probability goes to zero as n increases. On the related question of estimating the probability that a uniformly picked polynomial of degree d with $0, 1$ coefficients is reducible it seems that the state-of-the-art is the result of Konyagin [KO99] who proves that the probability that the polynomial has a factor of degree at most $cd/\log(d)$ is at most $C/\sqrt{d}$. See the thread [MO09] for some partial results on this question.

References

[A78] L. V. Ahlfors, *Complex Analysis*, third edition, McGraw-Hill Book Co., New York, 1978.

[BM71] P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arithmetica **18** (1971), 355–369.

[Ch14] M.-C. Chang, private communication, October 27, 2014.

[D79] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arithmetica **34** (1979), 391–401.

[FS16] O. N. Feldheim and A. Sen, *Double roots of random polynomials with integer coefficients*, (2016), arXiv:1603.03811.

[FK96] M. Filaseta and S. Konyagin, *Squarefree values of polynomials all of whose coefficients are* 0 *and* 1, Acta Arithmetica **74** (1996), 191–205.

[FL99] G. Freiman and S. Litsyn, *Asymptotically exact bounds on the size of high-order spectral-null codes*, Institute of Electrical and Electronics Engineers. Transactions on Information Theory **45** (1999), 1798–1807.

[K57] L. Kronecker, *Zwei sätse über Gleichungen mit ganzzahligen Coefficienten*, Journal für die Reine und Angewandte Mathematik **53** (1857), 173–175. See also *Leopold Kronecker's Werke*, Vol. 1, Chelsea Publishing Co., New York, 1968, pp. 103–108.

[KLP13] G. Kuperberg, Sh. Lovett and R. Peled, *Probabilistic existence of regular combinatorial structures*, in *STOC '12—Proceedings of the 2012 ACM Symposium on Theory of Computing*, ACM, New York, 2012, pp. 1091–1106.

[KO99] S. V. Konyagin, *On the number of irreducible polynomials with* $0, 1$ *coefficients*, Acta Arithmetica **88** (1999), 333–350.

[KZ13] G. Kozma and O. Zeitouni, *On common roots of random Bernoulli polynomials*, International Mathematics Research Notices **18** (2013), 4334–4347.

[L33] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Annals of Mathematics **34** (1933), 461–479.

[M96] P. Morandi, *Field and Galois Theory*, Graduate Texts in Mathematics, Vol. 167, Springer-Verlag, New York, 1996.

[M03] M. J. Mossinghoff, *Polynomials with restricted coefficients and prescribed noncyclotomic factors*, LMS Journal of Computation and Mathematics **6** (2003), 314–325.

[MO09] Mathoverflow discussion, http://mathoverflow.net/questions/7969/irreducible-polynomials-with-constrained-coefficients.

[MV07] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory. I. Classical Theory*, Cambridge Studies in Advanced Mathematics, Vol. 97, Cambridge University Press, Cambridge, 2007.

[OP93] A. M. Odlyzko and B. Poonen, *Zeros of polynomials with* $0, 1$ *coefficients*, L'Enseignement Mathématique **39** (1993), 317–348.

[SS65] A. Sárközi and E. Szemerédi, *Über ein Problem von Erdős und Moser*, Acta Arithmetica **11** (1965), 205–208.

[S78] C. L. Stewart, *Algebraic integers whose conjugates lie near the unit circle*, Bulletin de la Société Mathématique de France **106** (1978), 169–176.

[SN86] N. R. Saxena and J. P. Robinson, *Accumulator compression testing*, IEEE Transactions on Computers **C-35** (1986), 317–321.