IRREDUCIBILITY OF LITTLEWOOD POLYNOMIALS OF SPECIAL DEGREES

LIOR BARY-SOROKER, DAVID HOKKEN, GADY KOZMA, AND BJORN POONEN

Abstract. Let f be sampled uniformly at random from the set of degree n polynomials whose coefficients lie in $\{\pm 1\}$. A folklore conjecture, known to hold under GRH, states that the probability that f is irreducible tends to 1 as n goes to infinity. We prove unconditionally that

$$\limsup_{n\to\infty} \mathbb{P}(f \text{ is irreducible}) = 1.$$

1. Introduction

Let $f(X) = \sum_{i=0}^{n} \pm X^i$ be a Littlewood polynomial of degree n sampled uniformly at random; that is, its coefficients are independent random variables taking the values ± 1 with probability $1/2$ each. A folklore conjecture [2, 3, 4, 6, 8, 9] asserts that

$$\lim_{n\to\infty} \mathbb{P}(f \text{ is irreducible}) = 1. \tag{1.1}$$

Breuillard and Varjú [4] proved that the Generalized Riemann Hypothesis implies (1.1). Together with Koukoulopoulos, the first and third authors [2, Theorem 3.5] proved unconditionally that

$$\liminf_{n\to\infty} \mathbb{P}(f \text{ is irreducible}) > 0.$$

The goal of this paper is to prove (1.1) unconditionally when restricting to a subsequence of degrees:

Theorem 1.1. *In the notation above,*

$$\limsup_{n\to\infty} \mathbb{P}(f \text{ is irreducible}) = 1.$$

If $n = p - 1$ for a prime p such that 2 generates $(\mathbf{Z}/p\mathbf{Z})^\times$, then f is always irreducible over $\mathbf{F}_2$, so $\mathbb{P}(f \text{ is irreducible}) = 1$ for such n. Unfortunately, the infinitude of such primes is the content of the Artin primitive root conjecture, which is open. However, similar in spirit to this observation is the following more precise result, which implies Theorem 1.1 immediately.

Theorem 1.2. *There exists an absolute constant $c > 0$ such that the following holds. Suppose that either $p = 2$, or $p \geqslant 7$ is a prime number such that 2 generates $(\mathbf{Z}/p^2\mathbf{Z})^\times$. Let $r \geqslant 1$ be an integer. Set $n = p^r - 1$. Then*

$$\mathbb{P}(f \text{ is irreducible}) \geqslant 1 - n^{-c}. \tag{1.2}$$

Remark 1.3. We may assume that f is monic, since f is irreducible if and only if $-f$ is.

Remark 1.4. For every $n \geqslant 1$, there exists at least one irreducible Littlewood polynomial (see, e.g., [7, Corollary 2.2]), so we may adjust c to make (1.2) hold for any finite list of positive integers n. Thus, in proving Theorem 1.2, we may assume that n is sufficiently large, and it does not matter if n^{-c} is replaced by $O(n^{-c})$.

Acknowledgements. We thank Gunther Cornelissen, Arno Fehm, Berend Ringeling, and Mieke Wessel for feedback on an earlier version of this paper. LBS was partially supported by the Israel Science Foundation grant no. 702/19. DH was supported by the Dutch Research Council (NWO), project number OCENW.M20.233. GK was partially supported by the Israel Science Foundation grant no. 607/21. BP was supported in part by National Science Foundation grant DMS-2101040 and Simons Foundation grants #402472 and #550033. DH thanks his hosts at Tel Aviv University for their hospitality and support during his visit in Spring 2023 that led to this project.

Date: December 26, 2023.

2020 *Mathematics Subject Classification.* 11R09.

Key words and phrases. Random polynomials, irreducibility, Littlewood polynomials.

2. Proof of Theorem 1.2 for $p = 2$

We assume that n is large and f is monic. We have $(X-1)f(X) \equiv X^{n+1} - 1 \equiv (X-1)^{n+1} \pmod 2$, since $n+1$ is a power of 2. Let $g(X) = f(X+1)$, so $g(X) = X^n + \sum_{i=0}^{n-1} g_i X^i$ for some $g_i \in 2\mathbf{Z}$. The maps $f \mapsto (f \bmod 4) \mapsto (g \bmod 4)$ are injective, so the composition defines a bijection from the set of 2^n monic Littlewood polynomials to the set of 2^n monic degree n polynomials in $(\mathbf{Z}/4\mathbf{Z})[X]$ reducing to X^n in $(\mathbf{Z}/2\mathbf{Z})[X]$. Thus the $(g_i \bmod 4)$ take the values 0 and 2 uniformly and independently. Fix θ as in [2, Corollary 1], with $\theta \in (0, 1/2)$. With high probability, there exists $i < \theta n$ with $g_i \equiv 2 \pmod 4$; choose the smallest such i. Then the 2-adic Newton polygon of g has a segment of width $n - i$ and height 1, so g has a $\mathbf{Q}_2$-irreducible factor of degree $\geqslant n - i$, and hence a $\mathbf{Q}$-irreducible factor of degree $\geqslant n - i$, and so does f; any other irreducible factor of f has degree $\leqslant i < \theta n$ (see for example [5, Section 7.4] for a discussion on Newton polygons). On the other hand, by [2, Corollary 1(a)], with probability $\geqslant 1 - n^{-c}$, the polynomial f has no irreducible factors of degree $< \theta n$, so then f is irreducible.

3. Proof of Theorem 1.2 for $p > 1470$

For any $f \in \mathbf{Z}[X]$ and prime p, let $f_p := (f \bmod p) \in \mathbf{F}_p[X]$. Define a probability measure μ on $\mathbf{Z}$ by $\mu(1) = \mu(-1) = 1/2$; it induces a probability measure on the set of polynomials of degree n with integer coefficients by sampling each coefficient independently according to μ. Write $e(x) := e^{2\pi i x}$, and define the Fourier transform $\hat{\mu}\colon \mathbf{R}/\mathbf{Z} \to \mathbf{C}$ by

$$\hat{\mu}(\alpha) := \sum_{k \in \mathbf{Z}} \mu(k) e(\alpha k) = \frac{e(\alpha) + e(-\alpha)}{2} = \cos(2\pi\alpha). \tag{3.1}$$

Proof of Theorem 1.2 for $p > 1470$. Let Φ_m denote the mth cyclotomic polynomial, viewed in $\mathbf{F}_2[X]$. By [1, Exercise 12, p. 99], for each $k \geqslant 1$, the element 2 generates $(\mathbf{Z}/p^k\mathbf{Z})^\times$, so the Frobenius automorphism acts transitively on the roots of Φ_{p^k} in $\overline{\mathbf{F}}_2$, so Φ_{p^k} is irreducible over $\mathbf{F}_2$.

We have

$$f_2 = X^n + X^{n-1} + \ldots + 1 = \Phi_p \Phi_{p^2} \cdot \ldots \cdot \Phi_{p^r} \in \mathbf{F}_2[X] \tag{3.2}$$

and by the above argument each of the cyclotomic polynomials on the right-hand side in (3.2) is irreducible. If f is reducible over $\mathbf{Q}$, then $f = gh$ for some monic $g, h \in \mathbf{Z}[X]$ of positive degrees. Then $f_2 = g_2 h_2$, so Φ_{p^r} divides one of the factors over $\mathbf{F}_2$, say g_2, and then

$$\deg h = \deg f - \deg g \leqslant \deg f - \deg \Phi_{p^r} = (p^r - 1) - (p^r - p^{r-1}) = p^{r-1} - 1 < n/p < n/1470. \tag{3.3}$$

On the other hand, we will use [2, Theorem 7] to prove that if n is sufficiently large, then

$$\mathbb{P}(f \text{ has a divisor of degree} \leqslant n/1470) \text{ is } O(n^{-c}). \tag{3.4}$$

For $\gamma = 1/2$, $P = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$, and $s = 735$, we verify numerically that for all integers Q, R, ℓ with $QR = P$ and $Q > 1$,

$$\sum_{k \in \mathbf{Z}/Q\mathbf{Z}} |\hat{\mu}(k/Q + \ell/R)|^s \leqslant 0.9999\, Q^{1-\gamma};$$

thus if n is sufficiently large and $\mu_j := \mu$ for $j = 0, \ldots, n-1$, then the conditions of [2, Theorem 7] are satisfied, so (3.4) holds. By (3.3) and (3.4), with probability at least $1 - O(n^{-c})$, we obtain a contradiction showing that f is irreducible. □

4. Approximate equidistribution and divisors modulo 3

The main difference between the proof of Theorem 1.2 for large primes in the previous section §3 and the one for $7 \leqslant p \leqslant 1470$ in §5 is that the black box [2, Theorem 7] in the former combines information on the factorization of f_3, f_5, f_7 and f_{11} to rule out *all* positive integers $\leqslant n/1470$ as possible degrees of divisors of f; in contrast, since the factorization of f_2 shows that already many such values cannot occur as degrees of a divisor, in §5 we require information on the factorization of f_3 only.

The aim of this section is to bound the probability that the degree n polynomial f_3 has a divisor of fixed degree k. For this, we require some further results of [2]. Define

$$\Delta_p(n;m) := \sum_{\substack{D\in\mathbf{F}_p[X],\, X\nmid D\\ \deg D\leqslant m}} \max_{C\in\mathbf{F}_p[X]} \left|\mathbb{P}(f_p \equiv C \bmod D) - p^{-\deg D}\right|.$$

The quantity Δ_p measures the extent to which f_p fails to be equidistributed modulo $D \in \mathbf{F}_p[X]$ on average for all D not divisible by X of degree at most m. We study it for $p = 3$. Set $\theta^* := \frac{\log 2}{2\log 3} \approx 0.315$.

Lemma 4.1. *Fix a positive real number $\theta < \theta^*$. Then, as $n \to \infty$,*

$$\Delta_3(n;\theta n) \ll e^{-n^{1/10}}.$$

Proof. Applying [2, Proposition 2.3] with $\mathscr{P} = \{3\}$, we have

$$\Delta_3(n;\gamma n/s + n^{0.88}) \ll e^{-n^{1/10}}$$

for any $\gamma \geqslant 1/2$, positive integer s, and sufficiently large n satisfying

$$|\hat{\mu}(0)|^s + |\hat{\mu}(1/3)|^s + |\hat{\mu}(2/3)|^s \leqslant (1 - n^{-1/10}) \cdot 3^{1-\gamma}. \tag{4.1}$$

Using (3.1), we find that (4.1) holds for any $\gamma < \gamma(s) := 1 - \frac{\log(1+2^{1-s})}{\log 3}$ and n sufficiently large (depending on γ). The smallest s such that $\gamma(s) > 1/2$ is $s = 2$, in which case we find $\gamma(s)/s = \theta^*$. □

Let $\tau(f_p)$ be the number of (not necessarily irreducible) monic divisors in $\mathbf{F}_p[X]$ of the polynomial f_p. Denote by $f_p^{\mathscr{S}(m)}$ the m-smooth part of f_p, defined as the product of all monic irreducible divisors in $\mathbf{F}_p[X]$ of f_p (with multiplicity) of degree $\leqslant m$.

Definition 4.2. Fix $\epsilon \in (0, 1/2)$ and a positive real number $\theta < \theta^*$. Let $n \in \mathbf{Z}_{\geqslant 1}$ and $k \in \mathbf{R}_{\geqslant 1}$. For a random Littlewood polynomial f of degree n, define the *bounded smoothness event* $\mathscr{E}_{k,\theta,\epsilon,n}$ as the event in which

$$\deg(f_3^{\mathscr{S}(m)}) \leqslant \epsilon m \log m \quad \text{and} \quad \tau(f_3^{\mathscr{S}(m)}) \leqslant m^{(1+\epsilon)\log 2}$$

holds for all integers $m \in [k, 2\theta n/\log n]$.

Lemma 4.3. *Fix $\epsilon \in (0, 1/2)$ and $\theta < \theta^*$. Then there exist $c, C, C' > 0$ such that for all sufficiently large n and all positive integers $k < \theta n$, we have*

(i) $\mathbb{P}(\mathscr{E}_{k,\theta,\epsilon,n}) > 1 - Ck^{-c}$, *and*

(ii) $\mathbb{P}(\mathscr{E}_{k^{1/4},\theta,\epsilon,n}$ *holds and f_3 has a divisor of degree k*) $< C' \dfrac{(\log n)^2}{k^{1-\log 2-2\epsilon}}$.

Proof.

(i) Apply Lemma 4.1 and [2, Lemma 9.3], where $m_0 = k$, $\mathscr{P} = \{3\}$, and θ and ϵ are as here.

(ii) We will use [2, Lemma 9.4]. In [2] there is an extra parameter, λ, which will not be important for us; we set $\lambda = 1 - \epsilon$. The condition $\Delta_3(n; \theta n + n^\lambda) \leqslant n^{-7}$ of [2, Lemma 9.4] follows by using Lemma 4.1 with $\theta_{\text{Lemma 4.1}} = \frac{1}{2}(\theta + \theta^*)$, if n is sufficiently large (depending on θ and ϵ). Further parameters of [2, Lemma 9.4] are $\delta = 1$ and again $\mathscr{P} = \{3\}$, and θ, ϵ, and k as here. The $\mathscr{E}_{k,\lambda,\epsilon,\theta}$ of [2] is a larger event than our $\mathscr{E}_{k^{1/4},\theta,\epsilon,n}$, since our $k^{1/4}$ is a lower bound for the m_0 in [2, Lemma 9.4]. Thus [2, Lemma 9.4] implies the desired bound, but with $k^{(1-\log 2-\epsilon)\lambda}$ in the denominator. This is stronger than needed, since $(1 - \log 2 - \epsilon)\lambda > 1 - \log 2 - 2\epsilon$. □

5. Proof of Theorem 1.2 for $7 \leqslant p \leqslant 1470$

Since 2 does not generate $(\mathbf{Z}/7^2\mathbf{Z})^\times$, we have $p \geqslant 11$. We fix p and assume throughout that n is sufficiently large. For $1 \leqslant k < n$, let E_k be the event that f has a degree k factor. For $I \subset \mathbf{R}$, let $E_I = \bigcup_{k\in I} E_k$. By the argument of §3, if f is reducible, it has a factor h such that h_2 is a subproduct of $\Phi_p\Phi_{p^2} \cdot \ldots \cdot \Phi_{p^{r-1}}$. For $j \leqslant r-2$, let D_j be the set of integers $k > n^{1/10}$ such that k is the degree of such a subproduct whose largest factor is $\Phi_{p^{j+1}}$. Then $\#D_j \leqslant 2^j$, and $D_j \subset [p^j, p^{j+1})$. Let s be the largest positive integer such that $p^s \leqslant n^{1/10}$. Then the event that f is reducible is contained in $E_{[1,n^{1/10}]} \cup \bigcup_{j=s}^{r-2} E_{D_j}$.

Let $\theta := 1/p < \frac{\log 2}{2\log 3} = \theta^*$. Let $\epsilon = 0.001$. We have $n^{1/40} < \theta n$ for large n; let $\mathscr{E} = \mathscr{E}_{n^{1/40},\theta,\epsilon,n}$ (see Definition 4.2). Let $\mathscr{E}^{\text{comp}}$ be the complementary event. Then

$$\mathbb{P}(f \text{ is reducible}) \leqslant \mathbb{P}(E_{[1,n^{1/10}]}) + \mathbb{P}(\mathscr{E}^{\text{comp}}) + \sum_{j=s}^{r-2} \sum_{k \in D_j} \mathbb{P}(\mathscr{E} \cap E_k). \tag{5.1}$$

By [2, Proposition 2.1], $\mathbb{P}(E_{[1,n^{1/10}]}) \ll n^{-7/20}$. By Lemma 4.3(i), $\mathbb{P}(\mathscr{E}^{\text{comp}}) \ll n^{-c'}$ for some $c' > 0$. For $n^{1/10} < k < \theta n$, we have $n^{1/40} < k^{1/4} < \theta n$; then $\mathscr{E} \subset \mathscr{E}_{k^{1/4},\theta,\epsilon,n}$, and E_k is contained in the event that f_3 has a degree k divisor, so

$$\begin{aligned}\mathbb{P}(\mathscr{E} \cap E_k) &\leqslant \mathbb{P}(\mathscr{E}_{k^{1/4},\theta,\epsilon,n} \text{ holds and } f_3 \text{ has a degree } k \text{ divisor}) \\ &\ll \frac{(\log n)^2}{k^{0.3}} \qquad \text{(by Lemma 4.3(ii), since } 1 - \log 2 - 2\epsilon \geqslant 0.3\text{);}\end{aligned}$$

$$\sum_{j=s}^{r-2} \sum_{k \in D_j} \mathbb{P}(\mathscr{E} \cap E_k) \ll \sum_{j=s}^{r-2} \# D_j \frac{(\log n)^2}{p^{0.3j}} \leqslant (\log n)^2 \sum_{j=s}^{r-2} \left(\frac{2}{p^{0.3}}\right)^j \ll (\log n)^2 p^{-0.01s} \ll n^{-c''}$$

for any positive $c'' < 0.001$, since $2/p^{0.3} \leqslant p^{-0.01}$ for $p \geqslant 11$, and $p^s \gg p^{s+1} \geqslant n^{1/10}$ since p was fixed. We have now bounded all three terms on the right of (5.1), so $\mathbb{P}(f \text{ is reducible}) \ll n^{-c}$ for some $c > 0$.

References

1. G. E. Andrews, *Number Theory*, Dover Publications, Inc., New York, 1971.
2. L. Bary-Soroker, D. Koukoulopoulos, and G. Kozma, *Irreducibility of random polynomials: general measures*, Invent. Math. **233** (2023), 1041–1120.
3. L. Bary-Soroker and G. Kozma, *Irreducible polynomials of bounded height*, Duke Math. J. **169** (2020), 579–598.
4. E. Breuillard and P. Varjú, *Irreducibility of random polynomials of large degree*, Acta Math. **223** (2019), 195–249.
5. F. Q. Gouvêa, *p-adic Numbers: An Introduction*, third edition, Universitext, Springer Nature, Cham, 2020.
6. S. V. Konyagin, *On the number of irreducible polynomials with* 0, 1 *coefficients*, Acta Arith. **88** (1999), 333–350.
7. P. A. Martin, *The Galois group of* $x^n - x^{n-1} - \cdots - x - 1$, J. Pure and Applied Algebra **190** (2004) 213–223.
8. A. Odlyzko and B. Poonen, *Zeros of polynomials with* 0, 1 *coefficients*, Enseign. Math. (2) **39** (1993), 317–348.
9. B. Poonen, *Answer to question "Irreducible polynomials with constrained coefficients"*. Question posted by user "some guy on the street" on Math Overflow, `https://mathoverflow.net/q/7969/`, 2009.

LBS: Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
Email address: `barylior@tauexe.tau.ac.il`

DH: Mathematical Institute, Utrecht University, 3508 TA Utrecht, The Netherlands
Email address: `d.p.t.hokken@uu.nl`

GK: Department of Mathematics, The Weizmann Institute of Science, Rehovot 76100, Israel
Email address: `gady.kozma@weizmann.ac.il`

BP: Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
Email address: `poonen@math.mit.edu`