ON THE NUMBER OF REAL ROOTS OF RANDOM POLYNOMIALS

HOI NGUYEN, OANH NGUYEN, AND VAN VU

ABSTRACT. Roots of random polynomials have been studied exclusively in both analysis and probability for a long time. A famous result by Ibragimov and Maslova, generalizing earlier fundamental works of Kac and Erdős-Offord, showed that the expectation of the number of real roots is $\frac{2}{\pi}\log n + o(\log n)$. In this paper, we determine the true nature of the error term by showing that the expectation equals $\frac{2}{\pi}\log n + O(1)$. Prior to this paper, such estimate has been known only in the gaussian case, thanks to works of Edelman and Kostlan.

1. INTRODUCTION

Consider a random polynomial $P_{n,\xi}(z) = \sum_{i=0}^n \xi_i x^i$ where ξ_i are iid copies of a real random variable ξ with mean zero. Let $N_{n,\xi}$ denote the number of real roots of $P_{n,\xi}$. In what follows the asymptotic notations are used under the assumption that $n \to \infty$; notation such as $O_k(1)$ means that the hidden constant in big "O" may depend on a given parameter k.

Waring was the first to investigate roots of random polynomials as far back as 1782 (see, for instance, Todhunter's book on early history of probability [24, page 618], which also mentioned a similar contribution of Sylvester). As customary in those old days, the source of randomness was not specified in these works. More rigorous and systematic studies of $N_{n,\xi}$ started in the 1930s. In 1932, Bloch and Pólya [4] considered the special case when ξ is uniformly distributed in $\{-1, 0, 1\}$ and established the upper bound

$$\mathbf{E}N_{n,\xi} = O(n^{1/2}).$$

Their method can be extended to other discrete distributions such as Bernoulli ($\xi = \pm 1$ with probability 1/2); see [8]. This bound is not sharp, and it was a considerable surprise when Littlewood and Offord showed that random polynomials actually have a remarkably small number of real zeroes. In a series of fundamental papers [17, 18, 19], published between 1939 and 1945, they proved a strong bound

$$\frac{\log n}{\log\log\log n} \ll N_{n,\xi} \ll \log^2 n \tag{1}$$

with probability $1 - o(1)$, for many basic variables ξ (such as Bernoulli, Gaussian, and uniform on $[-1, 1]$).

During this time, in 1943, another fundamental result was achieved by Kac [14], who found an asymptotic estimate for $\mathbf{E}N_{n,\xi}$ in the case that ξ is standard real Gaussian $N(0, 1)$, showing

$$\mathbf{E}N_{n,N(0,1)} = \left(\frac{2}{\pi} + o(1)\right)\log n. \tag{2}$$

H. Nguyen is supported by research grant DMS-1358648.

O. Nguyen and V. Vu is supported by research grants DMS-0901216 and AFOSAR-FA-9550-09-1-0167.

It took much effort to extend (2) to other distributions. Kac's method does provide a formula for $\mathbf{E}N_{n,\xi}$ for any ξ. However, this formula is hard to estimate when ξ is not Gaussian. In a subsequent paper [15], Kac managed to extend (2) to the case when ξ is uniform on $[-1,1]$ and Stevens [22] extended it further to cover a large class of ξ having continuous and smooth distributions with certain regularity properties (see [22, page 457] for details). These papers relied on Kac's formula and the analytic properties of the distribution of ξ are essential. (*A historical remark* : In [14], Kac was very optimistic and thought that his argument would work for all random variables. However, he soon realized that it was not the case, and his proof for the uniform case was already substantially more complicated than that of the gaussian case; see [15].)

For random variables with no analytic properties, it is a completely different ball game. Since Kac's paper, it took sometime until Erdős and Offord in 1956 [6] found a new approach to handle discrete distributions. Considering the case when ξ is Bernoulli, they proved that with probability $1-o(\frac{1}{\sqrt{\log\log n}})$

$$N_{n,\xi} = \frac{2}{\pi}\log n + o(\log^{2/3} n \log\log n). \tag{3}$$

Erdős often listed this result among his favorites achievements (see, for instance [5]). In late 1960s and early 1970s, Ibragimov and Maslova [10, 11] successfully refined Erdős-Offord method to handle any variable ξ with mean 0. They proved that for any ξ with mean zero which belong to the domain of attraction of the normal law,

$$\mathbf{E}N_{n,\xi} = \frac{2}{\pi}\log n + o(\log n). \tag{4}$$

The error term $o(\log n)$ is implicit in their papers. However, by following the proof (see the last bound in [10, page 247]) it seems that one can replace it by a more precise term $O(\log^{1/2} n \log\log n)$. For related results, see also [12, 13]. Few years later, Maslova [20, 21] showed that if ξ has mean zero and variance one and $\mathbf{P}(\xi = 0) = 0$, then the variance of $N_{n,\xi}$ is $(\frac{4}{\pi}(1-\frac{2}{\pi}) + o(1))\log n$.

Fast forwarding twenty more years, one records another important development, made by Edelman and Kostlan [7] in 1995. They introduced a new way to handle the Gaussian case and estimate $\mathbf{E}N_{n,N(0,1)}$. Using delicate analytical tools, they proved the following stunningly precise formula

$$\mathbf{E}N_{n,N(0,1)} = \frac{2}{\pi}\log n + C_{N(0,1)} + \frac{2}{\pi n} + O(\frac{1}{n^2}) \tag{5}$$

where $C_{N(0,1)} \approx .625738072..$ is an explicit constant (it is the value of an explicit, but complicated, integral).

The approach used in [7] relies critically on the fact that a random Gaussian vector distributes uniformly on the unit sphere and cannot be used for other distributions. The true nature of the error term in $\mathbf{E}(N_{n,\xi})$ has not been known in general and all of the existing approaches lead to error term polynomial in $\log n$. In particular, it seems already very difficult to improve upon the order of magnitude of the error term in Ibragimov and Maslova's analysis.

In this paper, we provide a new method to estimate $\mathbf{E}N_{n,\xi}$. This method enables us to derive the following sharp estimate

Theorem 1. *For any random variable ξ with mean 0 and variance 1 and bounded $(2+\epsilon)$-moment*

$$\mathbf{E}N_{n,\xi} = \frac{2}{\pi}\log n + O_{\epsilon,\xi}(1).$$

Without loss of generality, we will assume ϵ to be sufficiently small. To emphasize the dependence of the hidden constant in big O on the atom variable ξ, let us notice that if ξ is Bernoulli, then the random polynomial $P_{n,\xi}$ does not have any real root in the interval $(-1/2, 1/2)$ with probability 1. On the other hand, one can show that if ξ is gaussian then the expectation of number of real roots in $(-1/2, 1/2)$ is $\frac{1}{\pi}\log 3 + o(n^{-17})$. Thus, it is reasonable to expect that the expectation in the Gaussian case exceeds that in the Bernoulli case by a positive constant. Our numerical experiment tends to agree with this.

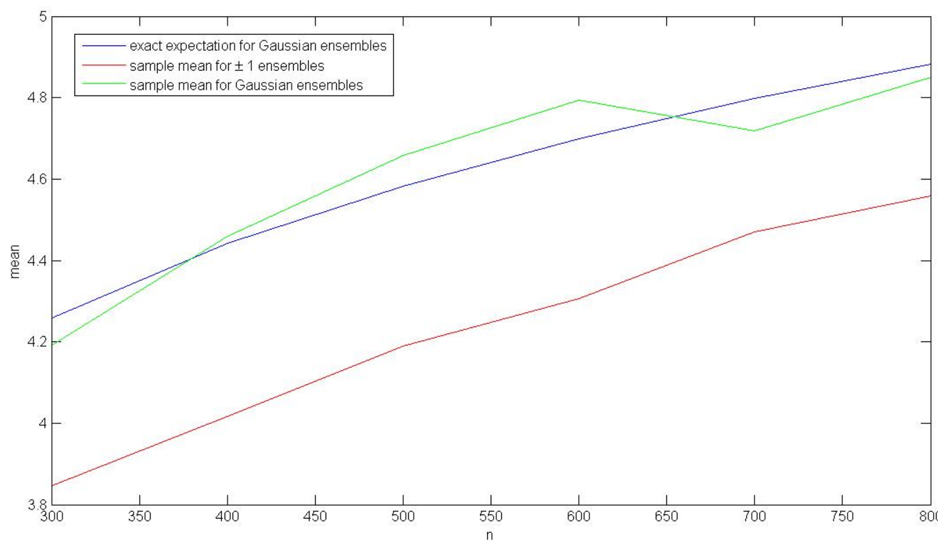

FIGURE 1. Sample means of the number of real roots for Gaussian and Bernoulli ensembles; the x-axis represents the degree. It seems that the expectation in the Gaussian cases exceeds that in the Bernoulli case by roughly .4.

Theorem 1 is a corollary of a stronger theorem, which provides an even more satisfying estimate on the main part of the spectrum. For any region $D \subset \mathbb{R}$, let $N_{n,\xi}D$ denote the number of real roots in D. It is well known (see for instance [3, 9]) that one can reduce the problem of estimating $N_{n,\xi}$ to $N_{n,\xi}[0,1]$; as a matter of fact

$$\mathbf{E}N_{n,\xi} = 4\mathbf{E}N_{n,\xi}[0,1].$$

Inside the interval $[0,1]$, most of the real roots are clustered near 1. For any constant C, the number of roots between 0 and $1-C^{-1}$ is only $O_C(1)$. More precisely,

Lemma 2. *For any positive constant C, there exists a constant $M(C)$ such that*

$$\mathbf{E}N_{n,\xi}[0, 1-C^{-1}) \le M(C). \tag{6}$$

Furthermore, there exists a constant C_0 such that for any C greater than C_0,

$$\mathbf{E}N_{n,\xi}[0, 1 - C^{-1}) \leq \frac{1}{2\pi} \log C + M(C_0). \tag{7}$$

Notice that C is allowed to depend on n in (7). Thus (by taking C to be, say, $100n$) (7) almost gives the upper bound in Theorem 1. As well known in this area, the lower bound is often the heart of the matter.

Let us focus on the bulk of the spectrum, the interval $(1 - C^{-1}, 1]$. For this part, we obtain the following precise estimates, regardless the nature of the atom variable ξ.

Theorem 3. *There exists a constant C_0 such that for any variable ξ with mean 0, variance 1, and bounded $(2 + \epsilon)$-moment*

$$\left| \mathbf{E}N_{n,\xi}(1 - C_0^{-1}, 1] - \int_{1-C_0^{-1}}^{1} \frac{1}{\pi} \sqrt{\frac{1}{(t^2-1)^2} - \frac{(n+1)^2 t^{2n}}{(t^{2n+2}-1)^2}} dt \right| \leq C_0^{-\epsilon}. \tag{8}$$

Furthermore, for any number $C \geq C_0$, there exists $C' \in [C^\epsilon, C]$ such that

$$\left| \mathbf{E}N_{n,\xi}(1 - C'^{-1}, 1] - \int_{1-C'^{-1}}^{1} \frac{1}{\pi} \sqrt{\frac{1}{(t^2-1)^2} - \frac{(n+1)^2 t^{2n}}{(t^{2n+2}-1)^2}} dt \right| \leq C'^{-1}. \tag{9}$$

The integral on the LHS of (8) is the explicit formula for $\mathbf{E}N_{n,N(0,1)}(1 - C_0^{-1}, 1]$ (see [7]). Thus, one can rephrase (8) as

$$\left| \mathbf{E}N_{n,\xi}(1 - C_0^{-1}, 1] - \mathbf{E}N_{n,N(0,1)}(1 - C_0^{-1}, 1] \right| \leq C_0^{-\epsilon}. \tag{10}$$

This, combining with the argument following Theorem 1, reveals an interesting fact that the impact of the distribution of ξ is felt only at the left "edge" of the spectrum.

Theorem 1 follows immediately from Lemma 2 and Theorem 3. Our proofs are quantitative and in principle one can derive an explicit value for C_0. However, this involves a tedious book keeping and in general we do not try to optimize the constants in this paper. Our proof also shows that (10) still holds if we replace the interval $(1 - C_0^{-1}, 1]$ by any subinterval. Furthermore, our approach, which makes use of a recent universality result from [23] and the non-existence of near double roots, is entirely different from previous approaches.

Remark 4. We would like to point out an important fact that our results hold, without any significant modification in the proof, for more general settings where the variables ξ_i in the definition of P_n are not iid. It suffices to assume that they all have mean 0, variance 1, and uniformly bounded $(2 + \epsilon)$-moments.

2. Number of real roots in an interval very close to 1

Our starting point is the following theorem, which is a corollary of [23, Theorem 25].

Theorem 5. *There is a positive constant α such that the following holds. Let $\epsilon > 0$ be an arbitrary small constant and ξ be any random variable with mean zero, variance one and bounded $(2+\epsilon)$-moment. Then there is a constant $C_1 := C_1(\epsilon)$ such that for any $n \geq C_1$ and any interval $I := (1-r, a) \subset (1-n^{-\epsilon}, 1]$*

$$|\mathbf{E}_{n,\xi} I - \mathbf{E}_{n,N(0,1)} I| \leq n^{-\alpha}. \tag{11}$$

This is close, in spirit, to (10). The main technical obstacle here is that the result holds only in a region polynomially close to 1. The key new ingredient we have in this paper is the observation that a random polynomial, with high probability, does not have double or near double roots. We discuss this observation, which is of independent interest, in the next section. At the end, we can prove (10) by combining (a sufficiently quantitative version of) this observation with Theorem 5. The proof of Lemma 2, which is independent from the main argument, is provided at the end of the paper.

3. Non-existence of near double roots

A double root λ satisfies $P_n(\lambda) = P_n'(\lambda) = 0$. We introduce a more general notion of *near double roots*: λ is a near double root if $P_n(\lambda) = 0$ and $|P_n'(\lambda)|$ is small. Existence of double roots and near double roots are of interest in analysis and numerical analysis (see for instance the studies of Newton's method for finding real roots [2]).

Our new tool is the following lemma, which asserts that there are no near double roots in the bulk of the spectrum with high probability.

Lemma 6. *For any constant $C > 0$, there exist $B = B(C), B_0 = B_0(C)$, and $B_1 = B_1(C)$ such that*

$$\mathbf{P}\Big(\exists x \in (1 - B_0^{-1}, 1 - \frac{B_1 \log n}{n}] : P_n(x) = 0, |P_n'(x)| \leq n^{-B}\Big) = o(n^{-C}).$$

3.1. Preliminaries.

To start, we deduce a property of polynomials having a near double root. Let δ be a small parameter to be chosen and $Q \subset (1/2, 1]$ be an interval of length 2δ centered at x_Q. If there is $x \in Q$ such that $P_n(x) = 0$ then by the mean value theorem $|P_n(x_Q)| \leq \delta |P_n'(y)|$ for some y between x and x_Q. (We can write $\delta/2$ instead of δ on the RHS, but this does not make any difference.)

Assume that $|P_n'(x)| \leq n^{-B}$, then by applying the mean value theorem again, we have $|P_n'(y)| \leq \delta |P_n''(z)| + n^{-B}$ for some z between x and y. Furthermore, with a loss of a probability bound $O(n^{-C-1})$, one can assume that $|\xi_i| \leq n^{C/2+1}$ for all i, and so $|P''(z)| \leq n^{4+C/2}$. Thus,

$$|P_n(x_Q)| \leq \delta^2 n^{4+C/2} + \delta n^{-B}. \tag{12}$$

Set $\delta := n^{-A}$ for some suitable constant A to be chosen, and $B := A - C/2 - 2$ so that the term $\delta^2 n^{4+C/2}$ dominates. We partition the interval $I := (1 - B_0^{-1}, 1 - \frac{C_1 \log n}{n}]$ into subintervals

$I_i = (1 - B_0^{-1} + (i-1)n^{-A-3}, 1 - B_0^{-1} + (i+1)n^{-A-3}]$ with center $x_i = 1 - B_0^{-1} + in^{-A-3}$ and length δ and show that with high probability (12) fails at every center.

3.2. **Small ball estimate.** Set $\gamma := 2\delta^2 n^{4+C/2}$, we are going to prove the following small ball estimate.

Lemma 7. *For any* $1 - B_0^{-1} < x < 1 - B_1 \log n/n$, *one has*

$$\mathbf{P}(|P(x)| \le \gamma) = O(\gamma^{.99}).$$

In order to prove this theorem, we first need the following elementary claim whose proof is left as an exercise.

Claim 8. *There exist positive constants* c_0 *and* p_0 *(depending on* ϵ*) such that for any* ξ *of mean 0, variance 1, and bounded* $(2+\epsilon)$*-moment, there exists* $c_0 \le c \le c_0^{-1}$ *such that*

$$\mathbf{P}(c < |\xi - \xi'| < 2c) \ge p_0.$$

By switching from ξ to ξ/c if needed, without changing the result of Lemma 7, one can assume that

$$\mathbf{P}(1 < |\xi - \xi'| < 2) \ge p_0.$$

Proof of Lemma 7. Let $\xi_1', \dots, \xi_n'$ be independent copies of $\xi_1, \dots, \xi_n$, let $\epsilon_1, \dots, \epsilon_n \in \{-1, 1\}$ be independent Bernoulli variables (independent of both ξ_i and ξ_i'), and let $\tilde{\xi}_i$ be the random variable that equals ξ_i when $\epsilon_i = +1$ and ξ_i' when $\epsilon_i = -1$. Then $\tilde{\xi}_1, \dots, \tilde{\xi}_n$ have the same joint distribution as $\xi_1, \dots, \xi_n$, so it suffices to obtain the bound

$$\mathbf{P}(|\sum_{i=0}^{n} \tilde{\xi}_i x^i| \le \gamma) = O(\gamma^{.99}).$$

Let $\delta_0 > 0$ be sufficiently small ($\delta_0 = .000001$ would suffice) and t_0 be such that

$$(1 - p_0)^{t_0} < \delta_0. \tag{13}$$

Let N be chosen so that x^{N+1} is approximately γ (such as $2\gamma \le x^{N+1} \le 4\gamma$ would suffice). Notice that as $1 - B_0^{-1} \le x \le 1 - B_1 \log n/n$ with sufficiently large B_0, B_1, we have

$$\Omega(\log n) \le N \le n.$$

Without loss of generality we assume that $N+1$ is divisible by t_0. Divide the set $\{0, 1, \dots, N\}$ into $m = N/t_0$ intervals $J_1, \dots, J_m$ with $J_1 := [0, \dots, t_0 - 1], J_2 := [t_0, \dots, 2t_0 - 1], \dots, J_m := [N - t_0, \dots, N]$.

Let $J \subset \{1, \dots, m\}$ be a (random) subset of indices k for which the following holds for at least one index i from J_k,

$$1 < |\xi_i - \xi_i'| < 2. \tag{14}$$

By definition, we have

$$\mathbf{P}(k \in J) \geq 1 - (1-p)^{t_0} \geq 1 - \delta_0.$$

Let $\mathcal{E}$ be the event that $|J| \geq m' := (1-2\delta_0)m$. From Chernoff's lower tail bound, one has

$$\mathbf{P}(\mathcal{E}^c) \leq 2\exp(-\frac{\delta_0^2}{2}m). \tag{15}$$

As $x \geq 1 - B_0^{-1}$ and B_0 is sufficiently large, we have

$$\exp(-\frac{\delta_0^2}{2}m) = \exp\big(-\frac{\delta_0^2}{2t_0}(N+1)\big) \leq (1-B_0^{-1})^{N+1} \leq x^{N+1} = O(\gamma),$$

where we recall that x^{N+1} is approximately γ.

From now on we condition on $\mathcal{E}$, thus assuming

$$m' \geq (1-2\delta_0)m. \tag{16}$$

By considering a subset of J if needed, one can assume that $|J| = m'$. From each interval J_k where $k \in J$, we choose one single index $i \in J_k$ such that (14) holds. In what follows we will fix the random variables ξ_i, ξ_i' for all i; and the signs ϵ_i if i was not chosen.

In summary, one obtain subsequences $1 \leq i_1 < \dots < i_{m'} \leq m$ and $0 \leq n_1 < n_2 < \dots < n_{m'} \leq N$ with the following properties:

- $1 < |\xi_{n_j} - \xi_{n_j}'| < 2$;
- $n_j \in J_{i_j}$.
- The (only) source of randomness comes from the sign $\epsilon_{n_1}, \dots, \epsilon_{n_{m'}}$.

Set

$$y := x^{t_0}.$$

By definition, as $n_j \in J_{i_j} = [(i_j-1)t_0, \dots, i_j t_0 - 1]$, one has the following double bound

$$y^{i_j} < x^{n_j} \leq y^{i_j-1}. \tag{17}$$

As $1 - B_0^{-1} < x < 1 - B_1 \log n/n$, there is a unique positive integer $l \leq m$ such that

$$1/4 < y^l < 1/2 \leq y^{l-1}. \tag{18}$$

Furthermore, since B_0 is sufficiently large, one has the following elementary bound

$$l \geq 1000. \tag{19}$$

Let k be the largest integer such that $(l+2)k \leq m$. Thus

$$y^{(l+2)k} \geq y^m = x^{t_0 m} = x^{N+1} \geq 2\gamma \text{ and } y^{(l+2)(k+1)} \leq y^m = x^{N+1} \leq 4\gamma. \tag{20}$$

Again, because B_0 is sufficiently large, $y^{l+2} = y^3 y^{l-1} \geq y^3/2 > 1/4$. Thus as $y^{(l+2)(k+2)} \leq 4\gamma$, k must have order at least $\Omega(\log n)$. This yields the following elementary bound (assuming n sufficiently large),

$$k \geq 1000. \tag{21}$$

Let S be the subset of multiples of $l+2$ in $\{0,\dots, \mathrm{m}\}$, $S := \{0, l+2, \dots, \lfloor m/(l+2) \rfloor (l+2)\}$. Consider the decomposition $\{0, \dots, m\}$ into $S \cup (S+1) \cup \dots \cup S + (l+1)$. By (16) and by the pigeon hole principle, there exists $i_0 \leq l+1$ such that

$$|S + i_0 \cap \{i_1, \dots, i_{m'}\}| \geq (1 - 2\delta_0) m/(l+2). \tag{22}$$

We now work with the partial sum of x^{n_j} with $i_j \in S + i_0$. To do this, we first introduce an elementary property of Bernoulli sums.

Given a quantity $t > 0$, we say that a set X of real numbers is *t-separated* if the distance between any two elements of X is at least t.

Claim 9. *The set* $\left\{ \sum_{1 \leq i \leq k} \epsilon_i y^{i(l+2)}, \epsilon_i \in \{-1, 1\} \right\}$ *is* $2y^{k(l+2)}$*-separated.*

Proof of Claim 9. Assume that there are two terms within distance smaller than $2y^{k(l+2)}$. Consider their difference, which has the form $2(\epsilon_{m_1} y^{m_1(l+2)} + \dots + \epsilon_{m_j} x_i^{m_j(l+2)})$ for some $m_1 < \dots < m_j \leq k$. As $y^{l+2} < y^l < 1/2$, this difference in absolute value is at least

$$2(y^{m_1(l+2)} - y^{m_2(l+2)} - \cdots - y^{m_j(l+2)}) \geq 2y^{k(l+2)}, \tag{23}$$

a contradiction. □

By following the same argument, one obtains the following.

Claim 10. *The set* $\left\{ \sum_{i_j \in S+i_0} \epsilon_j x^{n_j}, \epsilon_i \in \{\xi_{n_j}, \xi'_{n_j}\} \right\}$ *is* $2y^{i_0}y^{k(l+2)}$*-separated.*

Proof of Claim 10. Recall that by our conditioning,

$$1 < |\xi_{n_j} - \xi'_{n_j}| < 2.$$

Furthermore, if $i_j < i_{j'} \in S + i_0$ then $i_{j'} \geq i_j + l + 2$. So, by (17)

$$\frac{x^{n_{i_{j'}}}}{x^{n_{i_j}}} \leq \frac{y^{i_{j'}-1}}{y^{i_j}} < y^l < 1/2.$$

□

We now finish the proof of Lemma 7. By Claim 10, and by the bound (22)

$$\sup_{R\in\mathbb{R}} \mathbf{P}\Big(|\sum_{i_j\in S+i_0} \tilde{\xi}_{n_j} x^{n_j} + R| \leq 2y^{i_0}y^{k(l+2)}\Big) \leq 2^{-(1-2\delta_0)k}. \tag{24}$$

Using $2y^{i_0}y^{k(l+2)} \geq 2y^{(k+1)(l+2)} \geq \gamma$, we obtain

$$\sup_{R\in\mathbb{R}} \mathbf{P}\Big(|\sum_{i_j\in S+i_0} \tilde{\xi}_{n_j} x^{n_j} + R| \leq \gamma\Big) \leq 2^{-(1-2\delta_0)k}. \tag{25}$$

Consider the probability bound on the RHS. Notice from (19) and (21) that both k and l are at least 1000. So, $(l-1)k \geq .999(k+1)(l+2)$. Thus, with $\delta_0 = .000001$ and recall that $1/2 \leq y^{l-1}$

$$2^{-(1-2\delta_0)k} \leq y^{(1-2\delta_0)(l-1)k} \leq y^{(1-2\delta_0).999(k+1)(l+2)} \leq \gamma^{.99}, \tag{26}$$

where we used (20) in the last estimate, assuming n sufficiently large. □

We now complete the proof of our main result.

Proof of Lemma 6. Since there are less than δ^{-1} intervals, it follows from Lemma 7 and by the union bound,

$$\mathbf{P}(\exists i, |P(x_i)| \le \gamma) \le \delta^{-1}\gamma^{.99} = \delta^{.98} n^{.99(4+C/2)} = o(n^{-.98A+4+C/2}).$$

By setting $A := 3C + 6$ and recall our choice $B = A - C/2 - 2$, we have

$$\mathbf{P}\Big(\exists x \in (1 - B_0^{-1}, 1 - \frac{B_1 \log n}{n}] : P_n(x) = 0, |P_n'(x)| \le n^{-5C/2-4}\Big) = o(n^{-C}),$$

proving the desired statement.

□

Remark 11. It follows from our proof that instead of having bounded $(2+\epsilon)$-moment, it suffices to assume that there exist positive constants c_1, c_2 and p such that

$$\mathbf{P}(c_1 < |\xi - \xi'| < c_2) \ge p.$$

Remark 12. We can also extend our argument, with few modifications, to show the non-existence of near double roots in $(1 - B_0^{-1}, 1]$ for general ξ, and in the whole spectrum for Bernoulli polynomials; details will follow in a subsequent paper.

Using a similar argument (with the same definition of δ and I) we can prove the following.

Lemma 13. *For any constant $C > 1$, the following holds with probability $1 - o(n^{-C})$.*

- *There is no pair of roots in $I = (1 - B_0^{-1}, 1 - B_1 \log n/n)$ with distance at most $\delta = 2n^{-3C-6}$.*
- *For any given $a \in I$, there is no root with distance at most $\delta' := n\delta^2$ from a.*

Proof of Lemma 13. For the first statement, we can fix a δ-net $S = \{x_1, \dots, x_M\}$ on I such that for any $x \in I$, there is some $x_i \in S$ with distance at most δ to x and $M \le \delta^{-1} + 1$.

If $P_n(x) = P_n(x') = 0$, then there is a point y between x and x' such that $P_n'(y) = 0$. Thus, for any z with distance at most 2δ from y,

$$|P'(z)| \le 2n^{4+C/2}\delta.$$

There is a point x_i in the net such that $|x_i - x| \le \delta$. For this x_i, $|P_n(x_i)| = |x_i - x||P_n'(z)|$ for some z between x and x_i. Because x has distance at most δ from x', x also has distance at most δ from y, and so z has distance at most 2δ from y. It follows that

$$|P_n(x_i)| \le 2n^{4+C/2}\delta^2.$$

From the previous proof, the probability that the above bound holds for some i is $o(n^{-C})$.

For the second statement, assume that $P_n(x) = 0$ and $|a - x| \leq \delta'$, then $|P_n(a)| = |a-x||P_n'(y)|$ for some y between a and x. On the other hand, with a loss of n^{-C-1} in probability, one can assume that $|P_n'(y)| \leq n^{3+C/2}$ for any $y \in [0,1]$, it follows that $|P_n(a)| \leq n^{3+C/2}\delta' = n^{4+C/2}\delta^2$, using the notation in the previous proof. But again the previous proof provides that $\mathbf{P}(\exists a \in I, |P_n(a)| \leq n^{4+C/2}\delta^2) = o(n^{-C})$.

□

4. Near Double roots and Truncation

First of all, we need to truncate the random variables $\xi_0, \dots, \xi_n$. Let $d > 0$ be a parameter and let $\mathcal{B}_d$ be the event $|\xi_0| < n^d \wedge \dots \wedge |\xi_n| < n^d$. As ξ has unit variance, we have the following elementary bound

$$\mathbf{P}(\mathcal{B}_d^c) \leq n^{1-2d}.$$

In what follows we will condition on $\mathcal{B}_d$ with $d = 2$.

Consider $P_n(x) = \sum_{i=0}^n \xi_i x^i$ and for $m < n$, we set

$$g_m := P_n - P_m = \sum_{i=m+1}^n \xi_i x^i.$$

For any $0 < x \leq 1 - r$, Chernoff's bound yields that for any $\lambda > 0$

$$\mathbf{P}\Big(|g_m(x)| \geq \lambda n^2 \sqrt{\sum_{i=m+1}^n (1-r)^{2i}}\Big|\mathcal{B}_2\Big) \leq \mathbf{P}\Big(|g_m(x)| \geq \lambda n^2 \sqrt{\sum_{i=m}^n x^{2i}}\Big|\mathcal{B}_2\Big) \leq 2\exp(-\lambda^2/2).$$

Since

$$\sum_{i=m+1}^n (1-r)^{2i} \leq (1-r)^{2m+2} \frac{1}{1-(1-r)^2} := s(r,m),$$

it follows that

$$\mathbf{P}(|g_m| \geq \lambda n^2 \sqrt{s(r,m)}|\mathcal{B}_2) \leq 2\exp(-\lambda^2/2). \tag{27}$$

We next compare the roots of P_n and P_m in the interval $(0, 1-r)$. Our intuition is that if $s(r,T)$ is sufficiently small, then there is an bijection ϕ between the two sets of roots such that x and $\phi(x)$ are very close. In particular, the numbers of roots of two polynomials in this interval are the same with high probability.

Lemma 14. *Assume that $F(x) \in C^2(\mathbb{R})$ and $G(x)$ are continuous functions satisfying the following properties*

- $F(x_0) = 0$ *and* $|F'(x_0)| \geq \epsilon_1$*;*
- $|F''(x)| \leq M$ *for all* $x \in I := [x_0 - \epsilon_1 M^{-1}, x_0 + \epsilon_1 M^{-1}]$*;*
- $\sup_{x\in I} |F(x) - G(x)| \leq \frac{1}{4}\epsilon_1^2 M^{-1}$.

Then G has a root in I.

Proof of Lemma 14. We can assume, without loss of generality, that $G(x_0) \geq 0$. Consider two cases:

Case 1. $F'(x_0) \geq \epsilon_1$. Using the bound $|F''(x)| \leq M$ and the mean value theorem, it follows that $F'(x) \geq \frac{1}{2}\epsilon_1$ for all x satisfying $x_- := x_0 - \frac{1}{4}\epsilon_1 M^{-1} \leq x \leq x_0$. It follows that $F(x_-) \leq -\frac{1}{4}\epsilon_1^2 M^{-1}$. Thus, $G(x_-) \leq 0$ and so G must have a root between x_- and x_0.

Case 2. $F'(x_0) \leq -\epsilon_1$. Arguing similarly, we can prove that G has a root between x_0 and $x_+ := x_0 + \frac{1}{4}\epsilon_1 M^{-1}$. □

By combining Lemma 14 and Lemma 6, we obtain the following key observation.

Set $B := \max(B_1, B(2), 8)$, where $B_1, B(2)$ are the constants from Theorem 6 and Theorem 13 corresponding to $C = 2$.

Lemma 15 (Roots comparison for truncated polynomials)**.** *Let $r \in (B_1 \log n/n, B_0^{-1}]$ and $m = 4Br^{-1}\log n$. Then for any subinterval J of $(1 - B_0^{-1}, 1 - r)$ one has*

$$|\mathbf{E}N_n J - \mathbf{E}N_m J| \leq m^{-1}. \tag{28}$$

Proof of Lemma 15. Condition on $\mathcal{B}_2$, one has $\sup_{|x|\leq 1} \max(|P_n''(x)|, |P_m''(x)|) \leq n^5$ with probability one. Set $\lambda := \log n$, by (27), with probability at least $1 - 2\exp(-\log^2 n/2) \geq 1 - n^{-\omega(1)}$ the following holds

$$|P_n(x) - P_m(x)| \leq \lambda n^2 \sqrt{s(r,m)} = \lambda n^2 (1-r)^{m+1} \frac{1}{\sqrt{1-(1-r)^2}} \leq n^{-3B}$$

for all $0 \leq x \leq 1 - r$.

By Lemma 6 (with $C = 2$), $|P_n'(x)| \geq n^{-B}$ for all $x \in J$ with probability $1 - o(n^{-2})$. Applying Lemma 14 with $\epsilon_1 = n^{-B}, M = n^5$, $F = P_n, G = P_m$, we conclude that with probability $1 - o(n^{-2})$, for any root x_0 of $P_n(x)$ in the interval $(1 - B_0^{-1}, 1 - r)$ (which is a subset of $(1 - B_0^{-1}, 1 - B_1 \log n/n)$), there is a root y_0 of $P_m(x)$ such that $|x_0 - y_0| \leq \epsilon_1 M^{-1} = n^{-B-5}$.

On the other hand, applying Lemma 13 with $C = 2$, again with probability $1 - o(n^{-2})$ there is no pair of roots of P_n in J with distance less than n^{-B}. It follows that for different roots x_0 we can choose different roots y_0. Furthermore, by the second part of Lemma 13, with probability $1 - o(n^{-2})$, all roots of $P_n(x)$ must be of distance at least n^{-B} from the two ends of the interval. If this holds, then all y_0 must also be inside the interval. This implies that with probability at least $1 - o(n^{-2})$, the number of roots of P_m in J is at least that of P_n. Putting together, we obtain

$$\mathbf{E}N_m J \geq \mathbf{E}N_n J - (o(n^{-2}) + n^{-3})n \geq \mathbf{E}N_n J - n^{-1}, \tag{29}$$

where the extra term n^{-1} comes from the fact that P_n has at most n real roots.

Switching the roles of P_n and P_m, noting that as $r = 4B \log n/m \geq B_1 \log m/m$,

$$J \subset (1 - B_0^{-1}, 1 - r) \subset (1 - B_0^{-1}, 1 - B_1 \log m/m).$$

As such, Lemmas 6 and 13 are also applicable to $P_m(x)$. Argue similarly as above, we also have

$$\mathbf{E}N_n J \geq \mathbf{E}N_m J - (o(m^{-2}) + n^{-3})m \geq \mathbf{E}N_m J - m^{-1}. \tag{30}$$

It follows that

$$|\mathbf{E}N_n J - \mathbf{E}N_m J| \leq m^{-1}.$$

□

Remark 16. By applying Lemma 6 and Lemma 13 to higher values of C, with sufficiently large B_0 and B_1 one obtains the following bound for any interval J of $(1 - B_0^{-1}, 1 - r)$,

$$|\mathbf{E}N_n J - \mathbf{E}N_m J| \leq m^{-C}. \tag{31}$$

However, in later application $C = 1$ would be sufficient.

Remark 17. If one can show Lemma 6 for $B_0 = 1$, then Lemma 15 is true for any $J \subset (0, 1 - r)$.

5. Proof of Theorem 3

We first prove (9). Let $C_0 = \max(C_1, B_0^{1/\epsilon})$ where C_1 is the constant in Theorem 5 and let C be any number greater than C_0.

Let $\epsilon > 0$ be a small constant to be chosen. Set $n_0 := n, r_0 = n^{-\epsilon}$ and define recursively

$$n_i := 4Br_{i-1}^{-1} \log n_{i-1}, \text{ and } r_i := n_i^{-\epsilon}, i \geq 1.$$

It is clear that $\{n_i\}$ and $\{r_i\}$ are respectively decreasing and increasing sequences . Let L be the largest index such that $n_L \geq C$. By definition, $r_i \leq B_0^{-1}$ for all $1 \leq i \leq L$. Also, as $C > n_{L+1} = 4Bn_L^{\epsilon} \log n_L \geq n_L^{\epsilon}$, it follows that $n_L < C^{1/\epsilon}$. Thus,

$$n_L \in [C, C^{1/\epsilon}]. \tag{32}$$

Set $I_i := (1 - r_i, 1 - r_{i-1}]$ (with the convention that $r_{-1} = 0$). Because $I_i \subset (1 - B_0^{-1}, 1 - r_{i-1}] \subset (1 - B_0^{-1}, 1 - r_{j-1}]$ for $1 \leq j \leq i$, by (28),

$$|\mathbf{E}N_{n_{j-1}}I_i - \mathbf{E}N_{n_j}I_i| \le n_{j-1}^{-1}.$$

By the triangle inequality,

$$|\mathbf{E}N_{n_0}I_i - \mathbf{E}N_{n_i}I_i| \le \sum_{j=1}^{i} n_{j-1}^{-1} \le 2n_{i-1}^{-1}. \tag{33}$$

On the other hand, as $n_i \ge C_1$ for $i \le L$, by Theorem 5

$$|\mathbf{E}N_{n_i}I_i - \mathbf{E}N_{n_i,N(0,1)}I_i| \le n_i^{-\alpha}. \tag{34}$$

Combining (33) and (34), one obtains

$$|\mathbf{E}N_{n_0}I_i - \mathbf{E}N_{n_0,N(0,1)}I_i| \le 2n_{i-1}^{-1} + n_i^{-\alpha}. \tag{35}$$

Let $I = \cup_{i=0}^{L} I_i$, again by the triangle inequality

$$|\mathbf{E}N_nI - \mathbf{E}N_{n,N(0,1)}I| \le 2\sum_{i=0}^{n} n_i^{-1} + \sum_{i=0}^{n} n_i^{-\alpha}.$$

The left end point of I is $1 - n_L^{-\epsilon} = 1 - C'^{-1}$, where $C' := n_L^{\epsilon} \in [C^{\epsilon}, C]$ by (32). Furthermore, by definition of the n_i, it is easy to show that

$$\sum_{i=0}^{L} n_i^{-\alpha} \le 2n_L^{-\alpha} = o(C'^{-1}),$$

assuming (without loss of generality) that $\epsilon < \alpha/2$.

Thus, we can conclude that there exists $C' \in [C^{\epsilon}, C]$ such that for $I := (1 - C'^{-1}, 1]$,

$$|\mathbf{E}N_nI - \mathbf{E}N_{n,N(0,1)}I| \le C'^{-1},$$

concluding the proof of (9).

Remark 18. Notice that Theorem 5 holds for any subinterval of the form $(1 - r, a)$ where $r \le n^{-\epsilon}$. Thus, one can prove the same bound for I being any subinterval of $(1 - C'^{-1}, 1]$ by setting $I_i := (1 - r_i, 1 - r_{i-1}] \cap I$ in the above argument. As a consequence, by choosing $C = C_0$ and $I = (1 - C_0{}^{-1}, 1]$ one obtains

$$|\mathbf{E}N_n(1 - C_0{}^{-1}, 1] - \mathbf{E}N_{n,N(0,1)}(1 - C_0{}^{-1}, 1]| \le C'^{-1} \le C_0^{-\epsilon},$$

proving (8).

6. Proof of Lemma 2

6.1. **Justification of** (6)**.** We follow the approach developed in [11]. First, there exist some constants $q_1, c \in (0,1)$ depending only on ϵ and T, where T is an upper bound of $\mathbf{E}|\xi|^{2+\epsilon}$, such that $\mathbf{P}(|\xi| \le c) = q \le q_1 < 1$. Indeed, put $p = \mathbf{P}(|\xi| > c)$, then

$$\begin{aligned} 1 = \mathbf{E}|\xi|^2 &= \mathbf{E}\left(|\xi|^2, |\xi| \le c\right) + \mathbf{E}\left(|\xi|^2, |\xi| > c\right) \\ &\le c^2 + \mathbf{E}\left(|\xi|^{2+\epsilon}\right)^{\frac{2}{2+\epsilon}} \mathbf{P}\left(|\xi| > c\right)^{\frac{\epsilon}{2+\epsilon}} \\ &\le c^2 + p^{\frac{\epsilon}{2+\epsilon}} T^{\frac{2}{2+\epsilon}}. \end{aligned}$$

Thus, by choosing c small, we get p greater than some positive amount.

Next, let

$$B_k = \Big\{\omega : |\xi_0| \le c, \dots, |\xi_{k-1}| \le c, |\xi_k| > c\Big\}, \text{ where } k = 0, \dots, n+1.$$

Then $\mathbf{P}(B_k) = (1-q)q^k$. Note that if P_n has N zeros in $[-1+\frac{1}{C}, 1-\frac{1}{C}]$ then $P_n^{(k)}$ has at least $N-k$ zeros in that interval. Thus,

$$N_{P_n}[-1+\frac{1}{C}, 1-\frac{1}{C}] \le k + N_{P_n^{(k)}}[-1+\frac{1}{C}, 1-\frac{1}{C}].$$

By Jensen's inequality for $P_n^{(k)}$,

$$N_{P_n}[-1+\frac{1}{C}, 1-\frac{1}{C}] \le k + \frac{\log \frac{M_k}{P_n^{(k)}(0)}}{\log \frac{R}{r}},$$

where $R = 1 - \frac{1}{2C}, r = 1 - \frac{1}{C}$, and $M_k = \sup_{|z|=R} \left|P_n^{(k)}(z)\right|$.

Conditioned on B_k, we have

$$P_n^{(k)}(0) = k!\,|\xi_k| > k!c, \text{ and } M_k \le \sum_{j=k}^{n} j(j-1)\dots(j-k+1)|\xi_j| R^{j-k}.$$

Thus, on B_k,

$$
\begin{aligned}
N_{P_n}[-1+\frac{1}{C}, 1-\frac{1}{C}] &\le k + \frac{\log \frac{\sum_{j=k}^{n} j(j-1)\ldots(j-k+1)|\xi_j| R^{j-k}}{k!c}}{\log \frac{R}{r}} \\
&= k + \frac{\log \frac{\sum_{j=k}^{n} c_{jk}|\xi_j|}{c}}{\log \frac{R}{r}},
\end{aligned}
$$

where

$$c_{jk} = j(j-1)\ldots(j-k+1)R^{j-k}/k!. \tag{36}$$

So,

$$\mathbf{E}N_n[-1+\frac{1}{C}, 1-\frac{1}{C}] \le \sum_{k=0}^{n+1} k\mathbf{P}(B_k) + \frac{1}{\log \frac{R}{r}} \sum_{k=0}^{n+1} \int_{B_k} \log\left(\sum_{j=k}^{n} c_{jk}|\xi_j|\right) \mathrm{d}\mathbf{P} - \frac{\log c}{\log \frac{R}{r}} \sum_{k=0}^{n+1} \mathbf{P}(B_k).$$

Since $\sum_{k=0}^{n+1} k\mathbf{P}(B_k) = (1-q)q\sum_{k=0}^{\infty} kq^{k-1} = \frac{q}{1-q} \le \frac{q_1}{1-q_1}$, and $\log \frac{R}{r} = \log\left(1 + \frac{1/2C}{1-1/C}\right) \ge \frac{1}{4C}$, the proof is complete if we can show the following claim.

Claim 19. *There exists a constant C'' such that*

$$\sum_{k=0}^{n+1} \int_{B_k} \log\left(\sum_{j=k}^{n} c_{jk}|\xi_j|\right) d\mathbf{P} \le C''. \tag{37}$$

Proof of Claim 19. Let $X_k = \sum_{j=k}^{n} c_{jk}|\xi_j|$, where we recall c_{jk} from (36), and let $Z_k = \mathbf{E}X_k$. Then

$$Z_k \le \mathbf{E}|\xi| \sum_{j=k}^{\infty} c_{jk} = \frac{\mathbf{E}|\xi|}{(1-R)^{k+1}} \le \frac{1}{(1-R)^{k+1}} = (2C)^{k+1}. \tag{38}$$

Let $B_{ki} = \{\omega \in B_k : e^i Z_k \le X_k \le e^{i+1} Z_k\}$.

Then $\mathbf{P}(B_{ki}) \le e^{-i}$ by Markov's inequality. Let $i_0 = \lfloor -\log P(B_k) \rfloor$, then

$$\begin{aligned}
&\int_{B_k} \log X_k \mathrm{d}\mathbf{P} \le \mathbf{P}(B_k \setminus B_{ki_0}) \log\left(e^{i_0} Z_k\right) + \sum_{i=i_0}^{\infty} \int_{B_{ki}} \log X_k \mathrm{d}\mathbf{P} \\
\le\ & \mathbf{P}(B_k) \log\left(\frac{Z_k}{\mathbf{P}(B_k)}\right) + \sum_{i=i_0}^{\infty} \log\left(e^{i+1} Z_k\right) e^{-i} \\
\le\ & \mathbf{P}(B_k)\Big((k+1)\log(2C) - \log \mathbf{P}(B_k)\Big) + (k+1)\log(2C) \sum_{i=i_0}^{\infty} e^{-i} + \sum_{i=i_0}^{\infty} (i+1) e^{-i} \quad \text{by (38)} \\
\le\ & \mathbf{P}(B_k)\Big((k+1)C' - \log \mathbf{P}(B_k)\Big) + (k+1)C' e^{-i_0} + C'(i_0+1)e^{-i_0} \\
\le\ & \mathbf{P}(B_k)\Big((k+1)C' - \log \mathbf{P}(B_k)\Big) + (k+1)C'\mathbf{P}(B_k) + C'(1 - \log \mathbf{P}(B_k))\mathbf{P}(B_k) \\
\le\ & C'\mathbf{P}(B_k)\Big(k+1 - \log \mathbf{P}(B_k)\Big).
\end{aligned}$$

Thus,

$$\begin{aligned}
\sum_{k=0}^{n+1} \int_{B_k} \log\left(\sum_{j=k}^{n} c_{jk}|\xi_j|\right) \mathrm{d}\mathbf{P} \ &\le\ C' \sum_{k=0}^{n+1} q^k (1-q)(k+1 - k\log q - \log(1-q)) \\
&\le\ C' \sum_{k=0}^{\infty} q_1^k (k+1 - \log(1-q_1)) + C' \left(\log \frac{1}{q}\right) \sum_{k=0}^{\infty} k q^k \\
&\le\ C' + C' \left(\log \frac{1}{q}\right) \frac{q}{(1-q)^2} \\
&\le\ C' + C' \left(\log \frac{1}{q_1}\right) \frac{q_1}{(1-q_1)^2}.
\end{aligned}$$

This proves (37) and completes the proof.

□

6.2. **Justification of** (7)**.** Let C_0 as in the proof of Theorem 3. By Remark 18,

$$|\mathbf{E}N_n I - \mathbf{E}N_{n,N(0,1)} I| \le {C_0}^{-\epsilon} \le 1,$$

where I is any subinterval of $[1 - \frac{1}{C_0}, 1]$.

Let C be any number greater than C_0, and let $I = [1 - \frac{1}{C_0}, 1 - \frac{1}{C})$, then

$$|\mathbf{E}N_n I - \mathbf{E}N_{n,N(0,1)} I| \le 1.$$

Combining this with the bound in (6) for C_0, we obtain

$$\mathbf{E}N_n[0, 1 - \frac{1}{C}) \le \mathbf{E}N_{n,N(0,1)} I + M(C_0) + 1 \le \mathbf{E}N_{n,N(0,1)}[0, 1 - \frac{1}{C}) + M(C_0) + 1.$$

Now, by the Edelman-Kostlan formula (see [7]),

$$\begin{aligned}\mathbf{E}N_{n,N(0,1)}[0,1-\frac{1}{C}) &= \frac{1}{\pi}\int_0^{1-\frac{1}{C}}\sqrt{\frac{1}{(1-x^2)^2}-\frac{(n+1)^2x^{2n}}{(1-x^{2n+2})^2}}\mathrm{d}x \\ &\le \frac{1}{\pi}\int_0^{1-\frac{1}{C}}\frac{1}{1-x^2}\mathrm{d}x = \frac{1}{2\pi}\left(\log C+\log\left(2-\frac{1}{C}\right)\right) \\ &\le \frac{1}{2\pi}\log C + 1.\end{aligned}$$

Thus,

$$\mathbf{E}N_n[0,1-\frac{1}{C}) \le \frac{1}{2\pi}\log C + M(C_0) + 2.$$

This proves (7).

References

[1] L. Ahlfors, Complex analysis. An introduction to the theory of analytic functions of one complex variable, *International Series in pure and applied Mathematics* (3rd ed.), Dsseldorf: McGraw Hill, 1979.

[2] L. Blum, F. Cucker, M. Shub and S. Smale, Complexity and Real Computation, *Springer-Verlag*, New York, 1998.

[3] A. T. Bharucha-Reid, M. Sambandham, Random polynomials, *Probability and Mathematical Statistics*, Academic Press, Inc., Orlando, Fla., 1986.

[4] A. Bloch, G. Polya, On the roots of certain algebraic equations, *Proc. London Math. Soc.* **33**(1932), 102–114.

[5] P. Erdős, Some of my favorite problems and results, page 51-70, The mathematics of Paul Erdős 1, edited by R. Graham, J. Nesetril and S. Butler, Springer, 2013.

[6] P. Erdös, A. C. Offord, On the number of real roots of a random algebraic equation, *Proc. London Math. Soc.* **6** (1956), 139–160.

[7] A. Edelman, E. Kostlan, How many zeros of a random polynomial are real?, *Bull. Amer. Math. Soc.* (N.S.) **32** (1995), 1–37. Erratum: *Bull. Amer. Math. Soc.* (N.S.) **33** (1996), 325.

[8] T. Erdélyi, Extensions of the Bloch-Pólya theorem on the number of real zeroes of polynomials, *J. Théor. Nombres Bordeaux* **20** (2008), no. 2, 282—287.

[9] K. Farahmand, Topics in random polynomials, *Pitman research notes in mathematics series* 393. Longman, Harlow, 1998.

[10] I. A. Ibragimov, N. B. Maslova, The average number of zeros of random polynomials, *Vestnik Leningrad. Univ.* **23** (1968), 171–172.

[11] I. A. Ibragimov, N. B. Maslova, The mean number of real zeros of random polynomials. I. Coefficients with zero mean, *Theor. Probability Appl.* **16** (1971), 228–248.

[12] I. A. Ibragimov, N. B. Maslova, The mean number of real zeros of random polynomials. II. Coefficients with a nonzero mean., *Theor. Probability Appl.* **16** (1971), 485–493.

[13] I. A. Ibragimov, N. B. Maslova, The average number of real roots of random polynomials, *Soviet Math. Dokl.* **12** (1971), 1004–1008.

[14] M. Kac, On the average number of real roots of a random algebraic equation, *Bull. Amer. Math. Soc.* **49** (1943) 314–320.

[15] M. Kac, On the average number of real roots of a random algebraic equation. II. *Proc. London Math. Soc.* 50, (1949), 390–408.

[16] M. Kac, Probability and related topics in physical sciences. Lectures in Applied Mathematics. Proceedings of the Summer Seminar, Boulder, Colo., 1957, Vol. I Interscience Publishers, London-New York, 1959.

[17] J. E. Littlewood and A. C. Offord, On the number of real roots of a random algebraic equation. II. *Proc. Cambridge Philos. Soc.* **35**, (1939), 133–148.

[18] J. E. Littlewood and A. C. Offord, On the number of real roots of a random algebraic equation. III. *Rec. Math. [Mat. Sbornik] N.S.* **54**, (1943), 277–286.
[19] J. E. Littlewood, A. C. Offord, On the distribution of the zeros and a-values of a random integral function. II., *Ann. Math.* **49** (1948), 885–952. Errata, **50** (1949), 990–991.
[20] N. B. Maslova, The variance of the number of real roots of random polynomials. *Teor. Vero- jatnost. i Primenen.* **19** (1974), 36-51.
[21] N. B. Maslova, The distribution of the number of real roots of random polynomials. *Theor. Probability Appl.* **19** (1974), 461-473.
[22] Stevens, D. C. The average number of real zeros of a random polynomial. *Comm. Pure Appl. Math.* **22** (1969), 457–477.
[23] T. Tao and V. Vu, Local universality of zeros of random polynomials, submitted.
[24] Todhunter, I. A history of the mathematical theory of probability, Stechert, New York, 1931.

Department of Mathematics, The Ohio State University, 231 West 18th Avenue, Columbus, OH 43210

E-mail address: nguyen.1261@math.osu.edu

Department of Mathematics, Yale University, New Haven, CT 06520, USA

E-mail address: oanh.nguyen@yale.edu

Department of Mathematics, Yale University, New Haven , CT 06520, USA

E-mail address: van.vu@yale.edu