Journal of Theoretical Probability (2019) 32:1076–1104
https://doi.org/10.1007/s10959-018-0839-8

Low-Degree Factors of Random Polynomials

Sean O'Rourke[1] · Philip Matchett Wood[2]

Received: 12 June 2017 / Revised: 21 May 2018 / Published online: 23 June 2018

Abstract
We study the probability that a monic polynomial with integer coefficients has a low-degree factor over the integers, which is equivalent to having a low-degree algebraic root. It is known in certain cases that random polynomials with integer coefficients are very likely to be irreducible, and our project can be viewed as part of a general program of testing whether this is a universal behavior exhibited by many random polynomial models. Our main result shows that pointwise delocalization of the roots of a random polynomial can be used to imply that the polynomial is unlikely to have a low-degree factor over the integers. We apply our main result to a number of models of random polynomials, including characteristic polynomials of random matrices, where strong delocalization results are known.

Keywords Random polynomials · Irreducible · Random matrices · Delocalization

Mathematics Subject Classification (2010) 11C08 · 15B52

1 Introduction

Consider the following question: Is it true that a random monic polynomial with integer coefficients is irreducible with high probability? For example, a version of Hilbert's irreducibility theorem[1] states that if $h_{n,N}$ is a monic polynomial in one variable of fixed

[1] See [57] for a modern formulation of Hilbert's irreducibility theorem.

Philip Matchett Wood was partially supported by National Security Agency (NSA) Young Investigator Grant Numbers H98230-14-1-0149 and H98230-16-1-0301..

✉ Philip Matchett Wood
pmwood@math.wisc.edu

Sean O'Rourke
sean.d.orourke@colorado.edu

[1] Department of Mathematics, University of Colorado at Boulder, Boulder, CO 80309, USA

[2] Department of Mathematics, University of Wisconsin-Madison, 480 Lincoln Dr., Madison, WI 53706, USA

degree n where all coefficients except the degree n coefficient are chosen independently and uniformly at random from among all integers in the interval $[-N, N]$, then the probability that $h_{n,N}$ is irreducible approaches 1 in the limit as $N \to \infty$. This was first proved by van der Waerden in 1934 [54], and in fact, the probability that $h_{n,N}$ is reducible is of order $1/N$, which was proven by van der Waerden two years later [55]. (The existence and value of the limiting constant was determined by Chela [9] in 1963 in terms of the Riemann zeta function.) Van der Waerden [54,55] also showed that, with probability tending to 1, the Galois group of the random polynomial $h_{n,N}$ is the full symmetric group $\mathfrak{S}_n$ on n elements (which implies irreducibility) as $N \to \infty$. Estimates for the exact order for the probability that the Galois group is not $\mathfrak{S}_n$ have been improved since van der Waerden, first in 1955 and 1956 by Knobloch [29,30], then in 1973 by Gallagher [20] who applied the large sieve, followed by more recent progress in 2010 by Zwina [57], in 2013 by Dietmann [14], and in 2015 by Rivin [44]. (See also [10,11,56] and references therein.)

How the random polynomial is generated matters, and there is a general heuristic that if the random integer coefficients are generated so that "elementary" factorizations are avoided—for example, one ensures that the constant coefficient is not likely to be zero, in which case x would be a factor of the polynomial $f(x)$—then the polynomial is very likely to be irreducible. One can think of this heuristic as suggesting a kind of universality (see, for example, [6, Heuristic 1.1]), and in some specific instances, it has been conjectured that the behavior in Hilbert's irreducibility theorem extends to different settings, including when the degree n is growing. For example, one can define a random polynomial g_n where the constant coefficient and the degree n coefficient are equal to 1, and all other coefficients are 0 or 1 independently with probability $1/2$. In the limit as the degree n goes to infinity (in contrast to the degree being fixed in Hilbert's irreducibility theorem and the results discussed above) it has been conjectured that, once again, the probability that g_n is irreducible approaches one as $n \to \infty$. (See [28,37].)

The question of proving irreducibility in the case where the degree of the random polynomial tends to infinity and the support of the coefficients remains bounded (or bounded by a function of the degree) seems to be quite challenging. For example, in the specific case of the polynomials g_n described above, the current best result (due to Konyagin [28]) shows that the probability is bounded below by $c/\log n$, where c is a positive constant, and as far as the authors know, there is not a result showing that the probability that g_n is irreducible remains bounded away from zero as the degree increases, even though this probability is conjectured to approach 1. (Interestingly, Bary-Soroker and Kozma [4] have proven that bivariate polynomials with independent ± 1 do become irreducible with high probability as the degree increases, though the approach does not extend to a single-variable polynomial like g_n.) One key step in Konyagin's result [28] is showing that g_n is unlikely to have a factor over the integers with degree up to $cn/\log n$, which is step toward proving irreducibility; note that showing that there is no factor over the integers of degree up to $n/2$ would prove irreducibility for a degree n polynomial.

In the current note, we show that the phenomenon of random polynomials having no factors over the integers with small degree is quite general, and in fact can be implied by pointwise delocalization of the roots of the random polynomial. Generally speaking, we show that, for a random monic polynomial f with integer coefficients, if $\sup_{z\in\mathbb{C}} \mathbb{P}(f(z) = 0)$ is sufficiently small, then the probability of a low-degree factor over the integers is also small. We refer to the quantity $\sup_{z\in\mathbb{C}} \mathbb{P}(f(z) = 0)$ being small as *pointwise delocalization*. In particular, pointwise delocalization rules out the possibility that f has a deterministic (or near deterministic) root. More generally, pointwise delocalization can be viewed as measuring the probability that f has some "elementary" factorization. For instance, $\mathbb{P}(f(0) = 0)$ is the probability that z is a factor of $f(z)$.

Our main result provides useful bounds for random polynomials with correlated and highly dependent coefficients, because pointwise delocalization is a statement about the roots, rather than the coefficients. This is particularly useful, for example, when studying the characteristic polynomial of a random matrix: The coefficients are typically dependent and correlated, but often more is known about the roots, which are the eigenvalues of the matrix.

When f is the characteristic polynomial of a square random matrix, we can often show that the pointwise delocalization condition holds by using sufficiently general results which bound the probability that the matrix is singular or has a very small singular value. In Sect. 2, we consider various models of random polynomials and random matrices for which good pointwise delocalization results are known. For example, we show that for any $\epsilon > 0$ and for an n by n random matrix with each entry $+1$ or -1 independently with probability $1/2$, the characteristic polynomial factors over the integers with a factor of degree at most $n^{1/2-\epsilon}$ with probability at most $\left(\frac{1}{\sqrt{2}} + o(1)\right)^n$. (See Theorem 2.4.)

We begin by fixing some terminology and notation. If F is a field, a polynomial with coefficients in F is *irreducible over* F if the polynomial is nonconstant and cannot be factored into the product of two nonconstant polynomials with coefficients in F. More generally, a polynomial with coefficients in a unique factorization domain R (for example, the integers) is said to be *irreducible over* R if it is an irreducible element of the polynomial ring $R[x]$, meaning that the polynomial is nonzero, is not invertible, and cannot be written as the product of two noninvertible polynomials with coefficients in R. Irreducibility of a polynomial over a ring R generalizes the definition given for the case of coefficients in a field because, in the field case, the nonconstant polynomials are exactly the polynomials that are noninvertible and nonzero. We say f is *reducible over* R if f is not irreducible over R.

Recall that an *algebraic number* is a possibly complex number that is a root of a finite, nonzero polynomial in one variable with rational coefficients (or equivalently, by clearing the denominators, with integer coefficients). Given an algebraic number α, there is a unique monic polynomial with rational coefficients of least degree that has the number as a root. This polynomial is called the *minimal polynomial* for α, and if α is a root of a polynomial f with rational coefficients, then the minimal polynomial for α divides f over the rationals. If the minimal polynomial has degree k, then the algebraic number α is said to be of degree k. For instance, an algebraic number of degree one is a rational number. An *algebraic integer* is an algebraic number that is a root of a polynomial with integer coefficients with leading coefficient 1 (a monic polynomial). The question of whether a monic polynomial f with integer coefficients has an irreducible degree k factor when factored over the rationals is thus equivalent to whether f has a root α that is an algebraic number of degree k; in fact, by Gauss's lemma (see for instance [16]), f being monic implies that α is an algebraic integer.

Let f be a polynomial of degree n over $\mathbb{C}$. We let $\lambda_1(f), \ldots, \lambda_n(f) \in \mathbb{C}$ denote the zeros (counted with multiplicity) of f, and we define

$$\Lambda(f) := \{\lambda_1(f), \ldots, \lambda_n(f)\} \tag{1.1}$$

to be the set of zeros of f.

1.1 Models of Random Monic Polynomials with Integer Coefficients

As mentioned above, there are many ensembles of random polynomials. We begin with the most general ensemble of random monic polynomials with integer coefficients.

Definition 1.1 (*Random monic polynomial*) We say $f(z) := z^n + \xi_{n-1}z^{n-1} + \cdots + \xi_1 z + \xi_0$ is a degree n *random monic polynomial with integer coefficients* if $\xi_{n-1}, \ldots, \xi_0$ are integer-valued random variables (not necessarily independent).

We emphasize that the integer-valued random variables $\xi_{n-1}, \ldots, \xi_0$ are not assumed to be independent or identically distributed. There are many examples of such random polynomials.

Example 1.2 (Independent Rademacher coefficients) Let $\xi_0, \ldots, \xi_{n-1}$ be independent Rademacher random variables, which take the values $+1$ or -1 with equal probability. Then $f(z) := z^n + \xi_{n-1}z^{n-1} + \cdots + \xi_1 z + \xi_0$ is a random monic polynomial with integer coefficients. More generally, one can consider the case when $\xi_0, \ldots, \xi_{n-1}$ are independent and identically distributed (iid) copies of an integer-valued random variable (not necessarily Rademacher); see Example 1.3 below for one such example.

Example 1.3 (Independent uniform coefficients) Let $N \in \mathbb{N}$ be a given parameter. Let $\xi_0, \ldots, \xi_{n-1}$ be independent and identically distributed (iid) random variables uniformly distributed on the discrete set $\{0, 1, \ldots, N\}$. Then $f(z) := z^n + \xi_{n-1}z^{n-1} + \cdots + \xi_1 z + \xi_0$ is a random monic polynomial with integer coefficients.

Example 1.4 (Characteristic polynomial of random matrices) Let ξ be an integer-valued random variable, and let $\mathbf{X}$ be an $n \times n$ random matrix whose entries are iid copies of ξ. Then the characteristic polynomial $f(z) := \det(z\mathbf{I} - \mathbf{X})$ is a random monic polynomial with integer coefficients. Here, $\mathbf{I}$ denotes the identity matrix.

Example 1.5 (Random permutation matrices) Let π be a random permutation on $\{1, \ldots, n\}$ uniformly sampled from all $n!$ permutations. Let $\mathbf{P}_\pi$ denote the corresponding permutation matrix, i.e., the (i, j)-entry of $\mathbf{P}_\pi$ is one if $i = \pi(j)$ and zero otherwise. Clearly, $\mathbf{P}_\pi$ is an orthogonal matrix. The permutation π may be written as a product of ℓ disjoint cycles with lengths $c_1, \ldots, c_\ell$. Let f_π denote the characteristic polynomial of $\mathbf{P}_\pi$. Then, as can be seen by reordering the rows and columns of $\mathbf{P}_\pi$ so that it is block diagonal, we have

$$f_\pi(z) := \det(z\mathbf{I} - \mathbf{P}_\pi) = \prod_{j=1}^{\ell}(z^{c_j} - 1),$$

where $\mathbf{I}$ is the identity matrix. Clearly 1 is always a root of f_π, making $z - 1$ a factor and f_π reducible. In addition, f_π will have other (possibly repeated) factors as well if n is composite or if the number of cycles ℓ is at least 2. One way to measure randomness in the roots of a random polynomial is testing whether the polynomial has any double roots. For example, Tao and Vu [50] have shown that the spectrum of a random real symmetric n by n matrix with independent entries contains no double roots with probability tending to 1 as n increases. (See also [18,41] for a related question on another class of random polynomials.) For contrast, in the case of the characteristic polynomial of a random permutation matrix, the probability that the spectrum contains no double roots is the same as the probability of the permutation having only one cycle, which occurs with probability $1/n$ and tends to zero, rather than 1.

Example 1.6 (Erdős–Rényi random graphs) Let $G(n, p)$ be the Erdös–Rényi random graph on n vertices with edge density p. That is, $G(n, p)$ is a simple graph on n vertices (which we shall label as $\{1, \dots, n\}$) such that each edge $\{i, j\}$ is in $G(n, p)$ with probability p, independent of other edges. In the special case when $p = 1/2$, one can view $G(n, 1/2)$ as a random graph selected uniformly among all $2^{\binom{n}{2}}$ simple graphs on n vertices. The random graph $G(n, p)$ can be defined by its adjacency matrix $\mathbf{A}_n$, which is a real symmetric matrix with entry (i, j) equal to 1 if there is an edge between vertices i and j, and the entry equal to zero otherwise. It is widely believed (and numerical evidence suggests) that the characteristic polynomial of $\mathbf{A}_n$ is irreducible with probability tending to one as $n \to \infty$. We discuss this example more in Sects. 2.6 and 3.

We have chosen to focus on monic polynomials, but the question of irreducibility can also be asked for nonmonic random polynomials with integer coefficients (or equivalently, by dividing by the leading coefficient, for random monic polynomials with rational coefficients). For fixed-degree polynomials with independent coefficients, this question was addressed by Kuba [31]. When the degree tends to infinity, we again expect the answer to depend on the random polynomial model.

1.2 Main Results

In this paper, we focus on the algebraic degree of the roots of a random monic polynomial f.

Our main result below bounds above the probability that f has an algebraic root of degree k, for some given value of $1 \leq k \leq n$, which is related to the question of irreducibility since a monic polynomial with integer coefficients is irreducible if and only if its roots are all algebraic of degree n. We expect many random monic polynomial models to yield irreducible polynomials with high probability, and so intuitively, algebraic roots of small degree should be rare.

Theorem 1.7 *Let f be a degree n random monic polynomial with integer coefficients (as in Definition 1.1). Let $M > 0$ and $2 \leq k \leq n$. Take $\Omega \subseteq \{z \in \mathbb{C} : |z| \leq M\}$, and suppose there exists $p \in [0, 1]$ such that*

$$\sup_{z \in \Omega} \mathbb{P}(f(z) = 0) \leq p \tag{1.2}$$

(In other words, pointwise delocalization holds on Ω.) Then, the probability that f has an algebraic root of degree at most k in Ω is at most

$$p(eM)^{k^2} + \mathbb{P}(|\lambda_i(f)| > M \textit{ for some } i), \tag{1.3}$$

where $\lambda_1(f), \ldots, \lambda_n(f)$ are the roots of f. If $k = 1$, the result holds if $p(eM)^{k^2}$ is replaced with $p(3M)$ in (1.3).

For Theorem 1.7 to be useful, one needs to show that bound (1.3) is small. In Lemma 1.8 we collect bounds on $p(eM)^{k^2}$ that hold for specific random polynomial models that we will discuss in Sect. 2.

Lemma 1.8 *We have the following bounds on $p(eM)^{k^2}$ for various values of p (the pointwise delocalization parameter), M (the radius containing Ω), and k (the degree).*

(i) If $p = O(1/\sqrt{n})$ and $M = 2$ and $k \leq \sqrt{\frac{\log n}{4}}$, then $p(eM)^{k^2} = o(1)$.

(ii) If $p = \left(\frac{1}{\sqrt{2}} + o(1)\right)^n$ and $M = n$ and $k = n^{1/2-\epsilon}$ for some $\epsilon > 0$, then $p(eM)^{k^2} = \left(\frac{1}{\sqrt{2}} + o(1)\right)^n$. (The two $o(1)$ terms differ.)

(iii) If $p = 2e^{-n^c}$ for some $0 < c < 1$, $M = C\sqrt{n}$ for some $C > 0$, and $k \leq n^{c'}$ for $c' < c/2$, then $p(eM)^{k^2} \leq 2\exp\left(-\left(\frac{2}{3}\right)n^c\right)$ for sufficiently large n.

(iv) Let $B > 0$ and $m \geq 1$, and take $M = n^m$ and $k \geq 1$ constant. Then there exists $B' > 0$ (depending only on B, m, and k) such that if $p = n^{-B'}$, then $p(eM)^{k^2} \leq n^{-B}$ for sufficiently large n.

1.3 Random Polynomials Over Finite Fields

There are, of course, many other ensembles of random polynomials one can consider. For instance, one can study monic polynomials over the finite field $\mathbb{F}_q$, where q is a power of a prime. Indeed, there are q^n monic polynomials of degree n over $\mathbb{F}_q$, and we can consider selecting one uniformly at random. Using Galois theory for finite fields and Möbius inversion (see [16, Section 14.3]), one can show that the number of degree n irreducible polynomials over $\mathbb{F}_q$ is

$$\frac{1}{n}\sum_{d|n} \mu(d) q^{n/d},$$

where μ is the Möbius function. Thus, the probability that a randomly selected degree n monic polynomial over $\mathbb{F}_q$ is irreducible is

$$\frac{1}{nq^n}\sum_{d|n}\mu(d)q^{n/d}=\frac{1}{n}+O(q^{-n/2}),$$

(using the coarse bound $|\mu(d)|\leq 1$) for any n and q. Thus, in a finite field, a degree n polynomial chosen uniformly at random is irreducible only with probability close to $1/n$. This contrasts sharply with the case of polynomials over the integers, where Hilbert's irreducibility theorem shows that at randomly chosen polynomial is very likely to be irreducible. (See, for example, [57].)

1.4 Overview and Outline

The paper is organized as follows. In Sect. 2, we give some example applications of our main results, including the cases of random polynomials with iid coefficients, the characteristic polynomial of random matrices (nonsymmetric, nonsymmetric sparse, symmetric, and elliptical), and adjacency matrices of random graphs (directed, undirected, and fixed outdegree). Often we will consider the case where the underlying random variables are Rademacher ±1 for simplicity. Section 3 motivates the model of random polynomials studied in this paper by illustrating a connection that exists between irreducible random polynomials, random graphs, and control theory on large-scale graphs and networks. Theorem 1.7 and Lemma 1.8 are proven in Sect. 4. Finally, Sect. 5 contains the proof for one of the applications discussed in Sect. 2.

1.5 Notation

We use asymptotic notation (such as O, o) under the assumption that $n\to\infty$. In particular, $o(1)$ denotes a term which tends to zero as $n\to\infty$. Let $[n]:=\{1,\dots,n\}$ denote the discrete interval. We let $\sqrt{-1}$ denote the imaginary unit and reserve i as an index. For a finite set S, we use $|S|$ to denote the cardinality of S. For a vector v, we use $\|v\|$ for the Euclidean norm. We let $u^{\mathrm{T}}v=u\cdot v$ denote the dot product between two vectors $u, v\in\mathbb{R}^n$. For a matrix $\mathbf{A}$, we let $\|\mathbf{A}\|$ denote the spectral norm, i.e., $\|\mathbf{A}\|$ is the largest singular value of $\mathbf{A}$. We let $\mathbf{I}_n$ denote the $n\times n$ identity matrix; often we will drop the subscript n when its size can be deduced from context. For a polynomial f, $\deg(f)$ denotes the degree of f.

2 Example Applications of the Main Results

We now specialize Theorem 1.7 to some specific examples.

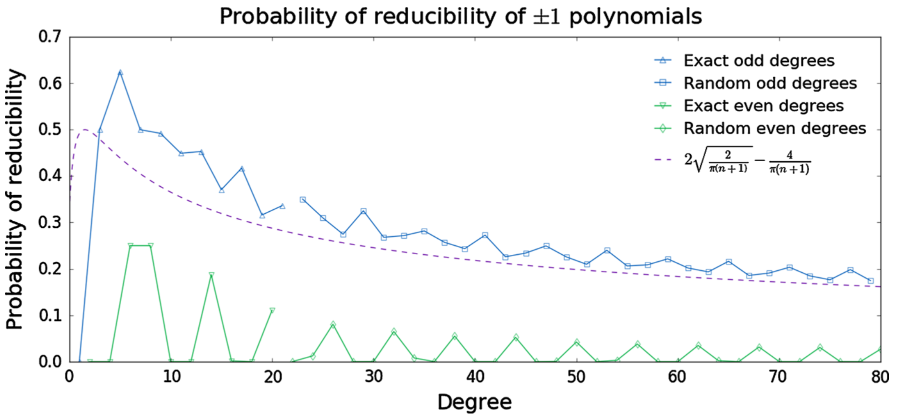

Fig. 1 Quoted from [6, Figure 3], the above shows the probability that $f_n(x) = x^n + \xi_{n-1}x^{n-1} + \cdots + \xi_1 x + \xi_0$ is irreducible, where the ξ_i are $+1$ or -1 independently with probability $1/2$. For degree up to $n = 21$, the probability was computed exactly by exhaustively generating all 2^n polynomials of the specified degree and checking each one for reducibility using the `IsIrreducible()` function in Magma. For degree 22 up to 80, the probability was estimated (again using Magma) by generating 150,000,000 random polynomials for each degree. The curve $2\sqrt{\frac{2}{\pi(n+1)}} - \frac{4}{\pi(n+1)}$ is an asymptotic lower bound for the probability of reducibility when the degree is odd. Figure produced by Borst et al. (see [6])

2.1 Random Polynomials with iid Coefficients

We now consider Example 1.2, where the coefficients of f are iid random variables.

Theorem 2.1 (Random polynomials with iid coefficients) *For each $n \geq 1$, let $f_n(z) = z^n + \xi_{n-1}z^{n-1} + \cdots + \xi_1 z + \xi_0$, where $\xi_0, \xi_1, \ldots$ are iid Rademacher random variables, which take the values $+1$ or -1 with equal probability. Then the probability that $f_n(x)$ has an algebraic root of degree at most $\frac{n^{1/3}}{\log^3 n}$ is at most $O\left(\frac{1}{\sqrt{n}}\right)$.*

Remark 2.2 Note that a weaker version of Theorem 2.1 follows easily from Theorem 1.7. In particular, by Lemma 5.2 all roots for f_n have absolute value between $1/2$ and 2 and by the Littlewood–Offord theorem (see, e.g., [47, Corollary 7.8]) $\mathbb{P}(f_n(z) = 0) \leq O(1/\sqrt{n})$ for any z. Thus, Lemma 1.8(i) combined with Theorem 1.7 implies that f_n has no algebraic roots of degree at most $\sqrt{\frac{\log n}{4}}$ with probability tending to 1 as n tends to infinity.

We present a proof of Theorem 2.1 in Sect. 5, and below we will comment on potential generalizations of Theorem 2.1 and its connections to the work of Konyagin [28]. See Fig. 1 for numerical evidence suggesting that, in fact, the probability that f_n is reducible goes to zero as $n \to \infty$.

Beyond Theorem 2.1, our methods can also be used when $\xi_0, \xi_1, \ldots$ are more general iid integer-valued random variables satisfying some technical assumptions. However, a number of complications can arise in this case [e.g., zero is always a root of f_n with probability $\mathbb{P}(\xi_0 = 0)$], and so we focus on the Rademacher ± 1 case for simplicity.

In [28], Konyagin studies the random degree n polynomial g_n which has 1 for the constant coefficient and the degree n coefficient, and every other coefficient is 0 or 1 independently with equal probability. In particular, he shows that there are constants $c, C > 0$ such that g_n has a root that is an algebraic number with degree at most $cn/\log n$ with probability at most $C/\sqrt{n}$. Konyagin's approach in [28] can also be adapted to more general distributions of the random integer coefficients (see forthcoming work of Terlov [51]); however, the method seems to require independence of the coefficients, whereas an application of Theorem 1.7 would allow for dependence, though at the expense of a weaker bound on the size of the low-degree factors.

Finally, one should note that elementary Galois theory can be used to prove that if $n + 1$ is prime and 2 generates the multiplicative group $\left(\mathbb{Z}/(n+1)\right)^\times$, then *every* random polynomial of degree n with coefficients iid Rademacher ± 1 random variables (as in Theorem 2.1) is in fact irreducible.[2] One can prove this by considering the polynomials modulo 2, in which case $+1 = -1$ mod 2 and every polynomial is equal to $x^n + x^{n-1} + x^{n-2} + \cdots + 1$ (i.e., there is no randomness); thus every root of the polynomial modulo 2 must be a $(n+1)$-st root of unity. To complete the argument, one can use the fact that $\mathbb{F}_{2^n}$ has cyclic multiplicative group and the fact that the Galois group $\mathrm{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2)$ is also cyclic and generated by the Frobenius endomorphism $x \mapsto x^2$. (See [16].) Interestingly, letting $p = n + 1$ be a prime, Artin's conjecture on primitive roots would imply that 2 should generate $(\mathbb{Z}/(p))^\times = \left(\mathbb{F}_p\right)^\times$ for infinitely many p, and in fact, the proportion of primes for which 2 generates $\left(\mathbb{F}_p\right)^\times$ should asymptotically approach Artin's constant, which is approximately $0.3739558136\ldots$. (See the survey [32].)

2.2 Random Matrices with iid Rademacher ± 1 Entries

While delocalization estimates for random polynomials with iid coefficients are fairly weak, we now consider random matrices with independent entries, for which much better delocalization bounds are known. Indeed, we will use the following theorem from [7] to bound the supremum in (1.2).

Theorem 2.3 (Bourgain–Vu–Wood, Corollary 3.3 in [7]) *Let q be a constant such that $0 < q \leq 1$ and let $S \subset \mathbb{C}$ be a set with cardinality $|S| = O(1)$. If $\mathbf{M}_n$ is an n by n matrix with independent random entries taking values in S such that for any entry x_{ij}, we have $\max_{s \in S} \mathbb{P}(x_{ij} = s) \leq q$, then*

$$\mathbb{P}(\mathbf{M}_n \textit{ is singular}) \leq \left(\sqrt{q} + o(1)\right)^n .$$

Furthermore, by inspecting the proof one can see that the $o(1)$ error term depends only on q and the cardinality of the set S, and not on the values in the set S.

In [7], it was shown using the above result that an iid random Rademacher ± 1 matrix (i.e., where each entry is $+1$ or -1 independently with probability 1/2) is

[2] We thank Melanie Matchett Wood for describing the formulation and proof of this result.

very unlikely to have a rational eigenvalue. Our result below extends this fact by showing that, for any $\epsilon > 0$, an eigenvalue that is algebraic with degree at most $n^{1/2-\epsilon}$ (which includes all rational numbers) is similarly unlikely. Our approach here does not extend to algebraic degree $\sqrt{n}$ or larger; however, in analogy with Hilbert's irreducibility theorem and related results described in introduction above, it seems likely that the characteristic polynomial of an iid random Rademacher ± 1 matrix is in fact irreducible with high probability, which would imply that the matrix has no algebraic roots of degree less than n. (See [6] for supporting data.)

Theorem 2.4 *Let $\epsilon > 0$ be a constant, and let $\mathbf{M}_n$ be an n by n matrix where each entry takes the value $+1$ or -1 independently with probability $1/2$. Then, the probability that $\mathbf{M}_n$ has an eigenvalue that is an algebraic number with degree at most $n^{1/2-\epsilon}$ is bounded above by $\left(\frac{1}{\sqrt{2}} + o(1)\right)^n$.*

Proof Let f be the characteristic polynomial of $\mathbf{M}_n$, so that the eigenvalues of $\mathbf{M}_n$ are the roots of f, all eigenvalues of $\mathbf{M}_n$ have absolute value at most n with probability 1 by an elementary bound. (In fact, the eigenvalues of M_n are all less than $O(\sqrt{n})$ with exponentially high probability using, for example, [46, Proposition 2.4]; we will not need such a refined bound here.)

Let $\Omega := \{z \in \mathbb{C} : |z| \leq n\}$. Using Theorem 2.3 above, we have for any $z \in \mathbb{C}$ that

$$\mathbb{P}(f(z) = 0) = \mathbb{P}(\mathbf{M}_n - z\mathbf{I}_n \text{ is singular}) \leq \left(\frac{1}{\sqrt{2}} + o(1)\right)^n, \tag{2.1}$$

where the $o(1)$ error is uniform for all $z \in \mathbb{C}$. (This follows using the facts that $\{1, -1, 1 - z, -1 - z\}$ is the set of values that can appear in $\mathbf{M}_n - z\mathbf{I}_n$ and that the cardinality of this set and the value of $q = 1/2$ are the same for any $z \in \mathbb{C}$.) Thus,

$$\sup_{z\in\Omega} \mathbb{P}(f(z) = 0) \leq \left(\frac{1}{\sqrt{2}} + o(1)\right)^n.$$

We now apply Lemma 1.8(ii) and Theorem 1.7 to complete the proof. □

2.3 Random Symmetric Matrices

In [52], Vershynin proves a general result for real symmetric random matrices bounding the singularity probability, quantifying the smallest singular value, and showing that the spectrum is delocalized with the optimal scale. Here, we will use the following special case showing only pointwise delocalization to illustrate an application of Theorem 1.7.

Theorem 2.5 (Vershynin, following from Theorem 1.2 in [52]) *Let $B > 0$ be a real constant and let $\mathbf{M}_n$ be a real symmetric n by n matrix whose entries x_{ij} on and above the diagonal (so for $i \leq j$) are iid random variables with mean zero and unit variance satisfying $|x_{ij}| \leq B$. Then, there exists an absolute constant $c > 0$ (depending only on B) such that, for every $r \in \mathbb{R}$,*

$$\mathbb{P}(r \textit{ is an eigenvalue of } \mathbf{M}_n) \leq 2e^{-n^c}. \tag{2.2}$$

It is natural to only consider real numbers r in (2.2) since real symmetric matrices have all real eigenvalues. Also, the constant c appearing in Theorem 2.5 is typically less than one and may be much smaller.

The more general version of the above result proven by Vershynin [52, Theorem 1.2] applies to real symmetric matrices with entries having subgaussian tails (see [53] for why bounded implies subgaussian), and the bound we will prove on the probability of having low-degree algebraic numbers as eigenvalues (Theorem 2.6 below) extends to this setting.

Theorem 2.6 *Let $B > 0$ be a real constant, let $c' > 0$ be an absolute constant satisfying $c' < c/2$, where $c < 1$ is the absolute constant from Theorem 2.5 (which depends only on B), and let $\mathbf{M}_n$ be an n by n real symmetric matrix whose entries on and above the diagonal are iid integer-valued random variables which are bounded in absolute value by B. Then the probability that $\mathbf{M}_n$ has an eigenvalue that is algebraic of degree at most $n^{c'}$ is bounded above by $e^{-n^c/2}$ for all sufficiently large n.*

Proof (Proof of Theorem 2.6) Let f be the characteristic polynomial of $\mathbf{M}_n$, so that the eigenvalues of $\mathbf{M}_n$ are the roots of f, and note that by [52, Lemma 2.3], all eigenvalues of $\mathbf{M}_n$ have absolute value at most $C\sqrt{n}$ with probability at least $1 - 2e^{-n}$ for some constant C (depending only on B).

Let $\Omega := \{r \in \mathbb{R} : |r| \leq C\sqrt{n}\}$. Since $\mathbf{M}_n$ is a real symmetric matrix, the eigenvalues of $\mathbf{M}_n$ are all real. Moreover, Theorem 2.5 implies that $\sup_{r\in\Omega} \mathbb{P}(f(r) = 0) \leq 2e^{-n^c}$. Thus, combining Theorem 1.7, Lemma 1.8(iii), and [52, Lemma 2.3]), we have that the probability that f has an algebraic root of degree at most $n^{c'}$ is bounded above by $2\exp(-\left(\frac{2}{3}\right)n^c) + 2e^{-n}$, which is at most $e^{-n^c/2}$ for all sufficiently large n. □

2.4 Elliptical Random Matrices

Elliptical random matrices interpolate between iid random matrices and random symmetric matrices. In an elliptical random matrix, all the entries are independent with the exception that the (i, j)-entry may depend on the (j, i)-entry, and one also requires that the correlation between the (i, j)-entry and the (j, i)-entry is a constant ρ for all $i \neq j$. Thus, if the matrix has iid entries, then $\rho = 0$, and if $\rho = 1$, the matrix is symmetric. There are results showing that the limiting distribution of the eigenvalues also interpolates between the limiting distributions for iid random matrices and for symmetric random matrices; in particular, for $-1 < \rho < 1$, the limiting eigenvalue distribution (suitably scaled) is an ellipse with eccentricity $\sqrt{1 - \frac{(1-\rho)^2}{(1+\rho)^2}}$; see Nguyen and O'Rourke [35] and Naumov [33].

To apply Theorem 1.7, we will use a result due to Nguyen and O'Rourke [35] bounding the smallest singular value, and we will focus on the special case of ±1 elliptical random matrices for simplicity. Let $\mathbf{M}_{n,\rho}$ be an elliptical random matrix with covariance parameter $-1 < \rho < 1$ with entries x_{ij} defined as follows: Let $\{x_{i,j} : i \leq j\} \cup \{\xi_{i,j} : i > j\}$ be a collection of independent random variables, where

$\mathbb{P}(x_{i,j} = 1) = \mathbb{P}(x_{i,j} = -1) = 1/2$ for $i \leq j$ and where

$$\xi_{i,j} := \begin{cases} 1 & \text{with probability } (1+\rho)/2 \\ -1 & \text{with probability } (1-\rho)/2, \end{cases}$$

for $i > j$. Then let $x_{i,j} := x_{j,i}\xi_{i,j}$ whenever $i > j$. Define

$$\mathbf{M}_{n,\rho} := \begin{pmatrix} x_{1,1} & x_{1,2} & x_{1,3} & \dots & x_{1,n} \\ x_{1,2}\xi_{2,1} & x_{2,2} & x_{2,3} & \dots & x_{2,n} \\ x_{1,3}\xi_{3,1} & x_{3,2}\xi_{3,2} & x_{3,3} & \dots & x_{3,n} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ x_{1,n}\xi_{n,1} & x_{2,n}\xi_{n,2} & \dots & x_{n-1,n}\xi_{n,n-1} & x_{n,n} \end{pmatrix},$$

and note that each entry takes the values $+1$ or -1 with equal probability. We will call $\mathbf{M}_{n,\rho}$ a *Rademacher elliptical random matrix with parameter* ρ.

Theorem 2.7 (Nguyen–O'Rourke, following from Theorem 1.9 in [35]) *Let* $\mathbf{M}_{n,\rho}$ *be an n by n Rademacher elliptical random matrix with parameter* $-1 < \rho < 1$*, and let* $B' > 0$ *be a constant. Then, for all sufficiently large n (depending only on* B' *and* ρ*), we have that*

$$\sup_{z\in\mathbb{C},\ |z|\leq n} \mathbb{P}(z \textit{ is an eigenvalue of } \mathbf{M}_{n,\rho}) \leq n^{-B'}.$$

We can now apply Theorem 1.7 to get the following result.

Theorem 2.8 *Let* $\mathbf{M}_{n,\rho}$ *be an n by n Rademacher elliptical random matrix with parameter* $-1 < \rho < 1$*, and let* $B > 0$ *and* $K \geq 1$ *be constants. Then, for all sufficiently large n (depending only on* B*,* ρ*, and* K*), the probability that the matrix* $\mathbf{M}_{n,\rho}$ *has an eigenvalue that is algebraic of degree at most* K *is bounded above by* n^{-B}*.*

Proof Let f be the characteristic polynomial of $\mathbf{M}_{n,\rho}$. All eigenvalues of $\mathbf{M}_{n,\rho}$ have absolute value at most n with probability 1 by an elementary bound. Let $\Omega := \{z \in \mathbb{C} : |z| \leq n\}$, and note that Theorem 2.7 lets us take $p = n^{-B'}$ for any constant $B' > 0$ in (1.2). Thus, we may apply Theorem 1.7 and Lemma 1.8(iv) (with $M = n$ and $m = 1$) to complete the proof. □

2.5 Product Matrices

We now show how Theorem 1.7 can be applied to products of independent random matrices. We begin with the following result from [38].

Theorem 2.9 (O'Rourke–Renfrew–Soshnikov–Vu, [38] Theorem 5.2) *Let* $m \geq 1$ *and* $B', \gamma > 0$ *be constants. Let* $\mathbf{M}_n^{(1)}, \dots, \mathbf{M}_n^{(m)}$ *be independent n by n matrices in which each entry takes the value* $+1$ *or* -1 *independently with probability* $1/2$*. Define the product*

$$\mathbf{M}_n := \mathbf{M}_n^{(1)} \cdots \mathbf{M}_n^{(m)}.$$

Then, for all sufficiently large n (depending only on m, B', and γ), we have

$$\sup_{z\in\mathbb{C},\ |z|\le n^{\gamma}} \mathbb{P}\left(z \textit{ is an eigenvalue of } \mathbf{M}_n\right) \le n^{-B'}.$$

We can now apply Theorem 1.7 to get the following result.

Theorem 2.10 *Let $K, m \ge 1$, and $B > 0$ be constants. Let $\mathbf{M}_n^{(1)}, \dots, \mathbf{M}_n^{(m)}$ be independent n by n matrices in which each entry takes the value $+1$ or -1 independently with probability $1/2$. Then, for all sufficiently large n (depending only on m, K, and B), the probability that the matrix*

$$\mathbf{M}_n := \mathbf{M}_n^{(1)} \cdots \mathbf{M}_n^{(m)}$$

has an eigenvalue that is algebraic of degree at most K is bounded above by n^{-B}.

Proof Let f be the characteristic polynomial of $\mathbf{M}_n$, and note that all eigenvalues of $\mathbf{M}_n$ have absolute value at most n^m with probability 1 by an elementary bound. Let $\Omega := \{z \in \mathbb{C} : |z| \le n^m\}$, and note that by Theorem 2.9 we can take $p = n^{-B'}$ for any constant $B' > 0$ in (1.2). Thus, we may apply Theorem 1.7 and Lemma 1.8(iv) (with $M = n^m$) to complete the proof. □

More generally, Theorem 2.9 can be extended to products of elliptical random matrices which satisfy a number of constraints. (See [38, Theorem 5.2] for details.) This leads naturally to a version of Theorem 2.10 for the product of m independent Rademacher elliptical random matrices with parameters $\rho_1, \dots, \rho_m$ satisfying $-1 < \rho_i < 1$.

2.6 Erdos–Rényi Random Graphs

We now consider Erdős–Rényi random graphs on n vertices, where each edge is present independently at random with a constant probability p satisfying $0 < p < 1$. We denote such a graph by $G(n, p)$ and observe that the graph can be defined by its adjacency matrix $\mathbf{A}_n$, which is a real symmetric matrix with entry (i, j) equal to 1 if there is an edge between vertices i and j, and entry equal to zero otherwise.

In the Erdős–Rényi model, the independence among edges means that all entries in the strict upper triangle of $\mathbf{A}_n$ are also independent. Thus, the following result due to Nguyen [34] is applicable.

Theorem 2.11 (Nguyen, following from Theorem 1.4 in [34]) *Let $0 < p < 1$ and $B' > 0$ be constants, and let $\mathbf{A}_n$ be the adjacency matrix of $G(n, p)$. Then, for n sufficiently large (depending only on p and B'),*

$$\sup_{z\in\mathbb{C},\ |z|\le n} \mathbb{P}(z \textit{ is an eigenvalue of } \mathbf{A}_n) \le n^{-B'}.$$

By following the proof of Theorem 2.8 and applying Theorem 2.11 in place of Theorem 2.7, we find that for any $K \geq 1$ and $B > 0$, the probability that $\mathbf{A}_n$ has an eigenvalue that is algebraic of degree at most K is bounded above n^{-B} for n sufficiently large (depending only on K, B, and p). We state this result explicitly in Sect. 3. (See Theorem 3.9.) The result is also true when the diagonal entries of $\mathbf{A}_n$ are allowed to be one. (This corresponds to the case where loops are allowed in the graph.)

2.7 Directed Random Graphs

In the case of directed random graphs where directed edges (including loops) are included independently at random with probability p, where $0 < p < 1$ is a constant, the adjacency matrix $\mathbf{M}_n$ is an n by n matrix with entries independently equal to 1 with probability p, and otherwise the entries are zero. In this case, Theorem 2.3 applies with $q := \max\{p, 1-p\}$, and thus, following the proof of Theorem 2.4, proves that for any $\epsilon > 0$, the probability that $\mathbf{M}_n$ has an eigenvalue that is an algebraic number with degree at most $n^{1/2-\epsilon}$ is bounded above by $\left(\sqrt{q} + o(1)\right)^n$.

2.8 Directed Random Graphs with Fixed Outdegrees

Let s be a positive integer, and let $x \in \{0,1\}^n$ be a random binary vector uniformly chosen from among all binary vectors containing exactly s ones. If $\mathbf{M}_n$ is the $n \times n$ matrix whose rows are iid copies of the vector x, then $\mathbf{M}_n$ can be viewed as the adjacency matrix of a random directed graph on n vertices (where loops are allowed) such that each vertex has outdegree s. In this case, $\mathbf{M}_n$ always has s as an eigenvalue (with the corresponding eigenvector being the all-ones vector), and hence not every eigenvalue of $\mathbf{M}_n$ can be of high algebraic degree. Using Theorem 1.7, we show that, besides this trivial eigenvalue, the other eigenvalues cannot be low-degree algebraic numbers.

Theorem 2.12 *Let $0 < \varepsilon \leq 1$, $K \geq 1$, and $B > 0$ be a constants, and let $x \in \{0,1\}^n$ be a random binary vector uniformly chosen from among all binary vectors containing exactly s ones for some s satisfying $|s - n/2| \leq (1-\varepsilon)n/2$. If $\mathbf{M}_n$ is a random n by n matrix whose rows are iid copies of the vector x, then, for all sufficiently large n (depending only on ε, K, and B), the probability that one of the nontrivial eigenvalues of the matrix $\mathbf{M}_n$ is algebraic of degree at most K is bounded above by n^{-B}.*

Proof The proof of Theorem 2.12 follows closely the proof of Theorem 2.8, where instead of using Theorem 2.7 we apply Theorem 2.13 below. The main difference comes from the fact that we must now deal with the trivial eigenvalue at s.

Let f be the characteristic polynomial of $\mathbf{M}_n$, and note that all eigenvalues of $\mathbf{M}_n$ have absolute value at most n with probability 1 by an elementary bound. Let $\Omega := \{z \in \mathbb{C} : |z| \leq n, z \neq s\}$, and note that by Theorem 2.13 below, we may take $p = n^{-B'}$ for any constant $B' > 0$ in (1.2). Thus, we may apply Theorem 1.7 and Lemma 1.8(iv) (with $M = n$ and $m = 1$) to complete the proof. □

It remains to verify the following bound.

Theorem 2.13 *Let $0 < \varepsilon \leq 1$ and $B > 0$ be a constants, and let $x \in \{0,1\}^n$ be a random binary vector uniformly chosen from among all binary vectors containing exactly s ones for some s satisfying $|s - n/2| \leq (1-\varepsilon)n/2$. If $\mathbf{M}_n$ is a random n by n matrix whose rows are iid copies of the vector x, then, for n sufficiently large (depending only on ε and B),*

$$\sup_{z\in\mathbb{C},\ z\neq s} \mathbb{P}(z \textit{ is an eigenvalue of } \mathbf{M}_n) \leq n^{-B} \tag{2.3}$$

and

$$\mathbb{P}(s \textit{ is an eigenvalue of } \mathbf{M}_n \textit{ with algebraic multiplicity at least } 2) \leq n^{-B}. \tag{2.4}$$

Proof The proof follows the arguments given by Nguyen and Vu in [36]. We begin with the bound in (2.3). Let $\Omega := \{z \in \mathbb{C} : |z| \leq n, z \neq s\}$. Since, with probability 1, all eigenvalues of $\mathbf{M}_n$ are contained in the disk $\{z \in \mathbb{C} : |z| \leq n\}$, it suffices to show

$$\sup_{z\in\Omega} \mathbb{P}(z \text{ is an eigenvalue of } \mathbf{M}_n) \leq n^{-B}$$

for n sufficiently large. Define the matrix $\mathbf{X}_n := 2\mathbf{M}_n - \mathbf{J}_n$, where $\mathbf{J}_n$ is the $n \times n$ all-ones matrix. In particular, $\mathbf{X}_n$ is an $n \times n$ random matrix with $+1$ and -1 entries whose rows are independent with row sum $2s - n$, where $|2s - n| \leq (1-\varepsilon)n$. Such matrices were explicitly studied in [36], and the estimate below follows from [36, Theorem 2.8]. Let $\mathbf{M}_{n-1}$ be the $(n-1) \times (n-1)$ submatrix of $\mathbf{M}_n$ formed from $\mathbf{M}_n$ by removing the last row and column. Similarly, let $\mathbf{X}_{n-1} := 2\mathbf{M}_{n-1} - \mathbf{J}_{n-1}$. Then, for any deterministic matrix $\mathbf{F}$ satisfying $\|\mathbf{F}\| \leq n^2$, [36, Theorem 2.8] implies that

$$\sup_{z\in\mathbb{C},\ |z|\leq 2n} \mathbb{P}(z \text{ is an eigenvalue of } \mathbf{X}_{n-1} + \mathbf{F}) \leq n^{-B} \tag{2.5}$$

for all n sufficiently large (depending only on ε and B).

The advantage of working with $\mathbf{M}_{n-1}$ is that it does not have a trivial eigenvalue at s. Thus, we will reduce to the case where the bound in (2.5) is relevant. Let m_{ij} denote the (i, j)-entry of $\mathbf{M}_n$. Define $\mathbf{M} := \mathbf{M}_n - z\mathbf{I}_n$. Then $\det(\mathbf{M}) = \det(\mathbf{M}')$, where $\mathbf{M}'$ is obtained from $\mathbf{M}$ by adding the first $n-1$ columns to the last column. Since each entry of the last column of $\mathbf{M}'$ takes the value $s - z$, $\det(\mathbf{M}') = (s - z)\det(\mathbf{M}'')$, where $\mathbf{M}''$ is obtained from $\mathbf{M}$ by replacing each entry in the last column by 1, i.e.,

$$\mathbf{M}'' := \begin{bmatrix} m_{1,1} - z & m_{1,2} & \dots & m_{1,n-1} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ m_{n-1,1} & m_{n-1,2} & \dots & m_{n-1,n-1} - z & 1 \\ m_{n,1} & m_{n,2} & \dots & m_{n,n-1} & 1 \end{bmatrix}.$$

Since $s \notin \Omega$, it now suffices to show

$$\sup_{z\in\mathbb{C},\ |z|\leq n} \mathbb{P}(\det(\mathbf{M}'') = 0) \leq n^{-B} \tag{2.6}$$

for n sufficiently large. Additionally, as $\det(\mathbf{M}_n - z\mathbf{I}) = (s - z)\det(\mathbf{M}'')$, the bound in (2.6) would also imply (2.4).

By subtracting the last row of $\mathbf{M}''$ from each of the previous $n-1$ rows, it follows that $\det(\mathbf{M}'') = \det(\mathbf{M}_{n-1} - \mathbf{Q}_{n-1} - z\mathbf{I}_{n-1})$, where $\mathbf{Q}_{n-1}$ is an $(n-1)\times(n-1)$ rank-one matrix whose rows are each given by $(m_{n,1}, \dots, m_{n,n-1})$. Since the entries $m_{n,1}, \dots, m_{n,n-1}$ are independent of the entries in $\mathbf{M}_{n-1}$, we condition on $\mathbf{Q}_{n-1}$ and now treat this matrix as deterministic. Observe that $\det(\mathbf{M}_{n-1} - \mathbf{Q}_{n-1} - z\mathbf{I}_{n-1}) = 0$ if and only if $2z$ is an eigenvalue of

$$2\mathbf{M}_{n-1} - 2\mathbf{Q}_{n-1} = \mathbf{X}_{n-1} - 2\mathbf{Q}_{n-1} + \mathbf{J}_{n-1} =: \mathbf{X}_{n-1} + \mathbf{F}.$$

By an elementary bound,

$$\|\mathbf{F}\| \leq 2\|\mathbf{Q}_{n-1}\| + \|\mathbf{J}_{n-1}\| \leq 3n \leq n^2$$

for $n \geq 3$. Therefore, we conclude from (2.5) that

$$\sup_{z\in\mathbb{C},\ |z|\leq n} \mathbb{P}(\det(\mathbf{M}_{n-1} - \mathbf{Q}_{n-1} - z\mathbf{I}_{n-1}) = 0) \leq n^{-B}$$

for n sufficiently large, and the proof is complete. □

2.9 Other Models

In the previous subsections, we focused on random polynomial models for which good pointwise delocalization bounds are known, especially characteristic polynomials of random matrices. For example, the approach above also works for sparse random matrices, using Tao and Vu's [49, Theorem 2.9] to show pointwise delocalization.

However, there are many other models of random matrices one could consider. For instance, sample covariance matrices arise in many applications and are well studied in the random matrix theory literature. Yet, the authors are not aware of delocalization bounds of the form required for Theorem 1.7. Another interesting model is random matrices with exchangeable entries. While Adamczak et al. [1] have obtained some delocalization bounds for such matrices, the bounds are not strong enough to use with Theorem 1.7. Some delocalization bounds have been proven by Cook [12,13] for the adjacency matrix and signed adjacency matrix of such graphs, and it would be interesting to see whether strong enough bounds could be proven to combine with Theorem 1.7.

3 Motivation: Random Graphs and Controllability

As discussed above, our main results are motivated by the question of whether a random polynomial with integer coefficients is likely to be irreducible. In particular, we have focused on characteristic polynomials of matrices, and it is natural to ask whether such models have applications.

In this section, we motivate these models by discussing graphs and their adjacency matrices. Unsurprisingly, certain properties of a graph can be deduced from the characteristic polynomial of its adjacency matrix. Specifically, we focus on the property of symmetry, which in turn is related to controllability properties of a certain linear system formed from the graph. In this section, we provide a brief introduction to linear control theory, random graphs, and their connection with our main results. The uninterested reader can safely skip this section.

3.1 Linear Control Theory

Generally speaking, linear control theory is concerned with controlling linear systems, so the output (or solution) of the system follows a desired path. In what follows, we shall consider a very specific linear system formed from a matrix $\mathbf{A}$ and a vector b.

Let $\mathbf{A}$ be an $n \times n$ matrix with real entries, and let b be a vector in $\mathbb{R}^n$. Then the *continuous time-invariant control system* formed from the pair $(\mathbf{A}, b)$ is defined by the equation

$$\dot{x}(t) = \mathbf{A}x(t) + u(t)b, \tag{3.1}$$

where $u : [t_0, t_1] \to \mathbb{R}$ is called the *control* and $x : [t_0, t_1] \to \mathbb{R}^n$ is called the *state* of the system. Here, $\dot{x}$ denotes the time derivative of x. We typically view $\mathbf{A}$, b, and u as given values and x as the solution to (3.1). In particular, given $\mathbf{A}$, b, an initial value $x(t_0)$, and sufficiently smooth u, the state x is uniquely determined by (3.1).

We want to consider the general property of being able to "steer" such a system from any given state to any other by a suitable choice of the control function u. This ability to "steer" the system is what we will mean by the term controllability.

Definition 3.1 (*Complete controllability*) Let $\mathbf{A}$ be an $n \times n$ matrix with real entries, and let b be a vector in $\mathbb{R}^n$. We say the pair $(\mathbf{A}, b)$ is *completely controllable* if, for any t_0, any initial state $x(t_0) = x_0$, and any given final state x_f, there exists $t_1 > t_0$ and a piecewise continuous control $u : [t_0, t_1] \to \mathbb{R}$ such that the solution (state) of (3.1) satisfies $x(t_1) = x_f$.

Remark 3.2 The qualifying term "completely" implies that the definition holds for all x_0 and x_f. In general, several other types of controllability can also be defined.

The basic problem that now arises is to describe exactly which pairs $(\mathbf{A}, b)$ are completely controllable. Kalman's rank condition [24–27] gives a general algebraic criterion.

Theorem 3.3 (Kalman [27]) *Let $\mathbf{A}$ be an $n \times n$ matrix with real entries, and let b be a vector in $\mathbb{R}^n$. The pair $(\mathbf{A}, b)$ is completely controllable if and only if the* controllability matrix

$$\left[\mathbf{b}\ \mathbf{A}b\ \mathbf{A}^2b\ \cdots\ \mathbf{A}^{n-1}b\right] \tag{3.2}$$

has full rank (that is, rank n). Here, the matrix in (3.2) is the $n \times n$ matrix with columns b, $\mathbf{A}b$, $\mathbf{A}^2b$, ..., $\mathbf{A}^{n-1}b$.

Theorem 3.3 is so convenient that this rank condition is often taken as the definition of controllability. In fact, from this point forward, we will no longer consider the linear system in (3.1). Instead, we will only focus on controllability matrix (3.2). To this end, we make the following definition.

Definition 3.4 (*Controllability*) Let $\mathbf{A}$ be an $n \times n$ matrix with real entries, and let b be a vector in $\mathbb{R}^n$. We say the pair $(\mathbf{A}, b)$ is *controllable* if the controllability matrix, defined in (3.2), has rank n. If $(\mathbf{A}, b)$ is not controllable, we say the pair is *uncontrollable*.

Remark 3.5 In view of Theorem 3.3, controllability and complete controllability are equivalent. We drop the qualifying term "complete" as this is the only type of controllability we will consider.

3.2 Controllable Subsets in Graphs

Let G be a simple graph on the vertex set $[n] := \{1, \dots, n\}$ with adjacency matrix $\mathbf{A}$, i.e., $\mathbf{A}$ is a real symmetric matrix with entry (i, j) equal to 1 if there is an edge between vertices i and j, and the entry is equal to zero otherwise. In this section, we focus on the controllability of $(\mathbf{A}, b)$. Of particular importance is the case when $b \in \{0, 1\}^n$ is a binary vector. Indeed, in this case, b can be viewed as the characteristic vector of some subset of the vertex set $[n]$. We make the following definitions. We say the simple graph G on n vertices is *controllable* if $(\mathbf{A}, \mathbf{1})$ is controllable, where $\mathbf{A}$ is the adjacency matrix of G and $\mathbf{1}$ is the all-ones vector in $\mathbb{R}^n$. Additionally, we say G is *minimally controllable* if $(\mathbf{A}, e_i)$ is controllable for every $1 \leq i \leq n$, where $e_1, \dots, e_n$ is the standard basis of $\mathbb{R}^n$.

Studying the controllability properties of large-scale graphs and networks has become an important and challenging task in control theory with several real-world applications. For instance, one of the emerging applications of network controllability is the control of neural networks inside the brain and its relation to behavioral regulation [19,22]. In this application,[3] the neural network in the brain is modeled as a graph with each vertex representing a neuron or region in the brain.

Another application involves studying social influence. Indeed, with the prevalence of online social networks, social influence is now a highly studied topic due, in part, to its use in categorizing efficient mechanisms for the spread of information as well as identification of susceptible members of society [2,5]. In this application, the graph in question is the social network, and the characteristic vector b can be viewed as identifying the "leaders" in the network who try to control the other individuals.

We recall the following elementary definitions. *Isomorphisms* of simple graphs are bijections of the vertex sets preserving adjacency as well as nonadjacency. *Automorphisms* of the graph G are $G \to G$ isomorphisms. Clearly, the identity map is always an automorphism. A graph is called *asymmetric* if it has no nontrivial automorphisms.

We now discuss some connections which exist between controllability, asymmetry, and the characteristic polynomial of the adjacency matrix.

Proposition 3.6 *(Godsil, following from Lemma 1.1 in [21]) If the simple graph G is controllable, then G is asymmetric.*

[3] Both of the applications mentioned here typically involve studying matrices other than the adjacency matrix of the underlying graph. For simplicity, we will only consider the adjacency matrix in this paper.

Godsil, in [21], showed a connection between the characteristic polynomial of the adjacency matrix and controllability.

Theorem 3.7 *(Godsil, Corollary 5.3 in [21]) Let G be a simple graph with adjacency matrix $\mathbf{A}$. If the characteristic polynomial of $\mathbf{A}$ is irreducible over the rationals, then G is controllable and minimally controllable.*

Putting these two results together, we recover the well-known implication (see, for example, [8]) that if G is a simple graph with adjacency matrix $\mathbf{A}$ and the characteristic polynomial of $\mathbf{A}$ is irreducible over the rationals, then G is asymmetric.

3.3 Conjectures and Results Concerning Random Graphs

Recall that $G(n, p)$ is the Erdös–Rényi random graph on the vertex set $[n]$ with edge density p. That is, $G(n, p)$ is a simple graph on n vertices (which we shall label as $1, \dots, n$) such that each edge $\{i, j\}$ is in $G(n, p)$ with probability p, independent of other edges. In the special case when $p = 1/2$, one can view $G(n, 1/2)$ as random graph selected uniformly among all $2^{\binom{n}{2}}$ simple graphs on n vertices. We let $\mathbf{A}_n$ be the zero-one adjacency matrix of $G(n, p)$.

It was proven by Pólya [42] and Erdős and Rényi [17] that $G(n, 1/2)$ is asymmetric with probability $1 - \binom{n}{2} n^{-n-2}(1 + o(1))$; see [3] and references therein for further details. In other words, most simple graphs are asymmetric. In view of Proposition 3.6, this gives an upper bound for the probability that $G(n, p)$ is controllable. In terms of a lower bound, Godsil [21] has recently conjectured that most simple graphs are controllable and minimally controllable.

Conjecture 3.8 (Godsil [21]) *The probability that $G(n, 1/2)$ is controllable and minimally controllable approaches 1 as $n \to \infty$.*

One can view Conjecture 3.8 as stating that controllability (alternatively, minimal controllability) is a universal property of graphs. Conjecture 3.8 was recently proven in [39,40]. The proof relies on Kalman's rank condition (Theorem 3.3) and one of its corollaries known as the Popov–Belevitch–Hautus (PBH) test. (See [23, Section 12.2] for details.) In particular, the proof given in [39,40] involves studying the additive structure of the eigenvectors of the random adjacency matrix $\mathbf{A}_n$.

It has also been conjectured (and numerical evidence suggests) that the characteristic polynomial of the adjacency matrix of $G(n, 1/2)$ is irreducible over the rationals with high probability. The authors are not aware of any progress in proving this conjecture. In view of Theorem 3.7, though, this conjecture would imply Conjecture 3.8. Specifically, Theorem 3.7 hints at another approach to prove Conjecture 3.8, which would be entirely different from the proofs given in [39,40]. While the proofs in these previous works focused on the eigenvector structure, this new method only requires working with the eigenvalues (in particular, the characteristic polynomial) of $\mathbf{A}_n$. If one could show, for instance, that, with high probability, $\mathbf{A}_n$ has no eigenvalues that are algebraic of degree at most $n/2$, then both conjectures would follow. While our main results do not go so far, they do hint that this may indeed be the case. Theorem 3.9 below follows from Theorem 2.11 and the reasoning in Sect. 2.6.

Theorem 3.9 *Fix $0 < p < 1$, and let $B > 0$ and $K \geq 1$ be constants. Let $G(n, p)$ be an Erdős–Rényi random graph on n vertices with edge density p. Then, for n sufficiently large (depending on B, K, and p), the probability that the adjacency matrix $\mathbf{A}_n$ of $G(n, p)$ has an eigenvalue that is algebraic of degree at most K is bounded above by n^{-B}.*

Note that Vershynin's result [52, Theorem 1.2] (and also the special case stated in Theorem 2.5) is not applicable here because then entries of the adjacency matrix do not have zero mean. It would be interesting to see whether [52, Theorem 1.2] could be extended to the case where the entries had nonzero mean; such a result would directly improve the bound in Theorem 3.9 above, likely giving a result analogous to Theorem 2.6.

4 Proof of Theorem 1.7 and Lemma 1.8

We prove Theorem 1.7 first and prove Lemma 1.8 at the end of this section. We prove Theorem 1.7 via a series of lemmata. Some of the results in this section can also be found in the text [16] by Dummit and Foote; we provide proofs in certain cases for completeness.

Lemma 4.1 *Let f be a polynomial with rational coefficients. If λ is a root of f, then the minimal polynomial of λ divides f over the rationals.*

Proof Let g denote the minimum polynomial of λ. By definition of the minimum polynomial, this implies that $\deg(g) \leq \deg(f)$. Hence, by the division algorithm, $f(z) = h(z)g(z) + r(z)$, where h and r are polynomials with rational coefficients and $\deg(r) < \deg(g)$. Since λ is a root of both f and g, we have that λ is a root of r. However, since $\deg(r) < \deg(g)$ and g is the minimum polynomial of λ, we must have that $r(z) = 0$. □

For the proof of the next lemma, we will need Gauss's lemma.

Theorem 4.2 *(Gauss's lemma; Proposition 5 on page 303 of [16]) Let f be a nonconstant polynomial with integer coefficients. If f is irreducible over the integers, then f is irreducible over the rationals.*

Lemma 4.3 *Let f be a monic polynomial with integer coefficients. If λ is a root of f with minimal polynomial g, then g is a monic polynomial with integer coefficients and λ is an algebraic integer.*

Proof We begin by factoring f over the integers into irreducible polynomials f_j for $1 \leq j \leq \ell$:

$$f(z) = \prod_{j=1}^{\ell} f_j(z).$$

It must be the case that each f_j is monic. Additionally, λ must be a root of one of the f_j's; without loss of generality, assume λ is a root of f_1. By Lemma 4.1, g divides f_1 over the rationals. However, from Gauss's lemma (Theorem 4.2), this implies (since f_1 is monic) that $g = f_1$. We conclude that g is a monic polynomial with integer coefficients, and by definition it follows that λ is an algebraic integer. □

Lemma 4.4 below is the main lemma we will need to prove Theorem 1.7. Roughly speaking, Lemma 4.4 says that if f is a monic polynomial with integer coefficients and bounded roots, then there are only a limited number of points in $\mathbb{C}$ that can be roots for f that are algebraic with low degree.

Lemma 4.4 (Counting bound) *Let $M > 0$ and $1 \leq k \leq n$. Then there exists a set $S \subset \mathbb{C}$ (depending only on M and k) of algebraic integers with cardinality*

$$|S| \leq k \prod_{j=1}^{k} \left(2\binom{k}{j} M^j + 1 \right)$$

such that the following holds. If f is a monic polynomial of degree n with integer coefficients whose roots are bounded in magnitude by M and λ is an root of f that is algebraic of degree k, then $\lambda \in S$.

Proof For each $c_0, \ldots, c_{k-1} \in \mathbb{Z}$, we define the monic polynomial with coefficients $c_0, \ldots, c_{k-1}$ as

$$h_{c_0,\ldots,c_{k-1}}(z) := z^k + \sum_{j=1}^{k} c_{k-j} z^{k-j}.$$

Each such polynomial is a monic polynomial with integer coefficients, and hence the roots of any such polynomial are always algebraic integers. Define the index set

$$T := \left\{ (c_0, \ldots, c_{k-1}) \in \mathbb{Z}^k : |c_{k-j}| \leq \binom{k}{j} M^j \text{ for } j = 1, \ldots, k \right\}.$$

By construction,

$$|T| \leq \prod_{j=1}^{k} \left(2\binom{k}{j} M^j + 1 \right).$$

We now define the set S as the collection of roots of all polynomials $h_{c_0,\ldots,c_{k-1}}$ whose coefficients $(c_0, \ldots, c_{k-1}) \in T$. In other words, recalling (1.1),

$$S := \bigcup_{(c_0,\ldots,c_{k-1}) \in T} \Lambda(h_{c_0,\ldots,c_{k-1}}).$$

Since each polynomial $h_{c_0,\dots,c_{k-1}}$ has at most k distinct roots, it follows that

$$|S| \leq k|T| \leq k \prod_{j=1}^{k} \left(2\binom{k}{j} M^j + 1 \right). \tag{4.1}$$

We now claim that S satisfies the conclusion of the lemma. Indeed, let f be a monic polynomial of degree n with integer coefficients whose roots are bounded in magnitude by M. Let $\lambda_1, \dots, \lambda_n$ be the roots of f, and suppose λ_1 is an algebraic root of degree k. It follows from Lemmas 4.1 and 4.3, that the minimal polynomial of λ_1, say g, is a monic polynomial with integer coefficients which divides f. This implies that the roots of g are also roots of f. (Clearly, λ_1 is a root of both f and g.) Without loss of generality, assume $\lambda_1, \dots, \lambda_k$ are the roots of g. Then

$$g(z) = (z - \lambda_1) \cdots (z - \lambda_k) = z^k + \sum_{j=1}^{k} d_{k-j} z^{k-j},$$

where $d_{k-j} := (-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq k} \lambda_{i_1} \cdots \lambda_{i_j}$. As noted above, each $d_{k-j} \in \mathbb{Z}$. In addition, since each root of f is bounded in magnitude by M, it follows that $|d_{k-j}| \leq \binom{k}{j} M^j$. This implies that $(d_0, \dots, d_{k-1}) \in T$. Therefore, we conclude that the roots of g are contained in S. □

With Lemma 4.4 in hand, we are now ready to prove Theorem 1.7. The main idea is simple: If f does have an algebraic root of degree k, then Lemma 4.4 shows it must be contained in the set S, which has small cardinality. We can then show that each of the points in S is unlikely to be a root of f using the bound in (1.2).

Proof of Theorem 1.7 Let f be a random monic polynomial with integer coefficients. Let $S \subset \mathbb{C}$ be the set of algebraic integers from Lemma 4.4. In particular, S is a deterministic set which only depends on M and k, and S has cardinality

$$|S| \leq k \prod_{j=1}^{k} \left(2\binom{k}{j} M^j + 1 \right). \tag{4.2}$$

Let $\mathcal{B}_{f,M}$ be the event that all roots z of f satisfy $|z| \leq M$. If f has an algebraic root of degree k in Ω and $\mathcal{B}_{f,M}$ holds, then Lemma 4.4 implies that this root must be in $S \cap \Omega$. Hence, by the union bound, we obtain

$$\begin{aligned}
&\mathbb{P}\left(f \text{ has an algebraic root of degree } k \text{ in } \Omega\right) \\
&\quad \leq \mathbb{P}\left(\{\text{there exists } w \in S \cap \Omega \text{ such that } f(w) = 0\} \cap \mathcal{B}_{f,M}\right) + \mathbb{P}(\overline{\mathcal{B}_{f,M}}) \\
&\quad \leq \left(\sum_{w \in S \cap \Omega} \mathbb{P}\left(f(w) = 0\right) \right) + \mathbb{P}(\overline{\mathcal{B}_{f,M}}) \\
&\quad \leq p|S| + \mathbb{P}(\overline{\mathcal{B}_{f,M}}).
\end{aligned}$$

The conclusion now follows from the cardinality bound given in (4.2) combined with Lemma 4.5 (based on Stirling's approximation) below. □

Lemma 4.5 *(Some useful bounds) For $M \geq 1$ and $k \geq 2$,*

$$M^{(k^2+k)/2} e^{(k^2-k\log(k))/2} \leq \prod_{j=1}^{k} \left(2\binom{k}{j}M^j + 1\right) \leq (eM)^{(k^2+k)/2} \tag{4.3}$$

$$\text{and} \qquad \sum_{l=1}^{k} l \prod_{j=1}^{l} \left(2\binom{l}{j}M^j + 1\right) \leq (eM)^{k^2}. \tag{4.4}$$

If $k = 1$, the upper bound of $3M$ holds in (4.3) and (4.4).

Proof of Lemma 4.5 To prove the upper bound in (4.3), we note that

$$\prod_{j=1}^{k} \left(2\binom{k}{j}M^j + 1\right) \leq \prod_{j=1}^{k} 3\binom{k}{j}M^j = 3^k M^{k(k+1)/2} \prod_{j=1}^{k} \binom{k}{j}.$$

Using falling factorial notation $(k)_j := k(k-1)\cdots(k-j+1)$, we compute

$$\begin{aligned}
3^k \prod_{j=1}^{k} \binom{k}{j} &= 3^k \frac{\prod_{j=1}^k j^j}{\prod_{j=1}^k j!} \leq 3^k \frac{\prod_{j=1}^k j^j}{\prod_{j=1}^k \sqrt{2\pi j}(j/e)^j} = \left(\frac{3}{\sqrt{2\pi}}\right)^k \frac{\exp(k(k+1)/2)}{\sqrt{k!}} \\
&\leq \left(\frac{3}{\sqrt{2\pi}}\right)^k \frac{\exp(k(k+1)/2 + k/2)}{(2\pi k)^{1/4} k^{k/2}} \\
&= \exp\left[k(k+1)/2 + k/2 + k\log\left(3/\sqrt{2\pi}\right) - \frac{k}{2}\log k - \frac{1}{4}\log(2\pi k)\right] \\
&\leq \exp\left[k(k+1)/2 + k\Big(1/2 + \log\left(3/\sqrt{2\pi}\right) - \frac{1}{2}\log k\Big)\right].
\end{aligned}$$

Note that the first and second inequalities above come from Stirling's approximation:

$$j! \geq \sqrt{2\pi j}\left(\frac{j}{e}\right)^j. \tag{4.5}$$

It is easy to see that $\left(1/2 + \log(3/\sqrt{2\pi}) - \frac{1}{2}\log k\right) = \log\left(\frac{3\sqrt{e}}{\sqrt{k2\pi}}\right)$ becomes negative for $k \geq 4$, proving the upper bound for $k \geq 4$. For the $k = 1, 2, 3$ cases, one can explicitly expand $\prod_{j=1}^k \left(2\binom{k}{j}M^j + 1\right)$ and use $M \geq 1$ to verify that it is at most $3M$ when $k = 1$ and is less than $(eM)^{(k^2+k)/2}$ when $k = 2$ or 3. This completes the proof of the upper bound in (4.3).

To show the upper bound in (4.4), we note that $\sum_{\ell=1}^k \ell = \frac{k^2+k}{2}$, and, for $k \geq 3$, we have $\left(\frac{k^2+k}{2}\right)(eM)^{(k^2+k)/2} \leq (eM)^{k^2}$ by elementary calculus. (Note the function

$e^{(k^2-k)/2} - \frac{k^2+k}{2}$ is positive and increasing for all $k \geq 3$.) Finally, for $k = 2$, one can check that $3M + 2(eM)^3 \leq (eM)^4$ for any $M \geq 1$, thus proving (4.4).

To show the lower bound in (4.3), we use the same approach as for the upper bound, noting that

$$\prod_{j=1}^{k} \left(2\binom{k}{j}M^j + 1\right) \geq \prod_{j=1}^{k} 2\binom{k}{j}M^j = 2^k M^{k(k+1)/2} \prod_{j=1}^{k} \binom{k}{j}.$$

To bound $2^k M^{k(k+1)/2} \prod_{j=1}^{k} \binom{k}{j}$, we use Stirling's approximation $j! \leq e\sqrt{j}\left(\frac{j}{e}\right)^j$ in each place where we used (4.5) in the upper bound proof above, eventually arriving at

$$\begin{aligned} 2^k \prod_{j=1}^{k} \binom{k}{j} &= 2^k \prod_{j=1}^{k} \frac{(k)_j}{j!} = 2^k \frac{\prod_{j=1}^{k} j^j}{\prod_{j=1}^{k} j!} \\ &\geq \exp\left[\frac{k^2}{2} + k - \frac{1}{2} - \frac{1}{4}\log k - k\log\left(\frac{e}{2}\right) - \frac{k}{2}\log k\right] \\ &\geq \exp\left[\frac{k^2}{2} - \frac{k}{2}\log k\right], \end{aligned}$$

where the last inequality holds since $k - \frac{1}{2} - \frac{1}{4}\log k - k\log\left(\frac{e}{2}\right)$ is positive for all $k \geq 1$. This completes the proof of the lower bound.

One can see from the proof that $\frac{k^2}{2} - \frac{k}{2}\log k + o(k\log k)$ is the correct order for the exponent on e in (4.3). □

Proof of Lemma 1.8 For (i), note that $O\left(\frac{1}{\sqrt{n}}\right)(2e)^{\frac{\log n}{4}}$ is equal to $O(\exp(-\frac{1}{2}\log n + \frac{1+\log 2}{4}\log n)) = o(1)$.

For (ii), note that $(en)^{n^{1-2\epsilon}} = \exp(n(n^{-2\epsilon}(1+\log n)) = (1+o(1))^n$.

For (iii), note that $2e^{-n^c}(eC\sqrt{n})^{n^{2c'}} \leq \exp(\log 2 + -n^c + n^{2c'}(1+\log(Cn))) = \exp\left(n^c(-1 + \frac{\log 2}{n^c} + n^{2c'-c}(\log n + \log C)\right) \leq \exp(n^c(-\frac{2}{3}))$ for sufficiently large n.

Finally, for (iv), given B, note that we can choose $B' = B + 2mK^2$ and then $n^{-B'}(en^m)^{K^2} = n^{-B}\exp(-2mK^2\log n + K^2(1 + m\log n)) \leq n^{-B}$ for n sufficiently large. □

5 Proof of Theorem 2.1

We will show that it is likely that $f_n(z)$ has no irreducible factor of degree $n^{1/3}/\log^3(n)$ or less, following a similar approach to Konyagin [28]. As in [28], we bound the probability as a sum of two cases, depending on whether the irreducible factor is cyclotomic or not. We have optimized the proof in the noncyclotomic case for the highest possible degree (up to log factors); however, a stronger result can be proved in the cyclotomic case. Pointwise delocalization in the noncyclotomic case will follow from an anti-concentration result proven by Tao and Vu (Lemma 5.1) which we discuss before giving the proof of Theorem 2.1.

Let Z be a complex-valued random variable. The *Lévy concentration function* of Z is defined as

$$\mathcal{L}(Z,t) := \sup_{u\in\mathbb{C}} \mathbb{P}(|Z-u| \le t)$$

for all $t \geq 0$. The Lévy concentration function bounds the *small ball probabilities* for Z, which are the probabilities that Z is in a ball of radius t.

Lemma 5.1 *(Tao–Vu, following from Lemma 9.2 in [48]) Let $\xi_1,\ldots,\xi_n$ be iid Rademacher random variables, which take the values $+1$ and -1 with equal probability. Let $x_0,\ldots,x_n$ be complex numbers, and suppose there is a subsequence $x_{i_1},\ldots,x_{i_m}$ with the property that*

$$|x_{i_j}| \geq 2|x_{i_{j+1}}|$$

for all $j=1,\ldots,m-1$. Consider the sum $S := \sum_{k=0}^n \xi_k x_k$. Then one has

$$\mathcal{L}(S,0) \leq C\exp(-cm)$$

for some absolute constants $C, c > 0$.

We now have the tools to prove Theorem 2.1.

Proof of Theorem 2.1 Let $\xi_0, \xi_1, \ldots$ be iid Rademacher random variables which take the values $+1$ and -1 with equal probability, and recall that $f_n(z) := z^n + \xi_{n-1}z^{n-1} + \cdots + \xi_1 z + \xi_0$. The general approach below follows Konyagin [28].

First, we bound the number of irreducible polynomials $g(z)$ of degree d that can divide $f_n(z)$. If $g(z)$ divides $f_n(z)$, then all roots of $g(z)$ are roots of $f_n(z)$ and so are algebraic integers with absolute value between $1/2$ and 2 (by Lemma 5.2). Also, the set of roots of any given monic irreducible $g(z)$ are disjoint from the set of roots of any other monic irreducible polynomial (by uniqueness of the minimal polynomial and Lemma 4.1); thus, the number of degree d algebraic integers that can be roots of $f_n(z)$ is an upper bound for the number of possible degree d irreducible polynomials $g(z)$ that can divide $f_n(z)$. Hence, by Lemmas 4.4 and 4.5, we have

$$\#\{\text{degree } d \text{ irreducible } g(z) \text{ that divide } f_n(z)\} \leq (2e)^{d^2}. \tag{5.1}$$

When $d \leq 2$, the total number of possible divisors $g(z)$ is a constant, so applying Remark 2.2, the probability that any such polynomial divides $f_n(z)$ is at most $O(1/\sqrt{n})$. Thus, it is sufficient to consider irreducible divisors with degree at least 3, and we assume for the remainder of the proof that a possible divisor $g(z)$ has degree $d \geq 3$.

For the noncyclotomic case, we will show sufficient delocalization so that the probability that $f_n(z)$ has an irreducible factor of degree d with $3 \le d \le n^{1/3}/\log^3(n)$ is exponentially small. Let $g(z)$ be an arbitrary noncyclotomic irreducible polynomial with degree d where $3 \le d \le n^{1/3}/\log^3(n)$. By Lemmas 4.1 and 4.3, we may assume g is monic; also, $g(z)$ divides $f(z)$ if and only if $f(w) = 0$, where w is any root of $g(z)$. By a result of Dobrowolski [15], since $g(z)$ is noncyclotomic, it must have a root w satisfying

$$|w| \ge 1 + \frac{c}{d}\left(\frac{\log\log d}{\log d}\right)^3,$$

where c is a positive constant; note that the lower bound strictly exceeds 1 since $d \ge 3$. We will show that the sequence $1, w, w^2, w^3, \ldots, w^n$ contains a subsequence that grows quickly, and then apply Lemma 5.1. Because $d \le n^{1/3}/\log^3 n$, we know that $|w| \ge 1 + \frac{c}{n^{1/3}}$ and so if we take a minimal integer b satisfying $b \ge \frac{4n^{1/3}}{c}$, we have that $|w|^b \ge (1 + \frac{c}{n^{1/3}})^b \ge \exp\left(\frac{cb}{2n^{1/3}}\right)$ for sufficiently large n (since $1 + x \ge e^{x/2}$ for all sufficiently small positive x) , which shows that $|w|^b \ge 2$. We can now take the subsequence $w^0, w^b, w^{2b}, \ldots, w^{\lfloor \frac{n}{b} \rfloor b}$, noting each term is at least twice the term before in absolute value, and so Lemma 5.1 implies the delocalization bound

$$\begin{aligned}\mathbb{P}(g(z) \text{ divides } f_n(z)) &= \mathbb{P}(f_n(w) = 0)\\ &\le C\exp\left(-c\left(\left\lfloor \frac{n}{b} \right\rfloor + 1\right)\right) \le C\exp(-cn^{2/3}),\end{aligned}$$

where C and c are constants that may change from line to line. By (5.1), there are at most $(2e)^{d^2} \le \exp\left(\frac{n^{2/3}}{\log^6 n}(1 + \log 2)\right)$ possible polynomials $g(z)$ with degree d where $3 \le d \le n^{1/3}/\log^3 n$. Taking a union bound over all possible $g(z)$ with all possible degrees d, we see that the probability that $f_n(z)$ has an irreducible noncyclotomic factor with degree in the range $3 \le d \le n^{1/3}/\log^3 n$ is at most $C\frac{n^{1/3}}{\log^3 n}\exp\left(-cn^{2/3} + \frac{n^{2/3}}{\log^6 n}(1 + \log 2)\right)$, which is less than $\exp(-cn^{2/3})$ for sufficiently large n.

For the cyclotomic case, we will use the union bound over all cyclotomic polynomials of a given degree. Let E_{cyl} be the event that there exists a cyclotomic polynomial of degree d with $3 \le d \le n^{1/3}$ that divides $f_n(x)$, and let $E_{\text{cyl},d}$ be the event that there exists a cyclotomic polynomial of degree d that divides $f_n(x)$. By the union bound, we have $\mathbb{P}(E_{\text{cyl}}) \le \sum_{d=3}^{n^{1/3}} \mathbb{P}(E_{\text{cyl},d})$, and so it remains to prove a bound on $\mathbb{P}(E_{\text{cyl},d})$.

Recall that the k-th cyclotomic polynomial is $\Phi_k(x) = \prod_{\substack{1\le a\le k\\ \gcd(a,k)=1}} \left(x - e^{2\pi i \frac{a}{k}}\right)$. Assume that $\Phi_k(x)$ has degree $d \ge 3$ (which implies $k \ge 3$) and divides $f_n(x)$. Then we have $f_n(\alpha) = 0$, where α is a root of $\Phi_k(x)$. Because $\alpha^k = 1$, we have that $f_n(\alpha) = \sum_{j=0}^{k-1} A_j\alpha^j$ where $A_j = \sum_{\substack{b\equiv j \pmod k\\ 0\le b\le n}} \xi_b$; note that the A_j are independent. Because $f_n(\alpha) = 0$ and α has algebraic degree d, we have $\sum_{j=0}^{d-1} A_j\alpha^j = -\sum_{j=d}^{k-1} A_j\alpha^j = \sum_{j=0}^{d-1} B_j\alpha^j$, for some integers B_j that are functions of $A_d, \ldots, A_{k-1}$, and so the B_j are independent of $A_0, \ldots, A_{d-1}$. Furthermore, because the minimal polynomial for

α has degree d, we must have $A_j = B_j$ for $0 \le j \le d-1$. We may condition on the B_j and apply the Littlewood–Offord inequality (see, for example, [47, Corollary 7.8]) to each equation $A_j = \sum_{\substack{b \equiv j \pmod k \\ 0 \le b \le n}} \xi_b = B_j$, resulting in the bound

$$\mathbb{P}(\Phi_k(x) \text{ divides } f_n(x)) \le \mathbb{P}(A_j = B_j \text{ for } 0 \le j \le d-1) = O\left(\frac{\sqrt{k}}{\sqrt{n}}\right)^d.$$

It is well known that if $\Phi_k(x)$ has degree d, then $k \le cd \log\log d$ for a constant c (following from, for example, Rosser and Schoenfeld [45, Theorem 15]), and so using the assumption that $d \le n^{1/3}$, we have

$$\mathbb{P}(\Phi_k(x) \text{ divides } f_n(x)) \le O\left(\frac{1}{n^{1/4}}\right)^d,$$

a bound independent of k. Because every cyclotomic polynomial is equal to $\Phi_k(x)$ for some k, we have that $\mathbb{P}(E_{\text{cyl},d}) \le O\left(\frac{1}{n^{1/4}}\right)^d N(d)$, where $N(d)$ is the number of cyclotomic polynomials with degree d. Pomerance [43] showed that $N(d) \le cd$. (In fact, [43] shows that the constant c tends slowly to zero as d tends to infinity.) Thus, $\mathbb{P}(E_{\text{cyl},d}) \le d\,O\left(\frac{1}{n^{1/4}}\right)^d$.

We now apply the union bound to $E_{\text{cyl}} = \bigcup_{3 \le d \le n^{1/3}} E_{\text{cyl},d}$. From the discussion after (5.1), we know that the probability of a factor with degree at most 2 is bounded by $O(1/\sqrt{n})$ (in fact, this bound is tight for the possible factors $x+1$ and $x-1$), and so by the previous paragraph, we need a similar bound on $\sum_{d=3}^{n^{1/3}} \left(\frac{c}{n^{1/4}}\right)^d d$ for any constant c. In fact, using the formula for an infinite arithmetico–geometric series, we have that

$$\sum_{d=3}^{\infty} \left(\frac{c}{n^{1/4}}\right)^d d \le 4\left(\frac{c}{n^{1/4}}\right)^3 \le O\left(\frac{1}{\sqrt{n}}\right)$$

for n sufficiently large, which completes the proof. □

Lemma 5.2 *If $f_n(z) := z^n + \xi_{n-1}z^{n-1} + \cdots + \xi_1 z + \xi_0$ is a polynomial in which the coefficients $\xi_0, \xi_1, \ldots \xi_{n-1}$ take values 1 or -1, all roots of f_n have absolute value strictly between $1/2$ and 2.*

Proof If $|z| \le 1/2$, then $\left|z^n + \sum_{j=1}^{n-1} z^j \xi_j\right| \le \sum_{j=1}^{n} \frac{1}{2^j} < 1$, and hence $|f_n(z)| \ge |\xi_0| - \left|z^n + \sum_{j=1}^{n-1} z^j \xi_j\right| > 0$. Thus, if $f_n(z) = 0$, we must have $|z| > 1/2$. Similarly, if $|z| \ge 2$, then $\left|\sum_{j=0}^{n-1} z^j \xi_j\right| \le \sum_{j=0}^{n-1} 2^j < 2^n$, and hence $|f_n(z)| \ge 2^n - \left|\sum_{j=1}^{n} z^j \xi_j\right| > 0$, showing that $|z| < 2$ for any value of z for which $f_n(z) = 0$. □

Acknowledgements We thank Melanie Matchett Wood for many useful conversations and for contributing key ideas for Theorem 1.7. The first author thanks Peter D.T.A. Elliott, Richard Green, and Katherine Stange for useful discussions and references. The second author thanks Van Vu for originally suggesting this line of inquiry. The authors also thank the anonymous referee for useful comments and suggestions which led to the current version of Theorem 2.1. Christian Borst, Evan Boyd, Claire Brekken, and Samantha Solberg produced Fig. 1 and were supported by NSF Grant DMS-1301690 and co-supervised by Melanie Matchett Wood. The second author thanks Steve Goldstein for helping direct Borst, Boyd, Brekken, and Solberg's research. The second author also thanks the Simons Foundation for providing Magma licenses and the Center for High Throughput Computing (CHTC) at the University of Wisconsin-Madison for providing computer resources.

References

1. Adamczak, R., Chafaï, D., Wolff, P.: Circular law for random matrices with exchangeable entries. Random Struct. Algorithms **48**(3), 454–479 (2016)
2. Aral, S., Walker, D.: Identifying influential and susceptible members of social networks. Science **337**(6092), 337–341 (2012)
3. Babai, L.: Automorphism groups, isomorphism, reconstruction. In: Graham, R.L., Grötschel, M., Lovász, L. (eds.) Chapter 27 of the Handbook of Combinatorics, vol. 2, pp. 1447–1540. North Holland Elsevier, Amsterdam (1995)
4. Bary-Soroker, L., Kozma, G.: Is a bivariate polynomial with ±1 coefficients irreducible? Very likely!. Int. J. Number Theory **13**(4), 933–936 (2017)
5. Bond, R.M., Fariss, C.J., Jones, J.J., Kramer, A.D.I., et al.: A 61-million-person experiment in social influence and political mobilization. Nature **489**(7415), 295–298 (2012)
6. Borst, C., Boyd, E., Brekken, C., Solberg, S., Wood, M.M., Wood, P.M.: Irreducibility of random polynomials. arXiv:1705.03709, 10 May 2017. To appear in Experimental Mathematics
7. Bourgain, J., Vu, V.H., Wood, P.M.: On the singularity probability of discrete random matrices. J. Funct. Anal. **258**(2), 559–603 (2010)
8. Chan, A., Godsil, C.D.: Symmetry and eigenvectors. Chapter 3 of Graph Symmetry: Algebraic Methods and Applications, Volume 497 of the series NATO ASI Series pp. 75–106 (edited by G. Hahn and G. Sabidussi) (1997)
9. Chela, R.: Reducible polynomials. J. Lond. Math. Soc. **38**, 183–188 (1963)
10. Cohen, S.D.: The distribution of the Galois groups of integral polynomials. Ill. J. Math. **23**(1), 135–152 (1979)
11. Cohen, S.D.: The distribution of Galois groups and Hilbert's irreducibility theorem. Proc. Lond. Math. Soc. **43**(3), 227–250 (1981)
12. Cook, N.: On the singularity of adjacency matrices for random regular digraphs. arXiv:1411.0243, 9 Nov (2015)
13. Cook, N.: The circular law for signed random regular digraphs. arXiv:1508.00208, 2 Aug (2015)
14. Dietmann, R.: Probabilistic Galois theory. Bull. Lond. Math. Soc. **45**(3), 453–462 (2013)
15. Dobrowolski, E.: On a question of Lehmer and the number of irreducible factors of a polynomial. Acta Arith. **34**(4), 391–401 (1979)
16. Dummit, D.S., Foot, R.M.: Abstract Algebra, 3rd edn. Wiley, Hoboken (2004)
17. Erdős, P., Rényi, A.: Asymmetric graphs. Acta Math. Hung. **14**(3), 295–315 (1963)
18. Feldheim, O.N., Sen, A.: Double roots of random polynomials with integer coefficients. arXiv:1603.03811, 11 Mar (2016)
19. Fox, M.D., Halko, M.A., Eldaief, M.C., Pascual-Leone, A.: Measuring and manipulating brain connectivity with resting state functional connectivity magnetic resonance imaging (fcMRI) and transcranial magnetic stimulation (TMS). Neuroimage **62**(4), 2232–2243 (2012)
20. Gallagher, P.X.: The large sieve and probabilistic Galois theory, Analytic number theory. In: Proceedings of Symposium Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), pp. 91–101. Am. Math. Soc., Providence, R.I (1973)
21. Godsil, C.: Controllable subsets in graphs. Ann. Comb. **16**(4), 733–744 (2012)
22. Gu, S., Pasqualetti, F., Cieslak, M., Telesford, Q.K., et al.: Controllability of structural brain networks. Nat. Commun. **6**, 8414 (2015)
23. Hespanha, J.P.: Linear Systems Theory. Princeton University Press, Princeton (2009)
24. Kalman, R.E.: Contributions to the theory of optimal control. Boletin de la Sociedad Matematica Mexicana **5**, 102–119 (1960)

25. Kalman, R.E.: On the general theory of control systems. In: Proceedings of 1st IFAC Congress, Moscow 1960, Vol. 1, pp. 481–492. Butterworth, London (1961)
26. Kalman, R.E.: Lectures on controllability and observability, pp. 1–151. C.I.M.E. Summer Schools, Cremonese, Rome (1969)
27. Kalman, R.E., Ho, Y.C., Narendra, K.S.: Controllability of linear dynamical systems. Contrib. Differ. Equ. **1**(2), 189–213 (1962)
28. Konyagin, S.V.: On the number of irreducible polynomials with 0, 1 coefficients. Acta Arith. **88**(4), 333–350 (1999)
29. Knobloch, H.-W.: Zum Hilbertschen Irreduzibilitätssatz. Abh. Math. Sem. Univ. Hamburg **19**, 176–190 (1955)
30. Knobloch, H.-W.: Die Seltenheit der reduziblen Polynome, Jber. Deutsch. Math. Verein. **59**, Abt. 1, 12–19 (1956)
31. Kuba, G.: On the distribution of reducible polynomials. Math. Slovaca **59**(3), 349–356 (2009)
32. Moree, P.: Artin's primitive root conjecture—a survey. Integers **12**(6), 1305–1416 (2012)
33. Naumov, A.A.: The elliptic law for random matrices, Vestnik Moskov. Univ. Ser. XV Vychisl. Mat. Kibernet. **2013**, no. 1, 31–38, 48
34. Nguyen, H.H.: On the least singular value of random symmetric matrices. Electron. J. Probab. **17**(53), 1–19 (2012)
35. Nguyen, H.H., O'Rourke, S.: The elliptic law, Int. Math. Res. Not. IMRN **2015**, no. 17, 7620–7689
36. Nguyen, H.H., Vu, V.H.: Circular law for random discrete matrices of given row sum. J. Comb. **4**(1), 1–30 (2013)
37. Odlyzko, A.M., Poonen, B.: Zeros of polynomials with 0, 1 coefficients. L'Enseignement Mathématique **39**, 317–348 (1993)
38. O'Rourke, S., Renfrew, D., Soshnikov, A., Vu, V.: Products of independent elliptic random matrices. J. Stat. Phys. **160**(1), 89–119 (2015)
39. O'Rourke, S., Touri, B.: Controllability of random systems: universality and minimal controllability. arXiv:1506.03125, 9 Jun (2015)
40. O'Rourke, S., Touri, B.: On a conjecture of Godsil concerning controllable random graphs. arXiv:1511.05080, 16 Nov (2015)
41. Peled, R., Sen, A., Zeitouni, O.: Double roots of random Littlewood polynomials. Israel J. Math. **213**(1), 55–77 (2016)
42. Pólya, G.: Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen. Acta Math. **68**, 145–254 (1937)
43. Pomerance, C.: Popular values of Euler's function. Mathematika **27**(1), 84–89 (1980)
44. Rivin, I.: Galois Groups of Generic Polynomials. arXiv:1511.06446, 19 Nov (2015)
45. Rosser, J.B., Schoenfeld, L.: Approximate formulas for some functions of prime numbers. Ill. J. Math. **6**, 64–94 (1962)
46. Rudelson, M., Vershynin, R.: Non-asymptotic theory of random matrices: extreme singular values. In: Proceedings of the International Congress of Mathematicians. Volume III, pp. 1576–1602, Hindustan Book Agency, New Delhi
47. Tao, T., Vu, V.: Additive Combinatorics, Cambridge Studies in Advanced Mathematics, vol. 105. Cambridge University Press, Cambridge (2006)
48. Tao, T., Vu, V.: Local Universality of Zeroes of Random Polynomials. Int. Math. Res. Not. (2014). https://doi.org/10.1093/imrn/rnu084
49. Tao, T., Vu, V.: Random matrices: the circular law. Commun. Contemp. Math. **10**(2), 261–307 (2008)
50. Tao, T., Vu, V.: Random matrices have simple spectrum. arXiv:1412.1438, 3 Dec (2014)
51. Terlov, G.: Low-degree factors of random polynomials with large integer coefficients. Work in progress
52. Vershynin, R.: Invertibility of symmetric random matrices. Random Struct. Algorithms **44**, 135–182 (2014)
53. Vershynin, R.: Introduction to the non-asymptotic analysis of random matrices. In: Compressed Sensing, pp. 210–268. Cambridge University Press, Cambridge (2012)
54. van der Waerden, B.L.: Die Seltenheit der Gleichungen mit Affekt. Math. Ann. **109**(1), 13–16 (1934)
55. van der Waerden, B.L.: Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt. Monatsh. Math. Phys. **43**(1), 133–147 (1936)
56. Weiss, B.L.: Probabilistic Galois theory over p-adic fields. J. Number Theory **133**(5), 1537–1563 (2013)
57. Zywina, D.: Hilbert's irreducibility theorem and the larger sieve. arXiv:1011.6465, 30 Nov (2010)